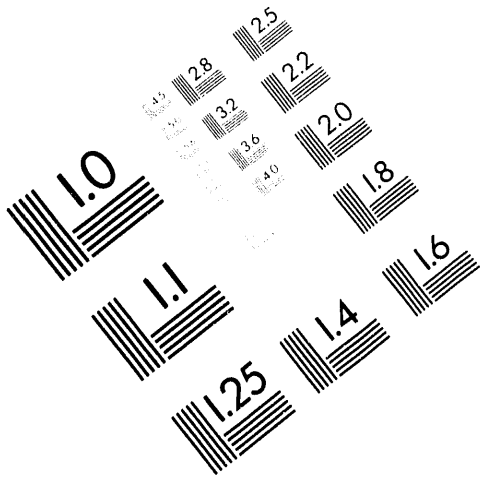


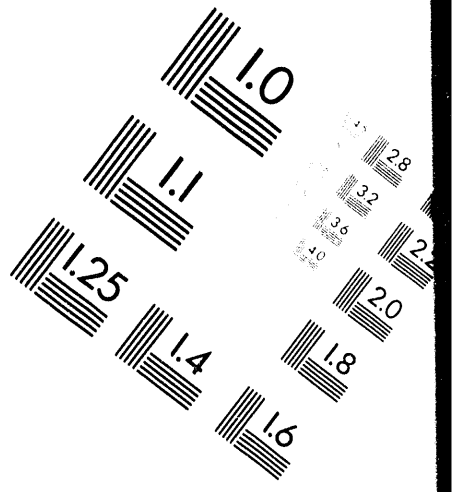


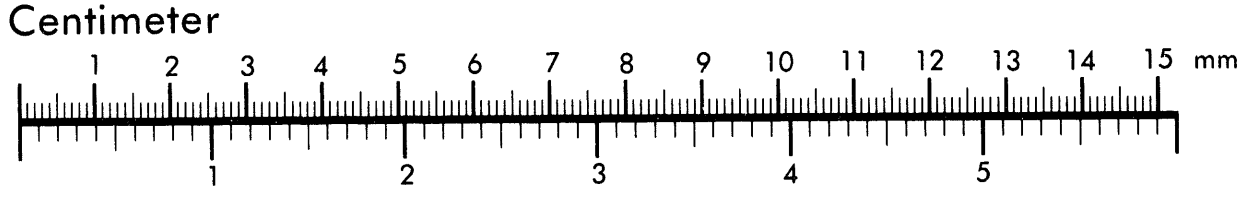
AIIM

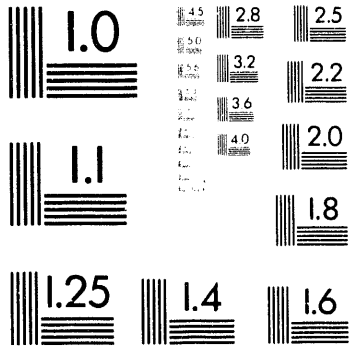
Association for Information and Image Management

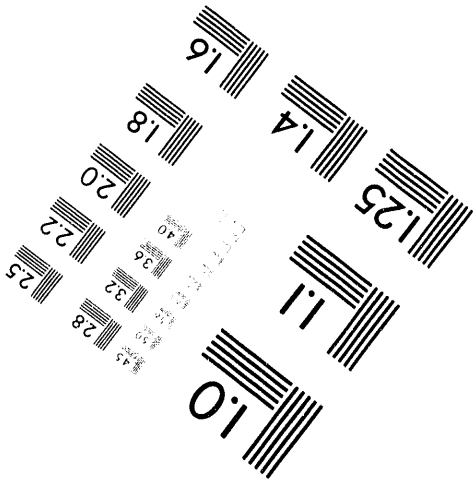
1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910

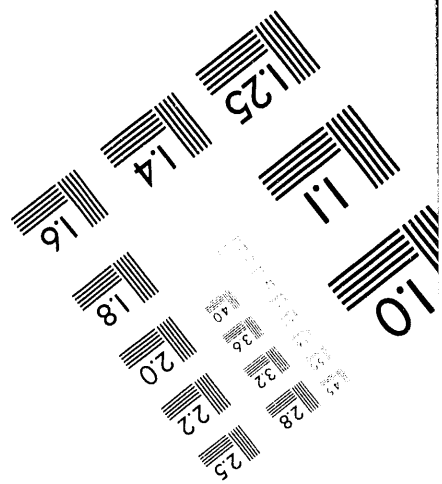
301/587-8202











MANUFACTURED TO AIIM STANDARDS
BY APPLIED IMAGE, INC.

1 of 7

CONF-931079--Vol.1

NUREG/CP-0133
Vol. 1

Proceedings of the U.S. Nuclear Regulatory Commission

Twenty-First Water Reactor Safety Information Meeting

Volume 1

- Plenary Session
- Advanced Reactor Research
- Advanced Control System Technology
- Advanced Instrumentation & Control Hardware
- Human Factors Research
- Probabilistic Risk Assessment Topics
- Thermal Hydraulics
- Thermal Hydraulic Research for Advanced Passive LWRs

Held at
Bethesda Marriott Hotel
Bethesda, Maryland
October 25–27, 1993

U.S. Nuclear Regulatory Commission

Office of Nuclear Regulatory Research

Proceedings prepared by
Brookhaven National Laboratory



NOTICE

These proceedings have been authored by a contractor of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in these proceedings, or represents that its use by such third party would not infringe privately owned rights. The views expressed in these proceedings are not necessarily those of the U.S. Nuclear Regulatory Commission.

Available from

Superintendent of Documents
U.S. Government Printing Office
Mail Stop SSOP
Washington, DC 20402-9328

and

National Technical Information Service
Springfield, VA 22161

NUREG/CP-0133
Vol. 1
R1,R2,R3,R4,R5,
R9,RD,RF,RG,
RM,RV,RW,RX

Proceedings of the U.S. Nuclear Regulatory Commission

Twenty-First Water Reactor Safety Information Meeting

Volume 1

- Plenary Session
- Advanced Reactor Research
- Advanced Control System Technology
- Advanced Instrumentation & Control Hardware
- Human Factors Research
- Probabilistic Risk Assessment Topics
- Thermal Hydraulics
- Thermal Hydraulic Research for Advanced Passive LWRs

Held at
Bethesda Marriott Hotel
Bethesda, Maryland
October 25-27, 1993

Manuscript Completed: March 1994
Date Published: April 1994

Compiled by Susan Monteleone

Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Proceedings prepared by
Brookhaven National Laboratory

MASTER

ABSTRACT

This three-volume report contains 90 papers out of the 102 that were presented at the Twenty-First Water Reactor Safety Information Meeting held at the Bethesda Marriott Hotel, Bethesda, Maryland, during the week of October 25-27, 1993. The papers are printed in the order of their presentation in each session and describe progress and results of programs in nuclear safety research conducted in this country and abroad. Foreign participation in the meeting included papers presented by researchers from France, Germany, Japan, Russia, Switzerland, Taiwan, and United Kingdom. The titles of the papers and the names of the authors have been updated and may differ from those that appeared in the final program of the meeting.

PROCEEDINGS OF THE
21st WATER REACTOR SAFETY INFORMATION MEETING

October 25-27, 1993

Published in Three Volumes

GENERAL INDEX

VOLUME 1

- Plenary Session
- Advanced Reactor Research
- Advanced Instrumentation and Control Hardware
- Advanced Control System Technology
- Human Factors Research
- Probabilistic Risk Assessment Topics
- Thermal Hydraulics
- Thermal Hydraulic Research for Advanced Passive LWRs

VOLUME 2

- Severe Accident Research

VOLUME 3

- Aging Research, Products and Applications
- Primary System Integrity
- Structural and Seismic Engineering
- Seismology and Geology

REGISTERED ATTENDEES (NON-NRC)
21st WATER REACTOR SAFETY INFORMATION MEETING

Y. ABE
NUCLEAR POWER ENGINEERING CORP.
3-17-1,TORANOMON,MINATO-KU
TOKYO, 105
JAPAN

S. ADDITON
TENERA/ARSAP
7272 WISCONSIN AVE., SUITE 300
BETHESDA, MD 20814
USA

K. AKHTAR
U.S. DEPT. OF ENERGY
19901 GERMANTOWN RD.
GERMANTOWN, MD 20874
USA

K. ALLARS
HM NUCLEAR INSTALLATIONS
BAYNARDS HOUSE, 1 CHEPSTOW PL.
WESTBOURNE GROVE, LONDON, W24TF
UK

R. ALLEN
PACIFIC NORTHWEST LABORATORY
BOX 999
RICHLAND, WA 99352
USA

M. ALLEN
SANDIA NATIONAL LABORATORIES
PO BOX 5800
ALBUQUERQUE, NM 87185
USA

C. ALLISON
INEL-EG&G, IDAHO
PO BOX 1625
IDAHO FALLS, ID 83402
USA

K. ALMENAS
UNIVERSITY OF MARYLAND
MAT. & NUCL. ENG. DEPT.
COLLEGE PARK, MD 20742
USA

A. ALONSO
MADRID POLYTEC. UNIV.
J. GUTIERREZ ABASCAL, 2
MADRID, 28006
SPAIN

A. AMAEV
KURCHATOV INSTITUTE
123182 KURCHATOV SQ.
MOSCOW,
RUSSIA

H. AMARISOORIYA
SCIENTECH
11821 PARKLAWN DR.
ROCKVILLE, MD 20852
USA

L. ANDERMO
SKI
PO BOX 27406
STOCKHOLM, 10252
SWEDEN

B. ARCIERI
SCIENTECH
11821 PARKLAWN. DR.
ROCKVILLE , MD 20852
USA

N. ARDEY
TECHNICAL UNIVERSITY MUNICH
SENSERSTRASSE 15
81371 MUNICH, 81371
GERMANY

H. ASAKA
JAPAN ATOMIC ENERGY RESEARCH INST.
SHIRAKATA
TOKA-MURA, IBARAKI-KEN 319-11
JAPAN

H. ASCHER
H.E. ASCHER & ASSOCIATES
11916 GOYA DRIVE
POTOMAC, MD 20854
USA

V. ASMOLOV
KURCHATOV INSTITUTE
123182 KURCHATOV SQ.
MOSCOW,
RUSSIA

K. BANDYOPADHYAY
BROOKHAVEN NATIONAL LABORATORY
PO BOX 5000, BLDG. 475C
UPTON, NY 11973-5000
USA

Y. BANG
KOREA INSTITUTE OF NUCLEAR SAFETY
ADVANCED REACTOR DEPT, KINS, PO BOX 6
TAEJON, 305-635
KOREA

A. BARATTA
PENN STATE UNIVERSITY
231 SACKETT
UNIVERSITY PARK, PA 16802
USA

R. BARI
BROOKHAVEN NATIONAL LABORATORY
P.O. BOX 5000, BLDG. 197C
UPTON, NY 11973-5000
USA

M. BARNES
AEA TECHNOLOGY
THOMSON HOUSE, RISLET, WARRINGTON
CHESHIRE, WA36A7
UK

V. BARNES
COMPA INDUSTRIES, INC.
270 WALKER DR., STE. 102
STATE COLLEGE, PA 16801
USA

E. BASSANSKY
KURCHATOV INSTITUTE
123182 KURCHATOV SQ.
MOSCOW,
RUSSIA

D. BHARGAVA
VIRGINIA POWER
5000 DOMINION BLVD.
GLEN ALLEN, VA 23060
USA

W.K BINNER
AUSTRIAN RESEARCH CENTER CONSULTANT
GORGENGASSE 30/3
WIEN, VIENNA A-1190
AUSTRIA

T. BLANCHAT
SANDIA NATIONAL LABORATORIES
PO BOX 5800
ALBUQUERQUE, NM 87185
USA

L. BOLSHOV
RUSSIAN ACADEMY OF SCIENCES
52 B. TULSKAYA
MOSCOW,
RUSSIA

M. BONNER
BROOKHAVEN NATIONAL LABORATORY
BLDG. 197C
UPTON, NY 11973
USA

S. BOUGAENKO
R&D INSTITUE OF POWER ENGINEERING
P.O. BOX 788
MOSCOW, 101000
RUSSIA

M. BOWMAN
BALTIMORE GAS & ELECTRIC
CCNPP BG&E
LUSBY, MD 20657
USA

B. BOYACK
LOS ALAMOS NATIONAL LABORATORY
PO BOX 1663, MS K551
LOS ALAMOS, NM 87545
USA

M. BRECK
NUS
910 CLOPPER ROAD
GAITHERSBURG, MD 20878
USA

G. BROWN
AEA TECHNOLOGY
THOMSON HOUSE, RISLEY
WARRINGTON, CHESHIRE 2A3 6AT
UK

D. BROWNSON
EG&G IDAHO, INC.
PO BOX 1625
IDAHO FALLS, ID 83415
USA

I. BRUCE
NUCLEAR INSTALLATIONS INSPECTORATE
ST. PETERS HOUSE, BALLIOL ROAD
BOOTLE, MERSEYSIDE
UK

C. BUCHHOLZ
GE NUCLEAR ENERGY
175 CURTNER AVE M/C 754
SAN JOSE, CA 95125
USA

R. BUDNITZ
FUTURE RESOURCES ASSOCIATES, INC.
2000 CENTER ST., SUITE 418
BERKELEY, CA 94704
USA

J. BURTT
INEL/EG&G IDAHO INC.
P.O. BOX 1625
IDAHO FALLS, ID 83415-3895
USA

R. CARO-MANSO
CONSEJO SEGURIDAD NUCLEAR
C/JUSTO DORADO
MADRID,
SPAIN

D. CASADA
OAK RIDGE NATIONAL LABORATORY
PO BOX 2009
OAK RIDGE, TN 37831-8038
USA

G. CENERINO
INST. DE PROTECTION ET DE SURETE NUCLEAIRE
60-68 AV. DU GENERAL LECLERC
FONTENAY-AUX-ROSES, 8P6-92265
FRANCE

S. CHAE
KOREA ATOMIC ENERGY RESEARCH INSTITUTE
PO BOX 7, DAEDUK-DANJI
TAEJEON, 305-606
KOREA

M. CHAIKO
PENNSYLVANIA POWER & LIGHT CO.
2 N. 9TH ST.
ALLENTOWN, PA 18101
USA

O. CHAKH
RRC KURCHATOV INSTITUTE
123182 KURCHATOV SQ.
MOSCOW,
RUSSIA

Y-B CHEN
ATOMIC ENERGY COUNCIL, R.O.C.
67 LANE 144, KEELUNG RD. SEC. 4
TAIPEI, TAIWAN
ROC

C. CHEN
GILBERT/COMMONWEALTH INC.
PO BOX 498
READING, PA 19603
USA

T. CHIBA
ISHIKAWAJIMA-HARIMA HEAVY INDUST.
1,SHIN-NAKAHARA-CHO, ISOGO-KU
YOKOHAMA, KANAGAWA 235
JAPAN

T-H CHIEN
ARGONNE NATIONAL LABORATORY
9700 S. CASS AVE.
ARGONNE, IL 60439
USA

O. CHOPRA
ARGONNE NATIONAL LABORATORY
9700 S. CASS AVENUE
ARGONNE, IL 60439
USA

T-L CHU
BROOKHAVEN NATIONAL LABORATORY
PO BOX 5000, BLDG. 130
UPTON, NY 11973-5000
USA

T. CHU
SANDIA NATIONAL LABORATORIES
PO BOX 5800
ALBUQUERQUE, NM 87185
USA

C. CHUANG
ATOMIC ENERGY COUNCIL, R.O.C.
67 LANE 144, KEELUNG RD. SEC. 4
TAIPEI, TAIWAN
ROC

V. CHUDANOV
NSI RUSSIAN ACADEMY
B. TULSKAYA
MOSCOW, 113191
RUSSIA

D. CHUNG
SCIENTECH
11821 PARKLAWN DR.
ROCKVILLE , MD 20852
USA

H. CHUNG
ARGONNE NATIONAL LABORATORY
9700 S. CASS AVENUE
ARGONNE, IL 60438
USA

M. COLIN
CEA
80-68 AVENUE DU GENERAL LECLERC
FONTENAY AUX ROSES CEDEX, 92365
FRANCE

A. COMBESCURE
CEA-CENTRE DE SACLAY
DRN/DMT/SEMT-BAT.454
GIF-sur-YVETTE CEDEX, 91191
FRANCE

S. CONVERSE
NORTH CAROLINA STATE UNIVERSITY
BOX 7801
RALEIGH, NC 27965
USA

S. COOPER
SCIENCE APPLICATIONS INTERNATIONAL CORP.
1710 GOODRIDGE DRIVE
MC LEAN, VA
USA

W. CORWIN
OAK RIDGE NATIONAL LABORATORY
P.O. BOX 2008
OAK RIDGE, TN 37831-6151
USA

K. COZENS
NUMARC
1776 I ST., NW, STE 300
WASHINGTON, DC 20006
USA

H. CURRIN
MARTIN-MARIETTA
1 RIVER ROAD
NISKAYUNA, NY 12302
USA

H. CURRIN
KNOLLS ATOMIC POWER LAB
RIVER RD.
SCHENECTADY, NY 12309
USA

R. CURTIS
AECL TECHNOLOGIES
9210 CORPORATE BLVD.
ROCKVILLE, MD 20850
USA

F. DAVIS
SANDIA NATIONAL LABORATORIES
PO BOX 5800, DEPT. 6429
ALBUQERQUE, NM 87185
USA

B. DE BOECK
AIB-VINCOTTE NUCLEAIRE
AVENUE DU ROI 157
BRUSSELS, B-1060
BELGIUM

J. DeBOR
SCIENCE & ENGINEERING ASSOCIATES
1700 ROCKVILLE PIKE, ST. 400
ROCKVILLE, MD 20852
USA

E. DEL ANGEL
CNSNS/MEXICO
DR. BARRAGN #779, COL NARVARTE
MEXICO D.F., 03020
MEXICO

J. DETERMAN
EG&G IDAHO, INC.
PO BOX 1625
IDAHO FALLS, ID 83415
USA

H. DEZFULI
SCIENTECH
11821 PARKLAWN DR.
ROCKVILLE, MD 20852
USA

M. DIETRICK
WESTINGHOUSE BETTIS
2895 O'NEILL DR.
BETHEL PARK, PA 15102
USA

M. DIMARZO
UNIVERSITY OF MARYLAND
MECHANICAL ENG. DEPT.
COLLEGE PARK, MD 20742
USA

S. DOCTOR
PACIFIC NORTHWEST LABORATORY
PO BOX 999, MSIN K5-26
RICHLAND, WA 99352
USA

S. DOROFEEV
KURCHATOV INSTITUTE
123182 KURCHATOV SQ.
MOSCOW,
RUSSIA

S. DRUCE
AEA TECHNOLOGY
REACTOR SVCS., B10-28
OXFORDSHIRE, OX11ORA
UK

G. DUPRE
CENTRE NATL. DE LA RECHERCHE SCIENTIFIQUE
1 C AVENUE DE LA RECHERCHE SCIENTIFIQUE
ORLEANS, CEDEX 2 45071
FRANCE

Z. ELAWAR
ARIZONA PUBLIC SERVICE CO.
PO BOX 52034
PHOENIX, AZ 85072
USA

B. EVANS
NUMARC
1776 I ST., NW, STE 300
WASHINGTON, DC 20006
USA

B. FINK
MPR ASSOCIATES, INC.
320 KING ST.
ALEXANDRIA, VA 22314-3238
USA

E. FOX
ORNL, MARTIN MARIETTA ENERGY SYSTEMS
PO BOX 2009
OAK RIDGE, TN 37831
USA

R. GAUNTT
SANDIA NATIONAL LABORATORIES
PO BOX 5800, DEPT. 6423
ALBUQUERQUE, NM 87185
USA

J. GIAMPETRO
WESTINGHOUSE BETTIS
2895 O'NEILL DR.
BETHEL PARK, PA 15102
USA

B. GITNICK
SCIENTECH
11821 PARKLAWN DR.
ROCKVILLE , MD 20852
USA

S. DINGMAN
SANDIA NATIONAL LABORATORIES
DEPT. 6413, PO BOX 5800
ALBUQUERQUE, NM 87185
USA

G. DOMINICI
L'ENERGIA E L'AMBIENTE
VIA MARTIRI DO MONTE SOLE, 4
BOLOGNA, 40129
ITALY

M. DOSTER
NORTH CAROLINA STATE UNIVERSITY
BOX 7909
RALEIGH, NC 27695
USA

R. DUFFEY
BROOKHAVEN NATIONAL LABORATORY
PO BOX 5000
UPTON, NY 11973-5000
USA

R. DURANTE
AECL TECHNOLOGIES
9210 CORPORATE BLVD.
ROCKVILLE, MD 20850
USA

G. EMBLEY
KAPL
BOX 1072
SCHENECTADY, NY 12301
USA

R. FAKORY
S3 TECHNOLOGIES, INC.
8930 STANFORD BLVD.
COLUMBIA, MD 21045
USA

M. FONTANA
OAK RIDGE NATIONAL LABORATORY
PO BOX 2009
OAK RIDGE, TN 37831-8056
USA

P. FULFORD
NUS
910 CLOPPER RD.
GAITHERSBURG, MD 20878
USA

G. GAUTHIER
CEA-IPSN
BP8 60-68 AVE. DU GENERAL LECLERC
FONTENAY AUX ROSES, P92265
FRANCE

R. GILLILAND
OAK RIDGE NATIONAL LABORATORY
PO BOX 2009
OAK RIDGE, TN 37831
USA

F. GIUDICE
AECL-CANDU
2251 SPEAKMAN DR.
MISSISSAUGA, ONTARIO L5K1B2
CANADA

N. DJEBAILI
CENTRE NATL. DE LA RECHERCHE SCIENTIFIQUE
1 C AVENUE DE LA RECHERCHE SCIENTIFIQUE
ORLEANS, CEDEX 2 45071
FRANCE

R. DOREMUS
ADVANCED RESOURCE DEVELOPMENT CORP.
9151 RUMSEY RD.
COLUMBIA, MD 21045
USA

Y. DRAGUNOV
EDO GIDROPRESS
STREET ORDZHONIKIDZE,21
MOSCOW DISTRICT, P 142103
RUSSIA

A. DUMONTET
ELECTRICITE DE FRANCE/SEPTEN
12-14 AVENUE DUTRIEVOZ
VILLEURBANNE, 69628
FRANCE

E. EASON
MODELING & COMPUTING SERVICES
CEDAR BLVD, SUITE 290
NEWARK, CA 94560
USA

H. ESMAILI
ENERGY RESEARCH, INC.
6290 MONTROSE RD.
ROCKVILLE, MD 20847
USA

N. FARUKHI
NUMARC
1776 I ST., NW, STE 300
WASHINGTON, DC 20006
USA

T. FOULT
COMMISSARIAT A L'ENERGIE ATOMIQUE
60-68 AVE. DU GENERAL LECLERC
FONTENAY-AUX-ROSES, 92265
FRANCE

H. GALE
TRW ENVIRONMENTAL SAFETY SYSTEMS, INC.
2650 PARK TOWER DR., STE 800
VIENNA, VA 22180
USA

G. GEISSLER
B&W NUCLEAR TECHNOLOGIES
3315 OLD FOREST RD, PO BOX 10935
LYNCHBURG, VA 24506-0935
USA

T. GINSBERG
BROOKHAVEN NATIONAL LABORATORY
PO BOX 5000, BLDG. 197D
UPTON, NY 11973-5000
USA

M. GOLOVKOV
DIAGNOSTIC COMPLEKS & SYSTEMS
KITAYSKIY PR., 7
MOSCOW, 103073
RUSSIA

M. GOMOLINSKI
INST. DE PROTECTION E DE SURETE NUCLEAIRE
321 RUE DE CHARENTON
PARIS, 75012
FRANCE

R. GREENE
OAK RIDGE NATIONAL LABORATORY
PO BOX 2009
OAK RIDGE, TN 37831-8038
USA

E. HARVEGO
IDAHO NATIONAL ENGINEERING LAB
PO BOX 1625
IDAHO FALLS, ID 83415
USA

M. HASTINGS
OHIO STATE UNIVERSITY
206 W. 18TH AVE
COLUMBUS, OH 43210-1107
USA

T. HEAMES
SCIENCE APPLICATIONS INTERNATIONAL CORP.
2109 AIR PARK RD.
ALBUQUERQUE, NM 87106
USA

L. HERRANZ
CIEMAT-ITN
AVENIDA COMPLUTENSE, 22
MADRID, 28040
SPAIN

J. HIGHTON
NUCLEAR INSTALLATIONS INSPECTORATE
ST. PETERS HOUSE, STANLEY PRECINCT
BOOTLE, MERSYSIDE L20
UK

P. HOFMANN
K/K NUCLEAR RESEARCH CENTER
PO BOX 3640
KARLSRUHE, 76021
GERMANY

Y. HORIKAWA
KANSAI ELECTRIC POWER
1100 17TH ST., NW
WASHINGTON, DC 20036
USA

T. HSU
VIRGINIA POWER
5000 DOMINION BLVD.
GLEN ALLEN, VA 23060
USA

M. ICHIKAWA
JAPAN ATOMIC ENERGY RESEARCH INST.
SHIRAKATA
TOKAI-MURA, IK 319-11
JAPAN

H. ISBIN
NSRRC
2815 MONTEREY PKWY.
ST. LOUIS PARK, MN 55416
USA

W. GRANT
AECB-CANADA
280 SLATER
OTTAWA, ONTARIO K1P 5S9
CANADA

F. GRIFFIN
OAK RIDGE NATIONAL LABORATORY
P.O. BOX 2009, M.S. 8057
OAK RIDGE, TN 37831-8057
USA

R. HARVEY
YANKEE ATOMIC ELECTRIC CO.
580 MAIN ST.
BOLTON, MA 01740
USA

J. HAWTHORNE
MATERIALS ENGINEERING ASSOCIATES, INC.
9700-B M.L. KING, JR. HWY.
LANHAM, MD 20706-1837
USA

M. HEITSCH
Gesellschaft fur Anlagen und Reaktorsicherheit
SCHWERTNERGASSE 1
KOLN 1, 50667
GERMANY

M. HESSHEIMER
SANDIA NATIONAL LABORATORIES
DEPT. 6449
ALBUQUERQUE, NM 87185
USA

H. HIRSCHMANN
PAUL SCHERRER INSTITUTE
CH-5232 VILLIGEN PSI
SWITZERLAND

C. HOFMAYER
BROOKHAVEN NATIONAL LABORATORY
BLDG. 475C
UPTON, NY 11973
USA

P. HOSEMANN
PAUL SCHERRER INSTITUT
WURENLINGEN UND VILLIGEN
VILLIGEN, CH-5232
SWITZERLAND

E. HUBNER
STONE & WEBSTER ENGINEERING
3 EXECUTIVE CAMPUS, PO BOX 5200
CHERRY HILL, NJ 08034
USA

K. IKONEN
VTT TECH. RESEARCH CENTRE OF FINLAND
PO BOX 208
ESPOO, 02151
FINLAND

M. ISHII
PURDUE UNIVERSITY
NUCLEAR ENGINEERING
WEST LAFAYETTE, IND 47907
USA

W. GRANT
MPR ASSOCIATES
320 KING ST.
ALEXANDRIA, VA 22314-3238
USA

C. HALIEMUN
ABACUS TECHNOLOGY CORP.
5454 WISCONSIN AVENUE, SUITE 1100
CHEVY CHASE, MD 20815
USA

H. HASHEMIAN
ANALYSIS & MEASUREMENT SERVICES CORP.
9111 CROSS PARK DR.
KNOXVILLE, TN 37923-4599
USA

P. HAYES
MPR ASSOCIATES
320 KING ST.
ALEXANDRIA, VA 22314-3238
USA

K. HENRIKSEN
CAE-LINK CORPORATION
5111 LEESBURG PIKE
FALLS CHURCH, VA 22041
USA

J. HIGGINS
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130
UPTON, NY 11973
USA

S. HODGE
OAK RIDGE NATIONAL LABORATORY
P.O. BOX 2009, M.S. 8057
OAK RIDGE, TN 37831-8057
USA

D. HOLCOMB
ORNL; MARTIN MARIETTA ENERGY SYSTEMS
PO BOX 2008
OAK RIDGE, TN 37831-6010
USA

M-T HSU
ATOMIC ENERGY COUNCIL, R.O.C.
67 LANE 144, KEELUNG RD. SEC. 4
TAIPEI, TAIWAN
ROC

R. HUDDLESTON
OAK RIDGE NATIONAL LABORATORY
PO BOX 2009
OAK RIDGE, TN 37831-8056
USA

M. INAGAKI
NUCLEAR POWER ENGINEERING CORP.
3-17-1 #7 FL, TORANOMON, MINATO-KU
TOKYO, 105
JAPAN

S. ISKANDER
OAK RIDGE NATIONAL LABORATORY
4500S MS6151/P.O. BOX 2008
OAK RIDGE, TN 37921
USA

N. ITO
MITSUBISHI HEAVY INDUSTRIES, LTD.
2-4-1,SHIBAKOEN, MINATO-KU
TOKYO, 105
JAPAN

J. JANSKY
BTB-JANSKY GmbH
GERLINGER STR. 152
725 LEONBERG,
GERMANY

G. JOHNSEN
IDAHO NATIONAL ENGINEERING LABS
PO BOX 1625
IDAHO FALLS, ID 83415
USA

C. JONES
SCIENTECH
11821 PARKLAWN DR.
ROCKVILLE, MD 20852
USA

J. JUDD
IDAHO NATIONAL ENGINEERING LABS
PO BOX 1625-3890
IDAHO FALLS, ID 83415
USA

H. KARWAT
TECHNICAL UNIV. MUNICH
FORSCHUNGSGELANDE
GARCHING, 85748
GER' ANY

M. KATO
TOSHIBA CORP.
8 SHINSUGITA-CHO, ISOGO-KU
YOKOHAMA, KANAGAWA 235
JAPAN

D. KELLY
GILBERT/COMMONWEALTH, INC.
PO BOX 1498
READING, PA 19603
USA

H. KIM
KOREA ATOMIC ENERGY RESEARCH INST.
PO BOX 7, DAEDUK-DANJI
TAEJEON, 305-606
KOREA

M. KINOSHITA
BROOKHAVEN NATIONAL LABORATORY
PO BOX 5000, BLDG. 197D
UPTON, NY 11973-5000
USA

D. KNUDSON
EG&G IDAHO, INC.
PO BOX 1625
IDAHO FALLS, ID 83415
USA

C. KOT
ARGONNE NATIONAL LABORATORY
9700 S. CASS AVE, BLDG. 331
ARGONE, IL 60439
USA

K. IWAMOTO
NUCLEAR POWER ENGINEERING CORP.
3-17-1,TORANOMON,MINATO-KU
TOKYO, 105
JAPAN

I. JANSSON
ABB ATOM AKTIEBOLAG

VASTERAS, S72163
SWEDEN

AB JOHNSON
PACIFIC NORTHWEST LABORATORY
BATTELE, N.W., P8-10
RICHLAND, WA 99352
USA

F. JOPPEN
STRALINGSKONTROLE, KEURING & VEILIGHEID
BOERETANG 200
, 2400 MOL
BELGIUM

F. KAM
OAK RIDGE NATIONAL LABORATORY
PO BOX 2009
OAK RIDGE, TN 37831-8056
USA

G. KARZOV
CENT. RES. INST.-STRUCTURAL ANALYSIS
193167 NABEREZHNAYA REKY MONASTYRKY I
ST. PETERSBURG,
RUSSIA

K. KAWANISKI
MITSUBISHI HEAVY INDUSTRIES
2-1-1 SHINNAMA ARAI-CHO
TAKASAGO, HYOGO 676
JAPAN

D. KELLY
IDAHO NATIONAL ENGINEERING LABS
11426 ROCKVILLE PIKE, STE. 300
ROCKVILLE, MD 20852
USA

I. KIM
BROOKHAVEN NATIONAL LABORATORY
PO BOX 5000, BLDG. 130
UPTON, NY 11973-5000
USA

P. KLOEG
KEMA
POST BOX 9035
ARNHEM, 6800ET
THE NETHERLANDS

K. KORSAH
OAK RIDGE NATIONAL LABORATORY
PO BOX 2008
OAK RIDGE, TN 37831-6010
USA

V. KOVYRSHIN
SCNRS

KIEV,
UKRAINE

A. IWANAGA
NUCLEAR POWER ENGINEERING CORP.
3-17-1 #7 FL, TORANOMON, MINATO-KU
TOKYO, 105
JAPAN

Y. JIN
KOREA ATOMIC ENERGY RESEARCH INST.
P.O. BOX 7, DAEDUK-DANJI
TAEGON,
KOREA

E. JONES
U.C. LAWRENCE LIVERMORE NAT'L LAB
PO BOX 808, L-190
LIVERMORE, CA 94550
USA

J. JOYCE
USNA, DEPT. OF MECHANICAL ENGINEERING

ANNAPOLIS, MD 21402
USA

H. KARASAWA
HITACHI LTD
5-2-2,OMIKA-CHO
HITACHI, IRARAKI 319-12
JAPAN

D. KATAYANAGI
HITACHI ENGINEERING CO., LTD.
2-1, SAIWAI-CHO 3-CHOME
HITACHI-SHI, IBARAKI-KEN 317
JAPAN

K. KELKAR
INNOVATIVE RESEARCH, INC.
2800 UNIVERSITY AVENUE SE
MINNEAPOLIS, MN 55414
USA

M. KHATIB-RAHBAR
ENERGY RESEARCH, INC.
6290 MONTROSE RD.
ROCKVILLE, MD 20852
USA

S. KINNERSLY
AEA TECHNOLOGY
LINFRITH TECHNOLOGY CENTRE
DORCHESTER, DORSET DT28DH
UK

L. KMETYK
SANDIA NATIONAL LABORATORIES
PO BOX 5800
ALBUQUERQUE, NM 87185-5800
USA

G. KORTH
EG&G IDAHO, INC.
PO BOX 1625
IDAHO FALLS, ID 83415-2216
USA

A. KRAEV
R&D INSTITUTE OF POWER ENGINEERING
P.O. BOX 788
MOSCOW, 101000
RUSSIA

C. KRAMER
GILBERT/COMMONWEALTH, INC.
PO BOX 1498
READING, PA 19603
USA

A. KRYUKOV
KURCHATOV INSTITUTE
123182 KURCHATOV SQ.
MOSCOW,
RUSSIA

J. KUJAL
NUCLEAR RESEARCH INSTITUTE REZ PLC
NUCL RES. INST./REZ NEAR PRAGUE
,
CZECH REP.

C. KUKIELKA
PENNSYLVANIA POWER & LIGHT CO.
2 N. 9TH ST.
ALLENTOWN, PA 18101
USA

Y. KURAKOV
USSR MINISTRY OF NUCLEAR POWER & INDUSTRY
STAROMONETNY 26
MOSCOW, 109180
RUSSIA

K. KUSSMAUL
MPA STUTTGART
PFAFFENWALDRING 32
STUTTGART, BADEN-WURTTEMBERG 70569
GERMANY

J. LAKE
EG&G IDAHO, INC.
PO BOX 1625, MS 3880
IDAHO FALLS, ID 83415
USA

A. LAKNER
VIKING SYSTEMS INTERNATIONAL
101 CHESTNUT ST.
GAITHERSBURG, MD 20877
USA

K. LAM
LOS ALAMOS NATIONAL LABORATORY
PO BOX 1663, MS K575
LOS ALAMOS, NM 87545
USA

L. LAMBERT
SANDIA NATIONAL LABORATORIES
DEPT. 6449
ALBUQUERQUE, NM 87185
USA

L. LARSON
WESTINGHOUSE BF[illegible]IS
2895 O'NEILL DR.
BETHEL PARK, PA 15102
USA

K. LAUGHERY
MICRO ANALYSIS AND DESIGN
4900 PEARL EAST CIRCLE
BOULDER, CO 80301
USA

R. LAW
VIRGINIA TECH
GEOLOGICAL SCIENCES
BLACKSBURG, VA 24061
USA

C. LECOMTE
INST. DE PROTECTION ET DE SURETE NUCLEAIRE
60-68 AV. DU GENERAL LECLERC
FONTENAY-AUX-ROSES, BP6-92265
FRANCE

M. LEE
NATIONAL TSING HUA UNIVERSITY
NATION TSING HUS UNIV, DEPT. N.E.
HSINCHU,
TAIWAN

J. LEHNER
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, PO BOX 5000
UPTON, NY 11973-5000
USA

C. LENGLADE
IDAHO NATIONAL ENGINEERING LABS
PO BOX 1625
IDAHO FALLS, ID 83415-3880
USA

A. LERIDON
COMMISSARIAT A L'ENERGIE ATOMIQUE
C.E. CADARACHE DEC/SECA
ST. PAUL LES DURANCE, 13108
FRANCE

S. LEVINSON
B&W NUCLEAR TECHNOLOGIES
3315 OLD FOREST RD
LYNCHBURG, VA 24501
USA

V. LEVIT
KURCHATOV INSTITUTE
123182 KURCHATOV SQ.
MOSCOW,
RUSSIA

D. LIDBURY
AEA TECHNOLOGY
RISLEY, WARRINGTON
CHESHIRE, WA36AT
UK

A. LING
ATOMIC ENERGY CONTROL BOARD
C/O ONTARIO HYDRO, PO BOX 160
PICKERING, ONTARIO L1V 2R5
CANADA

R. LINK
U.S. NAVY
CDNSWC 614
ANNAPOLIS, MD 21402
USA

M. LIVOLANT
INST. DE PROTECTION E DE SURETE NUCLEAIRE
CE/FONTENAY AUX ROSES
CEDEX, 92265
FRANCE

R. LOFARO
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130
UPTON, NY 11973
USA

P. LOPEZ
CNSNS/MEXICO
DR. BARRAGN #779 COL NARVAR
MEXICO D.F., 03020
MEXICO

R. LORENZ
OAK RIDGE NATIONAL LABORATORY
P.O. BOX 2008-6221
OAK RIDGE, TN 37831
USA

F. LOSS
MATERIALS ENGINEERING ASSOCIATES, INC.
9700-B M.L. KING, JR. HWY.
LANHAM, MD 20706-1837
USA

A. LOWE, JR.
LOWE ASSOCIATES
P.O. BOX 11964
LYNCHBURG, VA 24506-1964
USA

W. LUCKAS
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, PO BOX 5000
UPTON, NY 11973-5000
USA

J. LYLE
NIST
TECHNOLOGY BLDG B266
GAITHERSBURG, MD 20850
USA

P. MAC DONALD
EG&G IDAHO, INC
PO BOX 1625
IDAHO FALLS, ID 83415-3860
USA

H. MACHIBA
TOSHIBA CORP.
8 SHINSUGITA-CHO, ISOGO-KU
YOKOHAMA, KANAGAWA 235
JAPAN

A. MACHIELS
ELECTRIC POWER RESEARCH INSTITUTE
3412 HILLVIEW, PO BOX 10412
PALO ALTO, CA 94303
USA

T. MADDEN
STONE & WEBSTER ENGINEERING
3 EXECUTIVE CAMPUS, PO BOX 5200
CHERRY HILL, NJ 08034
USA

I. MADNI
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, PO BOX 5000
UPTON, NY 11973-5000
USA

D. MAGALLON
CED, JRC, ISPRA
HRC-EURATOM - ISPRA
ISPRA, 21020
ITALY

C. MALLON
NEWMAN & HOLTZINGER, PC
1615 L. SR. N.W.
WASHINGTON, DC 20036
USA

R. MARTINELLI
ENEA, ENERGY DEPT.
CRE CASACCIA, 301 V. ANGUILLARESE
ROME, 00060
ITALY

J. MARTINEZ
CSN SPAIN
C/JUSTO DORADO 11
MADRID, 28040
SPAIN

Y. MARUYAMA
JAPAN ATOMIC ENERGY RESEARCH INST.
TOKAI-MURA, NAKA-GUN
IBARAKI-KEN, 319-11
JAPAN

M. MASSOUD
BALTIMORE GAS & ELECTRIC
CALVERT CLIFFS NPP
LUSBY, MD 20657
USA

B. MAVKO
INSTITUTE J. STEFAN
JAMOVA 39, PO BOX 100
LJUBLIANA, 61111
SLOVENIA

W. McAFEE
MARTIN MARIETTA ENERGY SYSTEMS
P.O. BOX 2009
OAK RIDGE, TN 37831-8047
USA

R. McCARDELL
EG&G IDAHO, INC.
167 N. 4200 E
RIGBY, ID 83442
USA

N. McMILLAN
AEA TECHNOLOGY
THOMSON HOUSE, RISLEY
WARRINGTON, CHESHIRE 2A3 6AT
UK

C. MEDICH
SOCIETA INFORMAZIONE ESPERIENZE TERMOIDRA
VIA NINO BIXIO, 27
PIACENZA, 29100
ITALY

J. MEINCKE
CONSUMERS POWER CO.
1156 OAK HAMPTON RD.
HOLLAND, MI 49424
USA

E. MENARD
KNOLLS ATOMIC POWER LAB/MARTIN MARIETTA
P.O. BOX 1072
SCHENECTADY, NY 12301-1072
USA

M. MERILO
ELECTRIC POWER RESEARCH INST.
3412 HILLVIEW AVE.
PALO ALTO, CA 94304
USA

A. MEYER-HEINE
INST. DE PROTECTION ET DE SURETE NUCLEAIRE
CEN CADARACHE DRS/SENAR
ST. PAUL LEZ DURANCE, 13108
FRANCE

M. MILLER
DUKE POWER CO.
OCONEE DIV., PO BOX 219
SENECA, SC 29679
USA

N. MIYAZAKI
KYUSYU UNIVERSITY
6-10-1. HAKOSAKI,HIGASHI-KU
FUKUOKA, FUKUOKA 812
JAPAN

D. MODEEN
NUMARC
1776 I ST., NW, STE 300
WASHINGTON, DC 20006
USA

M. MODRO
EG&G IDAHO, INC.
P.O. BOX 1625, MS 3895
IDAHO FALLS, ID 83515
USA

D. MONHARDT
FRAMATOME S.A.
1 PLACE DE LA COUPOLE TOUR FIAT
PARIS-LA-DEFENSE, CEDEX 16-92084
FRANCE

S. MONTELEONE
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, PO BOX 5000
UPTON, NY 11973-5000
USA

S. MOROZOV
JCCCNRS-WG12

RUSSIA

I. MOSEVITSKI
RRC KURCHATOV INSTITUTE
123182 KURCHATOV SQ.
MOSCOW,
RUSSIA

PROF. MULLER
KERNFORSCHUNGSZENTRUM
POSTFACH 3640
KARLSRUHE, D-76021
GERMANY

R. MUMAW
WESTINGHOUSE STC
13100 BEULAH RD.
PITTSBURGH, PA 15235
USA

K. NAMATAME
JAPAN ATOMIC ENERGY RESEARCH INST.
SHIRAKATA
TOKAI-MURA, IK 319-11
JAPAN

R. NANSTAD
OAK RIDGE NATIONAL LABORATORY
45008 MS6151/P.O. BOX 2008
OAK RIDGE, TN 37831
USA

D. NAUS
OAK RIDGE NATIONAL LABORATORY
PO BOX 2009, MS-8056
OAK RIDGE, TN 37831-8056
USA

C. NEGIN
GROVE ENGINEERING
15215 SHADY GROVE RD., STE. 200
ROCKVILLE, MD 20850
USA

D. NEWLAND
ATOMIC ENERGY CONTROL BOARD
280 SLATER STREET
OTTOWA, ONTARIO K1P5S9
CANADA

G. NIEDERAUER
LOS ALAMOS NATIONAL LABORATORY
MS K 575
LOS ALAMOS, NM 87554
USA

V. NIKOLAEV
CENT. RES. INST.-STRUCTURAL ANALYSIS
193167 NABEREZHNAYA REKY MONASTY. 1
ST. PETERSBURG,
RUSSIA

L. NILSSON
STUDSVIK ECO & SAFETY
S-611 82 NYKOPING

SWEDEN

A. NONAKA
NUCLEAR POWER ENGINEERING CORP.
3-17-1,TORANOMON,MINATO-KU
TOKYO, 105
JAPAN

D. O'CONNOR
OAK RIDGE NATIONAL LABORATORY

OAK RIDGE, TN 37831-8063
USA

J. OGATA
MITSUBISHI HEAVY INDUSTRIES, LTD.
2-4-1,SHIBAKOEN, MINATO-KU
TOKYO, 105
JAPAN

C. OLAND
OAK RIDGE NATIONAL LABORATORY
PO BOX 2009
OAK RIDGE, TN 37831-8056
USA

M. ORTIZ
IDAHO NATIONAL ENGINEERING LABS
P.O. BOX 1625
IDAHO FALLS, ID 83415-3895
USA

L. OTT
OAK RIDGE NATIONAL LABORATORY
BLDG. 9104-1, PO BOX 2009
OAK RIDGE, TN 37831-8057
USA

F. PAZDERA
NUCLEAR RESEARCH INSTITUTE REZ PLC
NUC. RES. INST./REZ NEAR PRAGUE

CZECH REPUBLIC

W. PERSONS
LAWRENCE LIVERMORE NAT'L LAB
PO BOX 808, L-632
LIVERMORE, CA 94550
USA

W. PRATT
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, PO BOX 5000
UPTON, NY 11973-5000
USA

J. PTACEK
IRI
P.O. BOX 2034
ROCKVILLE, MD 20847
USA

E. PURVIS
CONSULTANT
10105 CLEAR SPRING RD.
DAMASCUS, MD 20872
USA

K. REIL
SANDIA NATIONAL LABORATORIES
PO BOX 5800, DEPT. 6423
ALBUQUERQUE, NM 87185
USA

W. RETTIG
U.S. DEPARTMENT OF ENERGY
765 DOE PLACE
IDAHO FALLS, ID 83402
USA

M. RILEY
WESTINGHOUSE BETTIS
2895 O'NEILL DR.
BETHEL PARK, PA 15102
USA

Z. ROSZTOCZY
ZEETECH INC.
10131 WEATHERWOOD CT.
ROCKVILLE, MD 20854
USA

I. ORLOV
NSI RUSSIAN ACADEMY
B. TULSKAYA 52
MOSCOW,
RUSSIA

D. OSETEK
LOS ALAMOS TECHNICAL ASSOCIATES
2400 LOUISIANA NE, BLDG. 1, STE 400
ALBUQUERQUE, NM 87110
USA

J. PAPIN
INST. DE PROTECTION ET DE SURETE NUCLEAIRE
CEN CADARACHE DRS/SENAR
ST. PAUL LEZ DURANCE, 13108
FRANCE

B. PEARSON
ATOMIC ENERGY CONTROL BOARD
280 SLATER STREET
OTTAWA, K1P5S9
CANADA

R. PIKUL
MITRE CORP.
7525 COLSHIRE DR.
MC LEAN, VA 22102
USA

D. PRELEWICZ
SCIENTECH
11821 PARKLAWN DR.
ROCKVILLE, MD 20852
USA

J. PUGA
UNESA
FRANCISCO GERVAS 3
MADRID, 28020
SPAIN

F. QUINN
SCIENTECH
11821 PARKLAWN DR.
ROCKVILLE, MD 20852
USA

J. REMPE
EG&G IDAHO, INC.
PO BOX 1625, MS 3840
IDAHO FALLS, ID 83415
USA

P. REVEL
FRAMATOME USA, INC.
1925 N. LYNN ST., STE. 1100
ROSSLYN, VA 22209
USA

G. ROBINSON
PENN STATE UNIVERSITY

UNIVERSITY PARK, PA 16802
USA

J. ROYEN
OECD NUCLEAR ENERGY AGENCY
12 BOULEVARD DES ILES
ISSY-LES-MOULINEAUX, F-92130
FRANCE

N. ORTIZ
SANDIA NATIONAL LABORATORIES
PO BOX 5800
ALBUQUERQUE, NM 87185-5800
USA

V. OSTREJKOVSKY
OBNINSK INST. OF NUCLEAR POWER ENGINEERING
STUDENT CAMPUS
OBNINSK, KOIUGA 249020
RUSSIA

M. PARKS
SANDIA NATIONAL LABORATORIES
PO BOX 5800, DEPT. 6429
ALBUQERQUE, NM 87185
USA

W. PENNELL
OAK RIDGE NATIONAL LABORATORY
PO BOX 2009
OAK RIDGE, TN 37831-8056
USA

M. PILCH
SANDIA NATIONAL LABORATORIES
PO BOX 5800
ALBUQUERQUE, NM 87185
USA

V. PROKLOV
RUSSIAN RESEARCH CTR KURCHOTOV INST
ROGOVA STREET, 7, AP 32
MOSKOW,
RUSSIA

C. PUGH
OAK RIDGE NATIONAL LABORATORY
P.O. BOX 2009
OAK RIDGE, TN 37831
USA

M. QUINN
PACIFIC SCIENCE & ENG.
6310 GREENWICH DRIVE
SAN DIEGO, CA 92122
USA

M. REOCREUX
INST. DE PROTECTION ET DE SURETE NUCLEAIRE
CEN CADARACHE DRS/SENAR
ST. PAUL LEZ DURANCE, 13108
FRANCE

L. RIB
AECL TECHNOLOGIES
9210 CORPORATE BLVD.
ROCKVILLE, MD 20850
USA

U. ROHATGI
BROOKHAVEN NATIONAL LABORATORY
BLDG. 475B
UPTON, NY 11973
USA

G. RUDY
NUS
910 CLOPPER ROAD
GAITHERSBURG, MD 20878
USA

K. RUSSELL
EG&G IDAHO, INC.
P.O. BOX 1625
IDAHO FALLS, ID 83415-3895
USA

Y. SAITO
NUCLEAR POWER ENGINEERING CORP.
8F FUJITA KANKO TORANOMON BLDG.
MINATO-KU, 3-17-1
JAPAN

T. SAITO
UNIVERSITY OF TOKYO
7-3-1 HONGO, BUNKYO-KU
TOKYO, 113
JAPAN

P. SAMANTA
BROOKHAVEN NATIONAL LABORATORY
PO BOX 5000, BLDG. 130
UPTON, NY 11973-5000
USA

R. SANDERS
OAK RIDGE NATIONAL LABORATORY
P.O. BOX 2009, M.S. 8057
OAK RIDGE, TN 37831-8057
USA

G. SANTAROSSA
ENEA
S.P. 101 CRE CASACCIA
ROMA,
ITALY

G. SAPONARO
ENEA
VIA V. BRANCATI 48
ROMA, 00144
ITALY

C. SAVAGE
JUPITER CORP.
2730 UNIVERSITY BLVD. W
WHEATON, MD 20902
USA

P. SCHEINERT
WESTINGHOUSE BETTIS
2895 O'NEILL DR.
BETHEL PARK, PA 15102
USA

R. SCHMIDT
SANDIA NATIONAL LABORATORIES
PO BOX 5800, DEPT. 6423
ALBUQUERQUE, NM 87185
USA

R. SCHNEIDER
ABB-COMBUSTION ENGINEERING
1000 PROSPECT HILL RD.
WINDSOR, CT 06095
USA

G. SCHUECKTANZ
SIEMENS AG
PO BOX 32 20
ERLANGEN, 91058
GERMANY

F. SCIACCA
SCIENCE & ENGINEERING ASSOCIATES
1700 ROCKVILLE PIKE, ST. 400
ROCKVILLE, MD 20852
USA

B. SEHGAL
ROYAL INST. TECHNOLOGY, STOCKHOLM
DEPT. NUCLEAR POWER SAFETY
STOCKHOLM, 10044
SWEDEN

S. SETH
MITRE CORP.
7525 COLSHIRE DR.
MC LEAN, VA 22102
USA

W. SHA
ARGONNE NATIONAL LABORATORY
9700 S. CASS AVE.
ARGONNE, IL 60439
USA

W. SHACK
ARGONNE NATIONAL LABORATORY
BLDG. 212
ARGONNE, IL 60439
USA

V. SHAH
IDAHO NATIONAL ENGINEERING LABS
PO BOX 1625
IDAHO FALLS, ID 83415-3870
USA

H. SHIBATA
YOKOHAMA NATIONAL UNIVERSITY
156 TOKIWADAI, HODOGAYA-KU
YOKOHAMA,
JAPAN

Y. SHIRAHIGE
NUCLEAR POWER ENGINEERING CORP.
3-17-1,TORANOMON,MINATO-KU
TOKYO, 105
JAPAN

E. SILVER
OAK RIDGE NATIONAL LABORATORY
PO BOX 2009, MS8065
OAK RIDGE, TN 37831
USA

F. SIMONEN
PACIFIC NORTHWEST LABORATORY
P.O. BOX 999
RICHLAND, WA 99352
USA

B. SINGH
JUPITER CORP.
STE. 900, WHEATON PLAZA NO., 2730 UNIV. BLVD.
WHEATON, MD 20902
USA

G. SLAUGHTER
OAK RIDGE NATIONAL LABORATORY
PO BOX 2000
OAK RIDGE, TN 37831-6152
USA

I. SMITH
AEA TECHNOLOGY
LINFRITH TECHNOLOGY CENTRE
DORCHESTER, DORSET DT28DH
UK

L. SMITH
LOS ALAMOS NATIONAL LABORATORY
PO BOX 1663, MS E561
LOS ALAMOS, NM 87545
USA

V. SNELL
AECL TECHNOLOGIES
9210 CORPORATE BLVD.
ROCKVILLE, MD 20850
USA

M. SOKOLOV
OAK RIDGE NATIONAL LABORATORY
P.O. BOX 2008
OAK RIDGE, TN 37831
USA

C. SORRELL
VIRGINIA POWER
5000 DOMINION BLVD.
GLEN ALLEN, VA 23060
USA

B. SPENCER
ARGONNE NATIONAL LABORATORY
9700 S. CASS AVENUE
ARGONNE, IL 60439
USA

D. STARCK
MPR ASSOCIATES
320 KING ST.
ALEXANDRIA, VA 22314-3238
USA

N. STARFELT
SKI
ORNBOGATAN 41
BROMMA, 16199
SWEDEN

M. STRAND
SCIENTECH
11821 PARKLAWN DR.
ROCKVILLE, MD 20852
USA

V. STRIZHOV
NSI RUSSIAN ACADEMY
B. TULSKAYA
MOSCOW, 113191
RUSSIA

E. STUBBE
TRACTEBEL INGENIERIE
AVENUE ARIANE, 7 BTE 1
BRUXELLES, B-1200
BELGIUM

D. STURM
STAATL.MAT.PRUFUNGSANSTALT U. STUTTGART
PFAFFENWALDRING 32
STUTTGART, BW 70569
GERMANY

R. SUMMERS
SANDIA NATIONAL LABORATORIES
PO BOX 5800
ALBUQUERQUE, NM 87185-5800
USA

J. SUN
ARGONNE NATIONAL LABORATORY
9700 S. CASS AVE.
ARGONNE, IL 60439
USA

A. SUSLOV
RUSSIAN RESEARCH CTR KUROHOTOV INST.
KURCHATOV SQUARE, 8
MOSKOW,
RUSSIA

M. SUZUKI
JAPAN ATOMIC ENERGY RESEARCH INST.
SHIRAKATA
TOKAI-MURA, IK 319-11
JAPAN

H. SUZUKI
HITACHI LTD.
5-2-2,OMIKA-CHO
HITACHI, 319-12
JAPAN

T. TAIRA
NUCLEAR POWER ENGINEERING CORP.
4-3-13 TORANOMON, MINATO-KU
TOKYO, 105
JAPAN

K. TAKUMI
NUCLEAR POWER ENGINEERING CORP.
3-17-1,TORANOMON,MINATO-KU
TOKYO, 105
JAPAN

N. TANAKA
NUCLEAR POWER ENGINEERING CORP.
4-3-13 TORANOMON, MINATO-KU
TOKYO, 105
JAPAN

J. TAYLOR
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, PO BOX 5000
UPTON, NY 11973-5000
USA

B. TEDESCO
SCIENTECH
11821 PARKLAWN DR.
ROCKVILLE , MD 20852
USA

H. TEZEL
ATOMIC ENERGY CONTROL BOARD
280 SLATER STREET
OTTOWA, ONTARIO K1P5S9
CANADA

G. THOMAS
LAWRENCE LIVERMORE NATIONAL LAB
7000 EAST AVE
LIVERMORE, CA 94550
USA

S. THOMPSON
SANDIA NATIONAL LABORATORIES
PO BOX 5800
ALBUQUERQUE, NM 87185-5800
USA

H. THORNBURG
ABB ATOM
901 S. WARFIELD DR.
MT. AIRY, MD 21771
USA

J. TILLS
JACK TILLS & ASSOCIATES, INC.
PO BOX 549
SANDIA PARK, NM 87047
USA

A. TUTNOV
KURCHATOV INSTITUTE
123182 KURCHATOV SQ.
MOSCOW,
RUSSIA

M. TUTTLE
LAMONT-DOHERGY EARTH OBS.

PALISADES, NY 10965
USA

R. VALENTIN
ARGONNE NATIONAL LABORATORY
9700 S. CASS AVE., BLDG. 308
ARGONNE, IL 60439
USA

K. VALTONEN
FINNISH CENTRE FOR RAD. & NUCL.SAFETY
PO BOX 268
HELSINKI, SF-00101
FINLAND

A. VASILE
COMMISSARIAT A L'ENERGIE ATOMIQUE
C.E. CADARACHE DEC/SECA
ST. PAUL LEZ DURANCE, 13108
FRANCE

W. VESELY
SCIENCE APPLICATIONS INTERNATIONAL CORP.
655 METRO PLACE SOUTH
DUBLIN, OH 43017
USA

R. VIJAYKUMAR
ERI
6290 MONTROSE ROAD
ROCKVILLE, MD 20852
USA

R. VOGEL
RICHARD C. VOGEL CONSULTANT
3432 STONERIDGE CT.
CALABASAS, CA 91302
USA

W. VON RIESEMANN
SANDIA NATIONAL LABORATORIES
ORG. 6403
ALBUQUERQUE, NM 87185
USA

J. WALKER
AECL RESEARCH
CHALK RIVER LABORATORIES
CHALK RIVER, ONTARIO K0J1J0
CANADA

D. WALLACE
NIST
BLDG. 225, RM B266
GAITHERSBURG, MD 20899
USA

W. WANG
STONE & WEBSTER ENGINEERING
3 EXECUTIVE CAMPUS, PO BOX 5200
CHERRY HILL, NJ 08034
USA

J. WARE
IDAHO NATIONAL ENGINEERING LABS
PO BOX 1625
IDAHO FALLS, ID 83415-3750
USA

K. WASHINGTON
SANDIA NATIONAL LABORATORIES
PO BOX 5800, DEPT. 6429
ALBUQUERQUE, NM 87185
USA

J. WEISSMAN
ABACUS TECHNOLOGY CORP.
5454 WISCONSIN AVENUE, SUITE 1100
CHEVY CHASE, MD 20815
USA

F. WHITE
KNOLLS ATOMIC POWER LAB/MARTIN MARIETTA
P.O. BOX 1072
SCHENECTADY, NY 12301-1072
USA

B. WHITESEL
NUMARC
1776 I ST., NW, STE 300
WASHINGTON, DC 20006
USA

K. WHITT
SOUTHERN NUCLEAR
3117 RENFRO RD
VESTAVIA HILLS, AL 35216
USA

G. WILKOWSKI
BATTELLE-COLUMBUS
505 KING AVE.
COLUMBUS, OH 43201
USA

V. WILLEMS
GILBERT/COMMONWEALTH, INC.
PO BOX 1498
READING, PA 19603
USA

K. WINEGARDNER
PACIFIC NORTHWEST LABORATORY
PO BOX 999
RICHLAND, WA 99352
USA

S. WINGATE
NUS
910 CLOPPER ROAD
GAITHERSBURG, MD 20878
USA

J. WOLF
IDAHO NATIONAL ENGINEERING LABS
PO BOX 1915
IDAHO FALLS, ID 83404
USA

R. YOUNGBLOOD
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, PO BOX 5000
UPTON, NY 11973-5000
USA

R. WITT
UNIV. OF WISCONSIN-MADISON
147 ERB, 1500 JOHNSON DR.
MADISON, WI 53706
USA

A. WRIGHT
OAK RIDGE NATIONAL LABORATORY
PO BOX 2009
OAK RIDGE, TN 37831-8088
USA

P. ZMOLA
C&P ENGINEERING
5409 NEWINGTON RD.
BETHESDA, MD 20816
USA

L. WOLF
BATTELLE INGENIEURTECHNIK GMBH
AM ROMERHOF 35
FRANKFURT AM MAIN, 60486
GERMANY

H. YASUI
TOKYO ELECTRIC POWER COMPANY
1901 L. STREE, N.W., SUITE 720
WASHINGTON, DC 20036
USA

R. ZOGRAN
MPR ASSOCIATES
320 KING ST.
ALEXANDRIA, VA 22314-3238
USA

PROCEEDINGS OF THE
TWENTY-FIRST WATER REACTOR SAFETY INFORMATION MEETING
October 25-27, 1993

CONTENTS - VOLUME 1

Page

ABSTRACT iii
GENERAL INDEX v
REGISTERED ATTENDEES vii

PLENARY SESSION

Changing Emphasis at the NRC's Office of Nuclear Regulatory Research 1
Dr. Forrest J. Remick, Commissioner (NRC)

Strategy of Severe Accident Physical Modeling
in View of Recent Requirements to Safety Analysis 7
Prof. Leonid A. Bolshov, Director, Russian Academy of Sciences

ADVANCED REACTOR RESEARCH
Chairperson: R. Meyer

Transient Analysis of the PIUS Advanced Reactor Design
with the TRAC-PF1/MOD2 Code 17
B. Boyack et al. (LANL)

CANDU3 Transient Analysis Using AECL Codes 41
R. Shumway, J. Judd (INEL), D. Ebert (NRC)

Database and Modeling Assessments of the CANDU3, PIUS,
ALMR and MHTGR Designs 71
D. Carlson, R. Meyer (NRC)

ADVANCED CONTROL SYSTEM TECHNOLOGY
Chairperson: J. Kramer

Assessing Functional Diversity by Program Slicing 85
D. Wallace et al. (NIST)

Software Reliability Assessment 95
M. Barnes, P. Bradley, M. Brewer (AEA Technology)

Class 1E Software Verification and Validation: Past, Present and Future 121
W. Persons, J. Lawrence (LLNL)

CONTENTS - VOLUME 1 (Cont'd)

Page

Comparison of the Effect of Paper and Computerized Procedures on Operator Error Rate and Speed of Performance 141
S. Converse et al. (NCSU)

Validation of the Use of Network Modeling of Nuclear Operator Performance 149
M. Lawless, R. Laughery (MA&D, Inc.), J. Persensky (NRC)

ADVANCED INSTRUMENTATION & CONTROL HARDWARE
Chairperson: C. Antonescu

A Review of Potential Uses for Fiber Optic Sensors in Nuclear Power Plants 161
D. Holcomb (ORNL), C. Antonescu (NRC)

Engineering the Development of Optical Fiber Sensors for Adverse Environments 173
M. Hastings (Ohio St. U.)

On-Line Calibration Monitoring for Instrumentation Channels in Nuclear Power Plants 191
H. Hashemian, D. Mitchell (Analysis & Measurement Svcs. Corp.)

Issues Arising with the Application of Optical Fiber Transmission in Class 1E Systems in Nuclear Power Plants 207
K. Korsah (ORNL), C. Antonescu (NRC)

A Dynamic Fail-Safe Approach to the Design of Computer-Based Safety Systems 219
I. Smith (AEA Technology), M. Miller (Duke Power Co.)

HUMAN FACTORS RESEARCH
Chairperson: J. Persensky

An Examination of Human Factors in External Beam Radiation Therapy: Findings and Implications 229
K. Henriksen, R. Kay, R. Jones (CAE-Link Corp.),
D. Morisseau, J. Persensky (NRC)

Human Error in Remote Afterloading Brachytherapy 253
M. Quinn, J. Callan (PSE), I. Schoenfeld, D. Serig (NRC)

Human Factors Issues in Severe Accident Management: Training for Decision-Making under Stress 273
R. Mumaw, E. Roth (Westinghouse), I. Schoenfeld (NRC)

CONTENTS - VOLUME 1 (Cont'd)

Page

Organization and Management Activities in the Nuclear Power Industry 293
R. Evans, R. Whitesel (NUMARC)

Potential Human Factors Research Relating to Modern Technology in Nuclear Power Plants 301
J. Ketchel (EPRI), R. Fink (MPR Assoc.), L. Hanes, R. Williges, B. Williges (Consultants)

An Assessment of Human Factors Research Facilities and Capabilities for the U.S. NRC 309
V. Barnes (Compa Industries), S. Parsons (Parsons & Assocs.), R. Laughery (MA&D, Inc.), J. Wachtel, J. Persensky (NRC)

PROBABILISTIC RISK ASSESSMENT TOPICS
Chairperson: M. Drouin

Implications of an HRA Framework for Quantifying Human Acts of Commission and Dependency: Development of a Methodology for Conducting an Integrated HRA/PRA 313
M. Barriere, W. Luckas, W. Brown (BNL), S. Cooper (SAIC), J. Wreathall (John Wreathall & Co.), D. Bley (PLG)

Results and Insights of a Level-1 Internal Event PRA of a PWR during Mid-Loop Operations 327
T. Chu et al. (BNL), B. Holmes (AEA Tech.), R-F. Su et al. (MIT), D. Bley et al. (PLG)

IPE Data Base Structure and Insights 339
J. Lehner, R. Youngblood (BNL)

Individual Plant Examination Program Aspirations and Achievements 349
J. Flack (NRC)

Handbook of Methods for Risk-Based Analysis of Technical Specification Requirements 363
P. Samanta (BNL), W. Vesely (SAIC)

Overview of AEOD's Program for Trending Reactor Operational Events 375
P. Baranowsky et al. (NRC)

The Capabilities and Applications of the SAPHIRE 5.0 Safety Assessment Software 395
K. Russell, S. Wood, K. Kvarfordt (INEL)

CONTENTS - VOLUME 1 (Cont'd)

Page

THERMAL HYDRAULICS
Chairperson: D. Bessette

Experiments on a Scaled Loop 415
J. Doster, E. Giavedoni (NCSU)

Core to Surge-Line Energy Transport in a Severe Accident Scenario 427
M. diMarzo, K. Almenas, S. Gopalnarayanan (UMCP)

Assessment of the Potential for HPME During a Station Blackout in the Surry and Zion PWRs 445
D. Knudson, P. Bayless, C. Dobbe (INEL), F. Odar (NRC)

Peer Review of RELAP5/MOD3 Documentation 469
W. Craddick (ORNL)

Benchmark Analyses with RELAP5 for USNRC Simulators 477
J. Burtt, R. Martin (INEL), L. Bell (NRC)

Depressurization as an Accident Management Strategy to Minimize Direct Containment Heating 489
D. Brownson (INEL), F. Odar (NRC)

THERMAL HYDRAULIC RESEARCH FOR ADVANCED PASSIVE LWRs
Chairperson: L. Shotkin

NRC Confirmatory Safety System Testing in Support of AP600 Design Review 511
G. Rhee, D. Bessette, L. Shotkin (NRC)

NRC Confirmatory Testing Program for SBWR 521
J. Han, D. Bessette, L. Shotkin (NRC)

RELAP5/MOD3 Calculations for GIST Data 531
K. Jones, J. Determan, G. McCreery (INEL), J. Han (NRC)

RELAP5/MOD3 Code Coupling Model 549
R. Martin, G. Johnsen (INEL)

RAMONA-4B Development for SBWR Safety Studies 563
U. Rohatgi et al. (BNL)

Changing Emphasis at the NRC's
Office of Nuclear Regulatory Research

Presented at the
21st Water Reactor Safety
Information Meeting

By

Dr. Forrest J. Remick
Commissioner, U.S. Nuclear Regulatory Commission

October 25, 1993

Pooks Hill Marriott
Bethesda, Maryland

Introduction:

Thank you, Mr. Beckjord, and good morning, ladies and gentlemen. It is a pleasure to welcome you to the NRC's 21st Water Reactor Safety Information Meeting.

I am in the last year of my five-year term as Commissioner and I am very proud to be associated with the people working at the Nuclear Regulatory Commission, in particular, the Office of Research, their contractors, and our international colleagues.

As a Commissioner I have had the pleasure of traveling and lecturing in many parts of the world. As a matter of fact, last evening I returned from an extremely interesting visit to Taiwan and the People's Republic of Korea. One of the perks of being a Commissioner is having a driver take me to local lecture halls. My driver, who has no technical training, impressed me by sitting in on most of my lectures.

Recently, on my way to a meeting to give the same lecture I have given for four years, I told the driver to take me back to my office because I had a terrible headache. The driver said he'd heard the lecture so many times, he could give it. Naturally I was amazed that a person with no technical background could lecture on the effects of transition from bubbly churn flow to inverted annular flow on the spatial distribution of neutron scattering in the core. But he kept insisting. I was curious to see if he could do it, so I let my driver take my place.

Well, my driver did a superb job. Unfortunately after the lecture, a hand rose from the audience, and there followed a very complicated, long-winded technical question. My driver stared the gentleman straight in the eyes and replied, "That is a stupid question. It is so

stupid that I will have my driver answer it!" I went to the podium and answered the question. So, if anyone has a question after I finish, I'll have my driver answer it.

I would like to extend a warm welcome to our distinguished colleague from the Russian Federation, Professor Leonid Bolshov, Director, of the Russian Academy of Sciences, Institute of Nuclear Safety, and his delegation. During my visits to Russia I was warmly treated by our Russian colleagues. The visits have confirmed and enlarged my respect for the technical competence and accomplishments of our Russian colleagues. There is no doubt in my mind that we have mutual interests and a lot to learn from each others' experiences. The Commission is looking forward to a long and mutually rewarding association between the people of our two countries.

I would also like to take this opportunity to welcome our colleagues from Austria, Belgium, Canada, the Czech Republic, Finland, France, Germany, Italy, Japan, the Republic of Korea, Slovenia, Spain, Sweden, Switzerland, Taiwan, the United Kingdom, and from any other country that I may have missed. In the future I hope to see representatives from more countries attend this meeting, because reactor safety research activities transcend international boundaries.

Changing Emphasis:

One of the major objectives of the Office of Research is to ensure availability of sound technical information for timely decision making in support of the NRC's safety mission. The Office of Research is changing some of its emphasis to better meet the expected needs of the NRC's regulatory offices. Long-standing programs in support of operating reactors are nearing completion. These programs include plant aging and severe accident research for currently operating plants. You will hear these programs discussed during the next few days. This meeting will also address the new challenges faced by the NRC in its review of the advanced light water and non-light water reactors. As plant aging and severe accident research programs are nearing completion, our research activities are coming to focus on the emerging technologies, for example, digital instrumentation and control systems, both as replacement equipment for operating plants and as the technology of choice and necessity for the advanced reactors. I say "necessity", because analog equipment is becoming obsolete. Other examples include the use of new materials in operating plants, human factors considerations in the design and operation of the advanced plants, thermal-hydraulic characteristics of the advanced reactors, and new construction techniques.

By necessity, the NRC research programs have become oriented to operating reactor issues. The Office of Research has established new procedures and programs for defining, categorizing, and closing technical and safety issues. The Office recently updated the NRC's regulatory analysis handbook by including use of the Commission's Safety Goals Policy in making backfit decisions.

The Office of Research has developed innovative tools and techniques for conducting probabilistic risk and safety assessments. These tools and techniques are being integrated into the NRC's decision making process. Today, we use probabilistic tools to prioritize safety issues, focus our resources on the risk-dominant issues, and assist in rendering safety decisions.

Beginning with the development of the WASH 1400 safety study, the Office of Research has demonstrated that PRAs (or PSAs) are powerful tools for suggesting improvements to plant design and operational safety. Some plants, both here and abroad, are applying PSA technology in their day-to-day operations. That practice is expected to grow and find its way into every plant's maintenance programs. To date, significant numbers of plant-specific safety enhancements have resulted from individual plant examination programs (IPE and IPEEE). An important consequence of these PSA-based efforts is that seismically-induced events will become the dominant risk contributors, if internal-hazard risks are further reduced.

Incidentally, last week, while attending an IAEA sponsored symposium in Seoul, Korea on Advanced Nuclear Power Systems, I urged the attendees that, as a professional courtesy, when quoting code damage frequency numbers, they should clearly indicate whether such calculations include only internal initiating events, or also external initiating events (e.g., seismic), shutdown risks, sabotage, etc.

Both the Office of Research and the industry have expended significant resources applying PRAs in the development of seismic hazards curves. Unfortunately, differences between the NRC's and the industry's curve have not been entirely resolved to either party's complete satisfaction. Delays in resolving the differences appear to be detracting from the overall objective of conducting full-scope PRAs on seismically-induced events. In lieu of the full-scale PRA analyses, margins analyses are being performed. I hope that both the NRC staff and the industry will continue to try to resolve the differences between the Lawrence Livermore and EPRI seismic hazards curves as soon as possible, so that we may begin to apply those tools with consistency in our analyses.

The use of PRA techniques has shown that small breaks, loss of offsite power, and operational accidents are now dominant internal contributors to risks. In addition, PRAs have brought to our attention that events at low power and shutdown conditions can also make significant contributions to risk. Based on these evaluations, the staff is pursuing rulemaking initiatives to ensure that a plant is not significantly more vulnerable to accidents in one operating mode than in another.

The changing emphasis in research activities is also seen in the area of transient and accident analysis. Through nearly two decades of extensive effort, research results have answered the safety concerns about large-break loss-of-coolant accidents (LOCA). The Office of Research has developed detailed analytical tools to predict the outcome of large-break LOCAs with reasonable accuracy. In fact, the Office has developed what is probably

the most extensive confirmatory test program there is for validating our computer programs for calculating thermal-hydraulic characteristics of the passive light water reactor plants. The Office is also assessing what it will need to do to support the Office of Nuclear Reactor Regulation's review of other advanced and evolutionary nuclear power plant designs, such as the CANDU-3 and the advanced liquid metal reactor (ALMR).

Maintenance of Expertise:

As I stated in my introductory remarks, one of the missions of the Office of Research is to ensure availability of sound technical bases for timely decision making in support of the NRC's safety mission. That requires concerted effort to maintain the technical expertise relevant to the mission of the agency.

The need for sound technical bases for timely decision making is, of course, not unique to the NRC. During a recent American Nuclear Society conference on Engineering Excellence, utility officials agreed that the industry must achieve higher standards in engineering. As William Conway, Vice President - Nuclear for Arizona Public Service Company, stated, "The importance of engineering cannot be overestimated." "Excellence can't be achieved by maintaining the status quo. Once one goal is met, a new one must be set -- you need stretched goals."

Conway's concept of "stretched goals" is certainly applicable to the NRC. For example, as the NRC closes its existing programs on plant aging and severe accidents, it must consider the impacts on its safety mission. It must ensure that it has established programs which maintain the state-of-the-art technical capability the agency relies on in reaching sound and timely technical safety decisions. In other words, the agency must establish a viable and effective program for maintenance of technical capability.

One element of a viable and an effective maintenance program is the establishment of "stretched goals." "Stretched goals" provide challenging work for our technical experts, build upon their knowledge base, and encourage the development of state-of-the-art tools which enhance the NRC's ability to respond to future safety concerns.

Another element of a viable and an effective maintenance program is the maintenance of the technical infrastructure to which the agency allocated significant resources to establish. This issue has recently become particularly important because retirements, both at the NRC and at our contractors, resulted in some significant loss of corporate memory and technical expertise. But not just retirements call for a maintenance program. Once the agency declares victory and says that a technical issue has been resolved, an effective maintenance program ensures that the technical infrastructure important to the mission of the agency does not deteriorate. An effective maintenance program provides security for the people with unique expertise important to the agency's mission, it provides a mechanism for

transferring technical expertise from one generation to the next, and it inspires a commitment to resolve safety concerns as quickly as possible.

Toward this end, the Commission requested the Nuclear Safety Research Review Committee to assist the Office of Research in identifying and categorizing the major disciplines and resources required to maintain a critical mass of experts available to fulfill this agency's unique mission. The initial review will focus on the thermal-hydraulic needs of the agency. The final recommendation in the thermal-hydraulic area is scheduled to be submitted to the Commission for review and approval by the end of this calendar year. Following Commission approval, similar assessments will be made for other technical disciplines.

Conclusion:

These are only a few highlights of the changing emphasis and challenges facing the Office of Research.

Nuclear energy is truly an international technology. Many of the ongoing activities involve cooperative agreements on an international scale. I am very pleased by the active participation in this Water Reactor Safety Meeting by our international colleagues. Working together we can more effectively build upon the state of the art in reactor safety and contribute to the safe design and operation of nuclear power plants. These international cooperative ventures are pursued not only by government agencies but by the nuclear industry as well. We greatly value and appreciate the international cooperative efforts.

To the NRC personnel from the Office of Research, and to their contractors from the national laboratories, universities, and other private enterprises, I would like to take this opportunity to express the Commission's sincere appreciation and continued support. Your dedicated and expert contributions to nuclear safety, while not always highly visible, or the object of a lot of comment by the Commissioners, has not gone unnoticed and have not gone unappreciated.

I wish you a productive meeting. I hope that all of you who are not from the Washington D.C. area will have a pleasant visit and will find the time to tour our Nation's Capital.

Thank you very much for your kind attention.

Strategy of severe accident physical modeling in view of recent requirements to safety analysis

L.A. Bolshov
Nuclear Safety Institute
Russian Academy of Sciences

Nuclear power destiny in various states including Russia is not free from questions. Where there is plenty of non-expensive natural gas or coal in a country, the competition of nuclear power with other power sources is especially intense. Until we consider the economic efficiency or environmental impact of the normally operating plant, the estimate of the proponents favorite choice may be rather optimistic in many cases. As soon as safety aspects of nuclear power are concerned it is necessary to answer very significant questions about the dangers resulting from severe accidents.

TMI and, to a greater extent, Chernobyl, demonstrated the other aspect of the severe accident problem. We consider it as being evident that the risk of additional radiation induced cancer cases is negligible in comparison with the number of road or mine accident victims. Some of the post Chernobyl actions, such as many of the relocations of some people, were probably excessive. But sometimes we do not completely realize that the contaminated (maybe slightly) surface after the Chernobyl accident covers in Russia 47000 km2 with over 2 million population (over 5 million on the FSU territory). These large numbers once appeared then influence a life stream in a specific way. That is why in 1992 (far from being the most successful financial year) a tenth of the budget in Russia invested in major construction has been spent on the reduction of the Chernobyl accident consequences.

It serves no purpose to dwell upon the inadequate reaction of the population on the radiation problem. It is of little use to try to prove that the health consequences of the Chernobyl or some other radiation accident are substantially overestimated. Post TMI and post Chernobyl reality is quite a new one. In this reality severe NPP accidents with significant radiation release occur. Period.

To make an advance we must substantially reduce the severe accident risk. Besides that it is necessary to give a convincing proof that such a reduction has really been made.

The solution of the problem of designing nuclear power plants (NPPs) with an acceptable risk for both the environment and population is divided at the moment into two stages. The radical solution is related to designing inherently safe NPPs using reactors based on the physical principles of the passive internal self-safety that exclude any severe accident. Such NPP projects are the subject of the future. In the framework of the present conference it is quite natural to reject serious considerations of the reactors with lead, salt or such other coolants.

The next generation of nuclear plants with improved safety, which may form a basis of the nuclear power production in the nearest decades, starts mainly from the evolutionary development of the light water reactor technology. Work in this direction is aimed at the reduction of the probability of severe

accidents with core damage to the level 10-6 and less. Simultaneously an echelonized defense-in-depth system of safety barriers is created providing a guaranteed localization of the radioactivity inside the containment in all foreseen hypothetical accidents. Nowadays there is a quantitative reference point for such an approach: the probability of containment system failure must guarantee that the probability of the activity releases to the environment would be lower than the probability of the disastrous external events destroying the reactor installation (superstrong earthquake, large meteorite falldown, etc.). In this case it is possible to consider the probability of an accident with significant activity release, when population protecting measures are required, to be less than 10-10 per year.

This approach results in new requirements for the accuracy and certainty of the analysis of containment system reliability against core meltdown accidents. We wouldn't like to accept and advocate the mentioned figures as a final truth. However it is essential that these figures are significantly less than those used previously for safety analysis by conventional methods.

The main difficulties met in attempts to provide a new level of analytical certainty are related to specific features of severe accident descriptions. The sources of this specificity are well known.

First of all, in severe accident analysis the object under investigation is, a priori, not exactly defined, in contrast with the case of design basis accidents. Depending on the scenario, one or another combination of the geometrical, physical - chemical and mechanical factors produces one or another object of studies.

The second, equally significant reason, is that the sample of the required input data (mixture parameters, multi-component phase diagrams, reaction velocities, etc.) is far from being complete. Often the underlying phenomenon mechanism itself is not yet understood.

The third is the necessity to produce numerous calculations under conditions of multi-variant accident progression, even in the framework of one scenario class.

The fourth, and perhaps the most significant fact, is that the attempts to tune and fit the numerical models experimentally on the basis of more or less real tests are obviously awkward. In the case of design basis accidents we at least know all the constituent elements of the large system to be modeled, as well as their relations. We are able to obtain correlations starting from the basic equations and then checking the correctness of the large system description considering the completeness of the essential block set and the fit of the appropriate dimensionless parameters. For severe accidents the same principles are faced with several problems, e.g. choice of an adequate geometry and description (any correlation is valid only in some exactly defined region; leaving it is fraught with large errors), reasonable scaling and so on.

Nevertheless, during the last 10 to 15 years various numerical models were developed for the severe accident descriptions. They make use of voluminous collected information on models, small--scale experimental data and some large scale tests. There have been significant successes in this area.

Today I would like to focus your attention on the following question.

Is it possible to use the methodological experience of the modern physical modeling successfully applied in space, thermonuclear, laser technologies, for the improvement and further development of the severe accident analysis methods, having in mind the reduction in level of uncertainties and conservatism of the safety assessments?

We would like to communicate to you some experiences in this direction obtained by the Nuclear safety Institute of the Russian Academy of Sciences and Kurchatov Institute and to demonstrate several specific features on examples.

Considering mainly NPPs of the next generation, we understand that the developed methodology would be useful for making decisions about the operating NPPs, including difficult decisions about those with insufficient safety level coupled with the situation of a lack of resources for modernization or replacement.

CORE DEGRADATION

Modeling of the reactor core degradation processes requires that the following phenomena should be taken into account:

- convective and radiation heat exchange between construction elements and coolant;

- chemical interaction of the construction elements with each other and with the coolant:

  reactions UO2 - Zr - steam;
  eutectic interactions Steel - Zr, Zr - B4C, Steel - B4C, etc;

- cladding damage due to mechanical tension;

- eutectic formation;

- melt flowdown;

- secondary interaction with coolant, etc.

Let us consider just one of these processes UO2 - Zr - steam interaction. In the integral codes it is usually described by the parabolic relations, which are valid, strictly speaking, only for isothermal processes in semi-infinite media. Known approximations with better physical motivation (PEXLOX solution of the diffusion problem simultaneously with the Stefan problem) are rather cumbersome and are not used in the integral codes.

A model based on the solution of the oxygen diffusion equation system in the multi-layer structure (up to 7 layers - see Fig. 1) was developed at the Nuclear Safety Institute (NSI). Due to theoretical analysis the equations were substantially simplified and an effective method for their numerical solution

was developed, without any loss of accuracy, for the whole region of parameter variation. This model allows for the following physical phenomena:

- consistent description of the oxidation on the external cladding surface and UO2 - Zr interaction on the internal one;

- cladding oxidation on the internal side;

- chemical dissolution of the ZrO2 layer with lack of oxygen;

- structural phase transition "cubic tetragonal" of the solid ZrO2 for non-isothermal temperature regimes;

- U - Zr - O mixture oxidation during flowdown.

Constant maintenance of the model is based on the analysis of the wide class of the experiments by Hoffman, Olander, Degaltsev and others. Data of both isothermic and non-isothermic experiments were used. In the latter case the database included the dependence of the diffusion coefficients on the temperature growth velocity (see Fig. 2). From this figure one can see that the calculations based on more physically motivated model give better results as compared with the classic parabolic correlations method URBANIC. The difference in the oxidation layer thickness between calculation and experiment is a factor of two.

This model supplied by the diffusion coefficient and phase concentration database is realized as a module UZRO which may be used both as a stand alone unit or implemented into integral codes like ICARE2, ATHLET, SCDAP et al. In particular, according to IPSN request this module is already implemented into the intensively developing code ICARE2. It makes it possible to start module validation in integral tests.

PHEBUS B9+ experiment modeling gave results comparable with the standard ones. The reason is the comparatively low velocities of the clad heating. The results of CORA - WWER1 experiment modeling with ICARE2 code are shown in Fig. 3. The red curve shows results obtained by ICARE2 code using the NSI diffusion model (UZRO module), the green one is the experimental results. In order to achieve the total description of the degradation in the oxidation process it is necessary to complement the considered model by the description of mechanical behavior of cladding, melt flowdown, etc.

Mechanical behavior of the clad was modeled on the basis of the combined work with the oxidation model:

- oxidation influence on the cladding strain;

- back influence of the surface cracks on the oxidation;
- description of the clad degradation including "flowering";

- account for internal and external pressure;

- multilayered structure b - Zr, a - Zr and ZrO2 with different physical and mechanical properties.

Some phenomena in the process of the melt flowdown were also modeled:

- drop and stream flowdown regimes, transition regimes;
- account for capillary forces;
- flowdown in the gaps.

Some of the described models are also implemented into ICARE2 code.

Single fuel element quenching.

We are developing two complimentary approaches. First is a qualitative description of the problem. Fig. Q-1 is the phase portrait, which shows evolution of the oxidation front position and temperature for a fixed point of fuel element. The separatrix divides initial conditions in oxidation of Zirconium and cooling regimes with reflooding. Second is a model for much more accurate description. But Fig. Q-2 and Q-3 show the same qualitative features.

LOWER HEAD FAILURE

Key problems

In view of perspective average-power reactors of the next generation (AP-600, WWER-500, WPBER-600) being designed a real possibility appeared to take advantage of the protective properties of the reactor vessel more completely using external cooling. The set of problems to be solved in detail in the models is as follows:

Thermal/hydraulics in Corium taking into account phase conditions to find thermal loading at vessel.

Scenario of melt formation.

Energy distribution between channels of losses.

Local thermal loading.

Thermal behavior of vessel and its interaction with corium.

Possibility of Cooling: In-Vessel and Ex-Vessel.
Mechanical Response of vessel.

Timing of Process.

Uncertainty Studies.

Problem status

Up to now the problem of the melt in-vessel localization for large power reactors was not considered. Reactor material properties and their interactions were studied. An additional push in the investigation of the problem came from the concept of in-vessel confinement. As far as programs are concerned there are no complete models of the melt thermal-hydraulic behavior

though some efforts in this direction are made (works by Patankar, Schmit etc. concerning natural convection in melts). Among large-scale tests it is worth noting experiments with modeling fluids (predominantly water), including large-scale ones (COPO).

The necessity to develop a complex code is caused by the requirement of an accurate safety calculation, especially when in-vessel confinement concept is used and system behavior must be predicted accurately enough since mistake here lead to consequences which are irreversible in this case.

The model

The 2D thermal-hydraulic model is developed based on the usage of the effective algorithms for convective flow calculations at large Raleigh numbers, with possible variation of the boundary conditions. This model may be used for the convective flow analysis when convection arises due to internal heat production or due to wall temperature difference, including external cooling case. Effectiveness of algorithm allows us to make calculations on a PC.

Validation

Model validation was made on the experiments with large and small Raleigh numbers and for variants of heat exchange between hot and cold walls.

Fig. 1. Here validation calculations for convection in the region of small Raleigh numbers are shown. They correspond to laminar and transient flow regimes. For these regime a comparison is made with correlation results.

Fig. 2. The same calculations for turbulent convection with large Raleigh numbers. There is a good agreement with correlations and COPO experiment.

Fig. 3. Time dependencies of the Nusselt number and temperature for the initial non-stationary phase of convection. A tendency to the asymptotic correlation behavior is demonstrated. Here the Raleigh number is 1014.

Fig. 4. Distribution of temperature, flow functions and thermal load at the vessel for a Raleigh number 1012.

Fig. 5. Application of the same model to the solution of the convection problem in the reactor pit. The Raleigh number calculated from the temperature difference is 108.

The essential problem here is to correctly describe the heat transfer between the outer surface of the vessel and the water in the reactor pit. The next pictures show the specific model and code VESSCOOL designed for this purpose. Again validation of the model demands additional efforts.

Other models

Elastic plastic deformations of the vessel were analyzed using the results for melting obtained by other programs. Vessel degradation dynamics is presented for the case of the ideal external cooling. The residual vessel thickness is several centimeters at maximal flows estimated to reach 1 MW/m2. It is

possible to reach such a cooling rate only by using intensified heat exchange on the external surface. The figure illustrates a movement of the film boiling transition point to the high-temperature region analyzed with the use of VESSCOOL code.

The possibility of melt confinement depends also on the internal state of the reactor, in particular on pressure. Plastic deformation intensities for the same vessel melting rate at different initial in-vessel conditions are shown in the figure. The critical internal pressure value for the considered interaction scenario is 2 MPa.

MOLTEN CORE - CONCRETE INTERACTION

The MCCI problem has been studied for a long time using the combined efforts of various countries. There are many programs for MCCI modeling. A large number of large-scale experiments have been made. Validation is the main problem of MCCI modeling since experiments cannot reproduce the real reactor case completely. As a result it is impossible to make a direct extrapolation of the obtained results to the reactor case.

The differences are related with

- geometry (2D for the model and 3D for many experiments (SURC, ACE))

- modeling of the heat release in the melt (induction heating in SURC and BETA results in non-uniformity of the heat release)

- difference in construction materials (e.g. magnesium ceramics in SURC and tungsten wall in ACE)

- differences in the interaction scenario: in the reactor case large molten core mass enters the pit, in the experiment there is a typical stage of the preliminary heating which changes the structure and properties of the concrete.
I show you just a couple of pictures from the ACE program (already published). You see one and another section of temperature field at the start of interaction. Isotherms of water release and isotherm of concrete decomposition are far from being close to each other as it should be in reactor case and as it done in major codes.

Model

Thermal-hydraulics of melt in RASPLAV code allows modeling of thermal processes in complex geometries including:

- heat transfer to various heat components: ceramics, concrete, metals, etc;

- thermal chemistry of the melt;

- heat sources inhomogeneity;

- self-consistent crust models;

- one-, two-, three-dimensional interaction, etc.;

Use of this code on a PC is quite effective.

Validation.

Let us see how is it work in the case of Sandia SURC tests.

Fig. 1. General geometry of SURC-4 experiment including various materials (concrete, ceramics, metal layer, oxide layer etc.).

Fig. 2. Melting depth accounting for the non-uniformity of heat release in the melt.

Fig. 3. Temperature behavior of the metal melt from the start of the preliminary heating to the end of interaction. Zirconium addition allows one to describe thermal effects of the reactions in the condensed phase.

Fig. 4. Temperature profiles in ceramics which determine the side losses and energy balance in melts.

Accompanying phenomena

Model for melt spread on the concrete or other base. The results of the model, tested by the standard tests like dam destruction, are demonstrated.

CONCLUSIONS

Let us try to formulate the main features of the strategy of severe accident physical modeling which were demonstrated on specific examples. The sequence of actions in the description of different stages of severe accidents are mainly the same in all cases.

Extraction of the major phenomena and division the process into possibly simplest separable parts.

Choice and adaptation of the theoretical model among the available set or, in absence of an appropriate model, development of a new one.

Theoretical model upgrading to an effective code.

Code validation using all the available experiments, including those out of scope of the reactor technology (model refers to the phenomenon in the corresponding parameter region rather than to some specific device).

Arrangement of additional experiments aimed on the revealing of the required details or data collection.

Implementation of the improved code in the integral code.

Comparison with the integral tests.

Proposal of new integral tests basing on extensive physical modeling (theory plus experiment).

Analysis of the test results and improvement of the model, code, integral code.

Experience over the last seven years (only several fragments of this work were discussed) has led us to some conclusions which may be useful to others.

1. The modern level of development of computer techniques and numerical methods makes it possible, sometimes, to use equations based on first principles (rather than correlations), making effective multi-variant calculations practical even on a PC.

2. Transition to the level of physical modeling appears to be effective in some cases of designing and validation of individual codes using supporting experiments and integral tests.

3. Planning of the integral tests in the framework of physical modeling strategy may sometimes improve their efficiency.

4. In several cases physical modeling increased the predictive power of the qualitative analysis of the complex system behavior and reduced the ambiguity gap in the quantitative results.

All the aforementioned lead us to the idea that the strategy of physical modeling has a right to exist and develop alongside with more traditional approaches where vast successful experience is already collected. Moreover, we hope that this strategy may become a basis for designing the next generation of integral codes for severe accident analyses. The necessity to develop such a product is now recognized more and more.

TRANSIENT ANALYSIS OF THE PIUS ADVANCED REACTOR DESIGN WITH THE TRAC-PF1/MOD2 CODE*

B. E. Boyack, J. L. Steiner, S. C. Harmony, H. J. Stumpf, and J. F. Lime
Technology and Safety Assessment Division
Los Alamos National Laboratory
Los Alamos, New Mexico 87545
(505) 667-2609

ABSTRACT

The PIUS advanced reactor is a 640-MWe pressurized water reactor developed by Asea Brown Boveri. A unique feature of the PIUS concept is the absence of mechanical control and shutdown rods. Reactivity is normally controlled by coolant boron concentration and the temperature of the moderator coolant. As part of the preapplication and eventual design certification process, advanced reactor applicants are required to submit neutronic and thermal-hydraulic safety analyses over a sufficient range of normal operation, transient conditions, and specified accident sequences. Los Alamos is supporting the US Nuclear Regulatory Commission's preapplication review of the PIUS reactor. Several models of the PIUS reactor have been developed for the system neutronic and thermal-hydraulic analysis code TRAC-PF1/MOD2. Analyses of five types of events have been completed. These are (1) reactor scram, (2) loss of offsite power, (3) main steam line break, (4) small-break loss-of-coolant, and (5) large-break loss-of-coolant. In addition to baseline calculations, sensitivity studies were performed to explore the robustness of the PIUS concept to severe off-normal conditions. The sensitivity study results provide insights into the robustness of the design. The results of the Los Alamos analyses are summarized in this paper.

INTRODUCTION

The PIUS advanced reactor is a four-loop, Asea Brown Boveri (ABB) designed pressurized water reactor with a nominal core rating of 2000 MWt and 640 MWe (Ref. 1). A primary design objective was to eliminate any possibility of a core degradation accident. A schematic of the basic PIUS reactor arrangement is shown in Fig. 1. Reactivity is controlled by coolant boron concentration and temperature, and there are no mechanical control or shutdown rods. The core is submerged in a large pool of highly borated water, and the core is in continuous communication with the pool water through pipe openings called density locks. The density locks provide a continuously open flow path between the primary system and the reactor pool. The reactor coolant pumps (RCPs) are operated so that there is a hydraulic balance in the density locks between the primary coolant loop and the pool, keeping the pool water and primary coolant separated during normal operation. Hot primary-system water is stably stratified over cold pool water in the density locks. PIUS contains an active scram system. The active scram system consists of four valved lines, one for each primary coolant loop, connecting the reactor pool to the inlets of the RCPs. Although the active scram piping and valves are safety-class equipment, operation of the nonsafety-class RCPs is required for effective delivery of pool water to the primary system. PIUS also has a passive scram system that functions should one or more of the RCPs lose their motive power, thereby eliminating the balance between the primary coolant loop and the pool, and activating flow through the lower and upper density locks. Highly borated water

*This work was funded by the US Nuclear Regulatory Commission's Office of Nuclear Regulatory Research

from the pool enters the primary coolant via natural circulation, and this process produces a reactor shutdown. The reactor pool can be cooled by either an active, nonsafety-class system or a fully passive, safety-class system.

As part of the preapplication and eventual design certification process, advanced reactor applicants are required to submit neutronic and thermal-hydraulic safety analyses over a sufficient range of normal operation, transient conditions, and specified accident sequences. ABB submitted a Preliminary Safety Information Document (PSID, Ref. 2) to the US Nuclear Regulatory Commission (NRC) for preapplication safety review in 1990. Early in 1992, ABB submitted a Supplemental Information Package to the NRC to reflect recent design modifications (Ref. 3). The ABB safety analyses are based on results from the RIGEL code (Ref. 4), a one-dimensional (1D) thermal-hydraulic system analysis code developed at ABB Atom for PIUS reactor analysis. An important feature of the PIUS Supplement design was the addition of the previously described active scram system that will function for most transient and accident conditions. However, this system cannot meet all scram requirements because the performance of the active scram system depends on the operation of the RCPs. Thus, the passive scram system of the original PSID design was retained. Because the PIUS reactor does not have the usual rod-based shutdown systems of existing and planned light water reactors, the behavior of the PIUS reactor trip and shutdown phenomena following a passive system scram must be understood. Review and confirmation of the ABB safety analyses for the PIUS design constitute an important activity in the NRC's preapplication review. Los Alamos is supporting the NRC's preapplication review of the PIUS reactor. This paper summarizes the results of Transient Reactor Analysis Code (TRAC, Ref. 5) baseline calculations of the PIUS Supplement design for five types of events. These are (1) reactor scram , (2) loss of offsite power (LOSP), (3) main steam line break (MSLB), (4) small-break loss-of-coolant (SBLOCA), and (5) large break loss-of-coolant (LBLOCA). Sensitivity studies were performed to explore the robustness of the PIUS concept to severe off-normal conditions associated with these events. The sensitivity study results provide insights into the robustness of the design.

TRAC ADEQUACY FOR THE PIUS APPLICATION

The TRAC-PF1/MOD2 code (Ref. 5), version 5.3.05, was used for each calculation. The TRAC code series was developed at Los Alamos to provide advanced, best-estimate predictions for postulated accidents in pressurized water reactors. The code incorporates four-component (liquid water, water vapor, liquid solute, and noncondensible gas), two-fluid (liquid and gas), and nonequilibrium modeling of thermal-hydraulic behavior. TRAC features flow-regime dependent constitutive equations, component modularity, multidimensional fluid dynamics, generalized heat structure modeling, and a complete control systems modeling capability. The code also features a three-dimensional (3D) stability-enhancing two-step method, which removes the Courant time-step limit within the vessel solution. Many of the features just identified have proven useful in modeling the PIUS reactor.

It is important that the issue of code adequacy for the PIUS application be addressed. If TRAC analyses were supporting a design certification activity, a formal and structured code-adequacy demonstration would be desirable. One such approach would be to (1) identify representative PIUS transient and accidents sequences, (2) identify the key systems, components, processes and phenomena associated with the sequences, (3) conduct a bottom-up review of the individual TRAC models and correlations, and (4) conduct a top-down review of the total or integrated code performance relative to the needs assessed in steps 1 and 2. The bottom-up review determines the technical adequacy of each model by considering its pedigree, applicability, and fidelity to experimental separate effect or component data. The top-down review determines the technical adequacy of the integrated code by considering code applicability and fidelity to data taken in integral test facilities.

Because the NRC conducted a preapplication rather than a certification review, the NRC and Los Alamos concluded that a less extensive demonstration of code adequacy would suffice. Steps 1 and 2 were performed and documented in Ref. 6. A bottom-up review specific to the PIUS reactor was not conducted. However, the bottom-up review of TRAC conducted for another reactor type (Ref. 7) provided some confidence that many of the basic TRAC models and correlations are adequate, although some that needed code modifications were also identified. A complete top-down review was not conducted. However, the ability of TRAC to model key PIUS systems, components, processes and phenomena was demonstrated in an assessment activity (Ref. 8) using integral data from the ATLE facility (Ref. 4). ATLE is a 1/308 volume scale integral test facility that simulates the PIUS reactor. Key safety features and components were simulated in ATLE, including the upper and lower density locks, the reactor pool, pressurizer, core, riser, downcomer, reactor coolant pumps, and steam generators. Key processes were simulated in ATLE including natural circulation through the upper and lower density locks, boron transport into the core (simulated with sodium sulfate), and control of the density lock interface. Core kinetics were indirectly simulated through a point kinetics computer model that calculated and controlled the core power based upon the core solute concentration, coolant temperature, and heater rod temperature. The results of this assessment activity will be discussed at the appropriate point in this paper. The ability of TRAC to model key PIUS systems, components, processes and phenomena was further demonstrated by benchmarking TRAC to the RIGEL code (Ref. 4). The results of three benchmark comparisons will be discussed at appropriate points in this paper.

TRAC includes the capability for multidimensional modeling of the PIUS reactor. This multidimensional model has been used to calculate the baseline transients for the LBLOCA transient. These results are reported in this paper. However, for many transients, the fully 1D model appears to be sufficient. We have concluded that 1D has the potential for adequately representing many PIUS transients and accidents. We do note a reservation. The most important physical processes in PIUS are related to reactor shutdown because the PIUS reactor does not contain control and shutdown rods. Coupled core neutronic and thermal-hydraulic effects are possible, including multidimensional interactions arising from nonuniform introduction of boron across the core. ATLE does not simulate multidimensional effects. The RIGEL thermal-hydraulic model is 1D and a point kinetics model is used. Although both 1D and multidimensional TRAC thermal-hydraulic models have been used for PIUS analyses, core neutronics are simulated with a point kinetics model in each case. At the present time, it is not known whether coupled core neutronic and thermal-hydraulic effects and multidimensional effects are important. We offer this important reservation along with the results that follow.

TRAC MODEL OF THE PIUS REACTOR

Space does not permit detailed descriptions of the fully 1D and multidimensional PIUS input models for TRAC. Detailed descriptions of the TRAC models of the original PSID design are provided in Refs. 9 and 10, respectively. The TRAC-calculated and PSID Supplement steady-state values are tabulated below for comparison.

	TRAC	PSID Supplement
Core mass flow (kg/s)	12,822	12,880
Core bypass flow (kg/s)	320	200
Cold-leg temperature (K)	531	527.1
Hot-leg temperature (K)	560.7	557.3
Pressurizer pressure (MPa)	9.5	9.5
Steam exit pressure (MPa)	4.0	4.0

Steam exit temperature (K)	540.3	543
Steam flow superheat (°C)	16.5	20
Steam and feedwater mass flow (kg/s)	243	243

Additional initial and boundary conditions for the calculated transients are generally as follows, except where otherwise noted. The reactor is operating at beginning of cycle (BOC) with a primary loop boron concentration of 375 parts per million (ppm) and 100% power. The boron concentration in the reactor pool is initially 2200 ppm. If the active scram system is activated, the scram valves open over a period of 2 s following event initiation, remain open for 180 s, and close over a period of 20 s. The feedwater pumps are tripped at the time of reactor trip and the feedwater flow rate decreases linearly to zero in 20 s. The steam pressure on the steam generator secondary side is kept constant at 3.88 MPa (steam drum).

In the following sections, the results for five types of events are presented. Results are summarized for both the baseline transients and the sensitivity studies. The fully 1D model was used for each of the five event types. In addition, the 3D model was used for the baseline LBLOCA analysis. Only a brief description of the comprehensive results is possible in this summary paper. Additional details are provided in Refs. 9–13. When applicable, the results of TRAC assessment activities are presented using data from the ATLE facility and comparisons of TRAC and RIGEL-calculated results for the same transient.

REACTOR SCRAM EVENTS

The active scram system was incorporated in the PSID Supplement design with the intent that it will function for most anticipated and accident transients. The baseline active scram transient is initiated by opening valves in all four scram lines that connect the reactor pool to the RCP inlets in each of the four primary loops. Essentially all important phenomena arise from opening the scram valves and terminating feedwater flow to the steam generators. The total scram line flow, which varies between 700 and 800 kg/s, produces several effects. First, primary coolant is displaced and enters the reactor pool through the upper and lower density locks as shown in Fig. 2. Second, the highly borated water enters the primary and mixes with the coolant. The boron concentration increases rapidly while the scram valves are open, but the increase is terminated when the scram valves shut and the primary boron concentration stabilizes at about 860 ppm (Fig. 3). The increasing concentration of boron in the core inserts sufficient negative reactivity to reduce the core power decreases to decay heat levels (Fig. 4,). Following closure of the scram valves, neither pool water nor boron are entering the primary system. Forced flows through the upper and lower density locks are also terminated. Control of the thermal interface in the lower density lock is recovered and no subsequent flows through the density lock occur. There is no primary-to-secondary heat transfer in the steam generators after 115 s. Thus, the core decay heat is deposited in the primary coolant, and fuel and coolant temperatures begin a steady increase at 40 K/hr. Should no action be taken, the primary would continue to heat, the RCPs would increase speed until their overspeed limit of 115% was reached, and the density locks would activate to initiate natural circulation between the primary system and the reactor pool. The pool contains both active (non-safety grade) and passive (fully safety grade) pool cooling systems that reject core decay heat to the ultimate heat sink.

Sensitivity studies were performed to explore the robustness of the PIUS concept to severe off-normal conditions following active-system trips. The most severe of these conditions are very low probability events. Fractional and complete blockages of the lower density locks were analyzed. Given the minimal flows through the lower density lock for the baseline transient, even a total blockage produces only a minimal impact on the course of the transient. As a further assessment of the robustness of the PIUS concept, total blockages of both the upper and lower density locks were assumed. A shutdown in reactor power was again achieved. However, with both density locks blocked, the amount of pool water injected through the scram lines is reduced

compared with the baseline because primary inventory can only be displaced into the reactor pool through the small standpipes that connect the pressurizer steam space and the reactor pool. With the reduced scram-line flow, the primary boron concentration increased to only 480 ppm before the scram valves closed. For this transient, the core power decreases more slowly than in the baseline and the fuel and moderator temperatures remain higher. Later in the transient, the increasing moderator temperature results in the largest negative reactivity contribution to the total reactivity. Sensitivity calculations were performed to examine the effect of reduced pool boron concentration. Active scrams with pool boron concentrations of 1800 and 1000 ppm were examined. The first corresponds to the level at which a reactor scram is initiated on low pool boron concentration. The second corresponds to the condition at which a critical core can be achieved at cold shutdown conditions and BOC. For the 1800 ppm case, reactor power decreases at a slightly slower rate than the baseline, but the power levels are indistinguishable by 200 s. The active-system scram with the pool boron concentration at 1000 ppm also leads to a hot-shutdown condition, although the phenomena are markedly different. The reactor power decreases at a slower rate than in the baseline, not reaching the same level as the baseline until 400 s. Consequently, the extra decay heat deposited in the primary causes the primary system to heat and pressurize. The pressure relief system safety valves open several times while the scram valves are open and periodically after the scram valves are closed. Follow-on actions to fully terminate this event were not examined.

A RIGEL calculation of the active-system scram was reported in Ref. 3. Several results from the RIGEL calculations have been coplotted with the TRAC-calculated results for this transient. The RIGEL calculations were terminated at 300 s, while the TRAC calculations were terminated at 1200 s. The TRAC- and RIGEL-calculated core powers are shown in Fig. 4. The upper and lower density lock flows are compared in Fig. 2 and the primary loop boron concentrations are compared in Fig. 3. The TRAC- and RIGEL-calculated results are both qualitatively and quantitatively similar, and are, therefore, in reasonable agreement. Because the two code methods were independently developed, this reasonable agreement provides an added element of confidence that the major trends and processes associated with the active scram are correctly represented within the inherent capabilities of the 1D thermal-hydraulics and the point kinetics models.

LOSS OF OFFSITE POWER EVENTS

A LOSP transient demonstrates the passive scram function of the PIUS reactor. Following the loss of motive power to all RCPs, the pumps coast down and the loop flows decrease, reverse, and, by 300 s, stagnate. The hydraulic balance in the density locks between the primary coolant loop and the pool is upset when the RCPs are tripped. There is a rapid inflow of water into the primary system through the lower density lock and a corresponding but lower flow from the primary back to the reactor pool through the upper density lock (Fig. 5). The difference between the two flows replaces the volumetric shrinkage of the primary system coolant as fluid temperatures decrease. The lower density lock flow peaks at 1225 kg/s shortly after the LOSP initiation, and decreases until the natural circulation flow through the density locks required to remove core decay heat is established. The large influx of water passing from the reactor pool into the primary through the lower density lock, rapidly lowers the core inlet boron concentration and temperature to 2200 ppm and 323 K, respectively. The rapid decrease in fuel and coolant temperatures lead to positive reactivity insertions. However, the negative reactivity insertion by the boron is larger than the positive contributions, and the total reactivity is negative. The decline in reactor power to decay heat levels is more rapid than with the active scram.

Sensitivity studies were performed to explore the robustness of the PIUS concept to severe off-normal conditions following active-system trips. The most severe of these conditions are very low probability events. Calculations were performed to examine the effect of lower density lock blockage fractions of 75% and 100%. For the 75% blockage case, the peak lower density lock flow was decreased to 450 kg/s from baseline peak flow of 1225 kg/s. This has several

consequences. The rate at which boron is introduced into the core is delayed. The core inlet boron concentration and temperature stabilize at the reactor pool values about 100 s later than in the baseline. The core outlet temperature reaches the saturation temperature shortly after the start of the transient, and there is a brief period of voiding in the core. The voiding lasts only a few seconds and there is no core dryout. The decline in reactor power to decay heat levels is only slightly slower in the blockage case and no difference can be detected after 100 s. We next review the 100% or complete blockage of the lower density lock, a very challenging transient with regards to phenomena. The PIUS reactor successfully accommodates this transient. There are two distinct phases to this transient, the periods before and after upper density lock activation with the transition occurring at 375 s. During initial phase, the interface in the upper density lock is agitated but there is essentially no net flow to or from the pool to the primary. Core flows are reduced because the RCPs coast down and stop following the LOSP. The core outlet temperatures increase rapidly as the core flow decreases more rapidly than the core power, but the core inlet temperatures remain at near normal values until the steam generator secondaries dry out at 235 s. The primary pressure increases and the safety relief valves first open at 50 s and continue to cycle until 350 s. Voiding occurs in the core immediately following the LOSP initiator and continues throughout the transient. However, the core average voiding is less than 2% except for a brief period of voiding that reaches 6.5% shortly after the start of the transient. The core power (Fig. 6) remains above 200 MWt for the first 200 s. During this period, voiding and moderator temperature increases are the mechanisms that reduce core power. Following dryout of the steam generators at 235 s, the moderator temperature increases further and the core outlet saturates. The additional increase in moderator temperature is sufficient to reduce the core power to decay levels. The increasing primary system temperatures following dryout of the steam generators eventually leads to the second transient phase. The primary coolant inventory swells and the liquid level in the pressurizer rises above the top of the standpipes that connect the pressurizer steam space and the reactor pool. A small but steady flow is established through the standpipes from the primary system to the reactor pool. The upper density lock then activates to replenish the primary inventory (Fig. 7) and the primary boron concentration increases and inserts negative reactivity into the core. The increasing boron content in the primary ensures the eventual progression to decay heat levels.

Sensitivity calculations were also performed to examine the effect of reduced pool boron concentration. LOSP transients with pool boron concentrations of 1800 and 1000 ppm were examined. The differences between the calculated baseline and 1800 ppm pool concentration case are small. The phenomena of the LOSP transient with the pool boron concentration at 1000 ppm are markedly different than either the baseline or the 1800 ppm case. Although the lower and upper density lock flows are similar to those in the baseline, the core inlet boron concentration can only increase to the concentration of the boron in the pool or 1000 ppm. The negative reactivity inserted by the boron is sufficient to produce an initial reduction in core power but is insufficient to reduce the core power to decay levels. The core power oscillates once between 1000 and 250 MWt and then settles to a near constant value of 500 MWt after 200 s. Once the steam generators cease to function as heat sinks at 85 s, the primary pressure increases to the setpoint of the safety relief valves. These valves continue to cycle to the end of the calculated transient at 1200 s. Although a stable condition has been reached, the power level remains high at 500 MWt and this energy is carried to the reactor pool. The reactor pool is cooled by both a non-safety active system and a completely passive safety-grade system. However, to reach a stable hot-shutdown condition, additional boron must be inserted at some point into the primary system.

The TRAC code has been assessed using ATLE data from a LOSP simulation test. The experiment was initiated by tripping both recirculation pumps. As the pump speeds decreased, the pressure balance in the lower density lock was disturbed, and pool water entered the primary system from the pool. The primary flow decreased more rapidly than the power, causing a brief increase in the core outlet temperature. The core outlet temperature subsequently decreased as the solute entered the core, and the core power was decreased according to the power calculations of the facility point kinetics model. Key TRAC-calculated results of the assessment calculation are

presented in Figs. 8–10 and the results compared with the ATLE data and the results calculated with the RIGEL code. A comparison of the measured and code-calculated lower density lock flows is presented in Fig. 8. The TRAC-calculated peak lower density lock flow is about 25% less than measured. The TRAC-calculated natural circulation flow rate at the end of the test is about 12% less than measured. The RIGEL-calculated peak flow is within 2% of the measured value. The RIGEL-calculated natural circulation flow rate at the end of the test is about 30% greater than measured. The TRAC-calculated heater rod power is compared with the measured and RIGEL-calculated values in Fig. 9. The initial decrease in the TRAC-calculated power is delayed but then falls at a faster rate than measured. The under prediction of the early surge of flow through the lower density lock, and the corresponding reduced rate at which boron is introduced into the core, are consistent with the initial delay. The TRAC-calculated core outlet temperature is compared with the measured and RIGEL-calculated values in Fig. 10. The relative differences in core outlet temperatures are consistent with the density lock flow and core power discrepancies discussed previously. For this transient, TRAC correctly calculated the major processes and phenomena. However, the qualitative differences in initial and peak lower density lock flows and the related discrepancies in heater rod power and core outlet temperature are significant and are, therefore, of concern. We have been unable to identify the specific causes for the differences. We are investigating whether the introduction of artificial viscosity with the numerical scheme might be a factor in the underprediction of the early surge in flow.

MAIN STEAM LINE BREAK EVENTS

The initiating event for the baseline transient is a break at the outlet nozzle of the loop 3 steam generator. The primary system steady-state boron concentration is 30 ppm, which is characteristic of end-of-cycle operation. A reactor scram signal is rapidly generated by the decreasing secondary pressure. The active scram system injects pool water into the RCP inlets. The lower and upper density locks are activated only during the period the active scram system is operating. The feedwater pumps are tripped at the time of reactor trip, and feedwater flows are terminated in the normal manner. The loop-3 steam generator secondary rapidly depressurizes through the break, causing overcooling of the coolant passing through the primary side of the steam generator. The colder liquid from the overcooled steam generator mixes with the coolant streams from the other steam generators in the downcomer and forced circulation inlet plenum. The core inlet coolant temperature decreases, as shown in Fig. 11. The decreasing coolant temperature is a source of positive reactivity in the core. The active scram system is also initiated by the reactor scram signal. Highly borated water enters the primary through the scram lines. The increasing core boron concentration is a source of negative reactivity in the core. The total core reactivity, which is the sum of the positive moderator temperature and the negative boron contributions, first decreases with the boron, increases when the cold temperature surge reaches the core, and then continues to decrease as highly borated pool water continues to enter the primary through the scram lines (Fig. 12). The core power follows the same trend, first decreasing to 1300 MWt with the initial boron entering the core, increasing to 1550 MWt when the cold coolant enters the core, and finally decreasing to decay heat levels as highly borated water continues to enter the primary system through the scram lines. Other than the brief period of positive reactivity insertion resulting from the moderator temperature, the main features of the PIUS primary system transient behavior are quite similar to those following the active-system scram.

Sensitivity studies were performed to explore the robustness of the PIUS concept to severe off-normal conditions, combined with the MSLB initiator. One sensitivity calculation was performed for the baseline MSLB transient with a concurrent 75% blockage of the lower density lock. The results could not be distinguished from those of the baseline transient because the lower density lock is only activated during the operation of the active scram system in the baseline transient, and the lower density lock flows during that period are small. A second sensitivity calculation was performed for the baseline MSLB transient with a concurrent pool boron concentration at 1800 ppm. Although there were slight differences in the course of the calculated

transients, the differences were not significant. The reduction of the core power to decay levels was slightly delayed by the lower concentration boron entering the primary from the pool. After the scram valves were closed, the primary boron concentration stabilized at 500 ppm compared with 600 ppm in the baseline. This led to slightly elevated coolant temperatures throughout the transient. A third sensitivity calculation was performed for the baseline MSLB transient but with a concurrent failure of the active scram system. The phenomena occurring in this event sequence were markedly different from the baseline. In the baseline MSLB transient, the positive reactivity insertion from the overcooling of primary water in the steam generator experiencing the break was offset, to a large extent, by the negative reactivity of the boron entering the primary through the scram lines. With the assumed failure of the active scram system, the positive reactivity insertion from the overcooled primary water caused the core power to increase to 2550 MWt (Fig. 13). The primary system heated up and the pressure increased to the setpoints of the safety relief valves. These valves continued to cycle for the duration of the calculated transient. Associated with the heatup of the primary coolant (moderator) was the insertion of negative reactivity, and this was the means by which the power increase was terminated and the power decreased. The primary system coolant heatup was gradual and the RCP were able to maintain control of the lower density lock interface by increasing speed until the 115% overspeed limit was reached at 520 s. Within 60 s, the lower density lock activated and a natural circulation loop was established between the reactor pool and the primary (Fig. 14). The primary system boron concentration began to steadily increase and was at 160 ppm by the end of the calculated transient. This transient clearly illustrates the inherent operation of the density locks in the PIUS reactor once the thermal interface in the lower density lock can no longer be maintained. The density locks were activated, and the reactor pool to primary natural circulation loop was established, even though the RCPs continued to operate throughout the calculated transient.

SMALL-BREAK LOSS-OF-COOLANT EVENTS

The initiating event for the baseline transient is a break in the pressure relief system piping at the flange just outside the steel pressure vessel and upstream of the safety relief valves. Steam flows through the break at a peak rate of 105 kg/s and then decreases in concert with the primary pressure until a two-phase flow through the break begins at 230 s. A scram is initiated at 18 s when the primary system depressurizes to 8.5 MPa. Injection of highly borated water into the primary system through the scram lines causes a rapid decrease in the core power to decay levels. During the interval the scram valves are open, inventory is displaced from the primary system, through the upper and lower density locks, and into the reactor pool (Fig. 15). While the scram valves are open, the RCP inlets are full of liquid. However, closure of the scram valves induces a marked change in primary system behavior. Immediately following termination of the scram line flow, voiding occurs in the pump inlets, the RCPs increase to their overspeed limit of 115 % of nominal, and, subsequently, the RCP discharges become oscillatory. The oscillatory behavior of the RCP discharges propagates throughout the primary system. For example, the density lock flows oscillate, as shown in Fig. 15. However, a net circulation pattern is established with pool water entering the primary system through the lower density lock and exiting the primary system through the upper density lock. The net inflow through the lower density lock produces a continuing, albeit oscillatory, increase in the primary boron concentration. Coolant temperatures decrease, for the most part, throughout the transient (Fig. 16). However, the core inlet temperature increases following closure of the scram lines and the core outlet periodically saturates as the core flow oscillates in concert with the RCP discharges.

We completed several sensitivity studies. The first study examined the response of the PIUS reactor to the baseline SBLOCA initiator concurrent with a 75% blockage of the lower density lock. The baseline and 75% blockage results were similar in all major trends and average quantities. There was, however, an important phenomenological difference between the two calculations. The baseline calculation displayed a strong oscillatory character when the RCP inlets voided following termination of the scram line flows. The blockage case was markedly different.

Oscillations during the few intervals of existence were much smaller and decayed with time. We hypothesize that partial blockage of the lower density lock "stiffened" the coupled primary-pool system with the result that pump-induced oscillations did not grow to detectable levels and, when they did become detectable, were damped. The second sensitivity study examined the response of the PIUS reactor to the baseline SBLOCA initiator concurrent with a reactor pool boron concentration of 1800 ppm. The lowered pool boron concentration was of no consequence; the only impact was to slightly lengthen the time to reduce primary system temperatures to a same level as occurred in the baseline. Oscillatory behavior occurred in this sensitivity calculation. The third sensitivity study examined the response of the PIUS reactor to the baseline SBLOCA concurrent with a failure of the active scram system. Similar end states were reached for the two calculations by 1200 s when the transient calculations were terminated. The course of the sensitivity study transient differed, however, in several respects. Lacking the rapid injection of boron from the active scram system, core power decreased more slowly than in the baseline. The initial decline in core power was due to the negative reactivity insertions from increasing moderator temperatures and voiding in contrast to the baseline where the only source of negative reactivity insertion was from boron entering the core. Oscillatory behavior occurred in this sensitivity calculation.

A RIGEL calculation of a SBLOCA in the pressure relief system piping was reported in Ref. 3. The RIGEL calculations were terminated at 300 s while the TRAC calculations were terminated at 1200 s. The TRAC and RIGEL results are generally in qualitative agreement until 230 s when the scram valves close. There are moderate differences in the parameter values but the same trends are predicted by the two codes. There are important phenomenological differences between the two calculations after 230 s. However, we believe that these differences arise from the timing at which events occur, and, when considered in the perspective of extended transient times (e.g., 1200 s), are not significant. The TRAC-calculated results show the RCP controller demands an increase in speed at 210 s, about 10 s after the scram valves begin to close. The 115% RCP overspeed limit is reached by 260 s. The flow oscillations predicted by TRAC arise approximately 40 s after the RCPs have reached their overspeed limit and are caused by voiding in the inlets to the RCPS subsequent to closure of the scram valves. The RIGEL-calculated results show that the RCP controller demands an increase in speed at 255 s and the 115% overspeed limit is reached shortly before 300 s. We would expect that oscillatory RCP flows would be predicted by RIGEL at times greater than 300 s. We note that a RIGEL calculation was performed for a break in the same location for the original PSID design and the outcome documented in Ref. 2. During that transient, the RCP outlet flows were oscillatory after voiding arose in the inlets to the operating RCPs and after the RCP overspeed limit was reached.

LARGE-BREAK LOSS-OF-COOLANT EVENTS

The first baseline LBLOCA calculation was performed with the fully 1D input model. The initiating event for the baseline transient is a double-ended guillotine break in one cold leg just outside the steel pressure vessel (loop 3 of the TRAC model). The break flows from the vessel side and the RCP side of the break are shown in Fig. 17. Immediately after the start of the LBLOCA, flows in both the core and downcomer reverse. The lower density lock activates, but the density lock flow joins with the reversed core flow and passes upward through the downcomer to the vessel side of the break. The flow reversal lasts to approximately 6.5 s, and during this period a large fraction of the core reaches saturation temperatures (Fig. 18) and voids. This period of core voiding is terminated when the downcomer and core flows reverse and coolant once again enters the core. The reversal occurs when flows from the intact cold legs entering the cold-leg plenum and flowing to the break can fully supply the rapidly decreasing vessel-side break flow. Prior to that time, vessel inventory was needed, in addition to the flows from the intact loops, to supply the break flow. The core power rapidly decreases immediately following the LBLOCA initiator, experiences a sharp rise of 2 s duration beginning at 15 s, and remains at decay levels throughout the remainder of the calculated transient. The point kinetics model may not be adequate for predicting this criticality event. Voiding in the core is the single largest negative reactivity

insertion early in the transient. The active scram system is activated shortly after the LBLOCA initiating event. However, the active scram system is only effective for the first 11 s of the transient, after which the reactor pool drops below the level of the scram-line takeoff from the pool. A second core flow reversal begins at approximately 20 s and continues until 30 s. Prior to this time, the inlets of the RCPs begin to void, and RCP performance degrades. With the sharp decrease in pumped flow, saturation temperatures are reached in much of the core (Fig. 18), and the resultant void generation causes the core flow to reverse. The core then refills with water from the reactor pool that enters the primary through the lower density lock. However, this flow is not sufficient to prevent core coolant temperatures in the upper part of the core from reaching saturation, and final, and smallest, core voiding episode occurs. The core voiding causes the final large core flow reversal, which begins at 42 s and ends at about 55 s. Subsequent flow reversals are not sufficiently large to cause saturation temperatures to be reached in the core. Neither core dryout nor cladding temperature heatup excursions are calculated during the transient. The maximum cladding temperature is about 605 K. The minimum collapsed liquid level within the internal flow structure containing the core, riser and pressurizer occurs at 55 s (Fig. 19). This level is well above the top of the core. The liquid level is generally increasing thereafter.

The second baseline LBLOCA calculation was performed with the 3D input model. In major phenomena and trends, the 1D and 3D calculations were similar, although there were some differences in detail. There were no differences that could be specifically attributed to the multidimensional model. We do note, however, that since TRAC currently has only a point kinetics model, potential couplings between multidimensional core kinetics and multidimensional core flows could not be examined in the calculation. The calculated peak break flows for the 1D and 3D baseline transients were similar. The core power exhibited an early decrease to decay heat levels followed by a subsequent power increase to about 450 MWt at about 20 s. The predicted core power increase is much less than in the 1D baseline calculation and occurred about 5 s later. The initial core flow reversal lasted about 5 s and was terminated when the vessel-side break flow could be supplied by the coolant flows through the intact loops. The subsequent positive core flow was terminated when the inlets of the RCPs voided and pump performance degraded. These phenomena were the same as those in the 1D baseline. The following differences were noted. The second core flow reversal caused an extended period of core voiding that lasted until about 40 s. There were no subsequent periods of core voiding as were calculated in the 1D baseline calculation. The core inlet flow rate displayed smaller oscillations than in the 1D baseline. The peak cladding temperature was approximately 590 K, about 10 K lower than in the 1D baseline.

We completed several sensitivity studies. The first study examined the response of the PIUS reactor to the baseline LBLOCA initiator concurrent with a 75% blockage of the lower density lock. The phenomena occurring during this low probability transient were similar to the baseline. The same core flow reversal pattern occurred and for the same reasons presented in the baseline discussion. However, during the periods of positive core flow, the flow rates through the core were smaller because the flow entering the primary through the lower density lock was reduced by the lower density lock flow blockage. The amount of boron entering the core through the lower density lock was reduced. The amount of voiding in the core was larger during the second and third core flow reversal periods. Thus, void contributed more to the total negative core reactivity and boron contributed less during the calculated transient. After the initial decrease in core power immediately following the LBLOCA initiator, a power increase was again calculated. The power increase was to about 1100 MWt, less than in the baseline. The peak cladding temperature during the transient was 600 K. Neither cladding dryout nor cladding heatup were predicted. The second sensitivity study examined the response of the PIUS reactor to the baseline LBLOCA initiator concurrent with a reactor pool boron concentration of 1800 ppm. The course of this transient was nearly identical to the baseline with one exception. The core power increase beginning at about 15 s is more severe than in the baseline because there is less negative reactivity inserted into the core from the pool at 1800 ppm. There is, however, no core dryout or heatup. The peak cladding temperature is again about 600 K. The third sensitivity study examined the

response of the PIUS reactor to the baseline LBLOCA concurrent with a failure of the active scram system. As discussed for the baseline transient, the active scram system is only effective for the first 11 s of the transient, after which the reactor pool drops below the level of the scram-line takeoff from the pool. Because the core flow is reversed for the first 6.5 s of the transient, the active scram system has limited impact on the course of the baseline transient. Thus, the course of the transient for the sensitivity calculation was nearly identical to the baseline calculation.

A RIGEL calculation of a LBLOCA in a double-ended guillotine break in one cold leg just outside the steel pressure vessel was reported in Refs. 14 and 15. In general, the TRAC- and RIGEL-calculated results display the same phenomena and trends. There are, however, differences in the details. The calculated break flows are compared in Fig. 17. The RCP-side break flows are similar. The RIGEL-calculated peak vessel-side break flow is about 23,000 kg/s while the TRAC-calculated maximum flow is 17,800 kg/s. This result suggests that there may be differences between the RIGEL and TRAC critical flow models. An immediate reversal of the downcomer and core flows and the complete bypass of the lower density lock flow are predicted by both codes. However, the magnitude of the RIGEL-calculated peak reversed core flow is greater than the TRAC-calculated peak flow, the flows are approximately 10,000 and 3,700 kg/s, respectively. This result is consistent with the peak vessel-side break flow calculated by RIGEL, which was approximately 5,200 kg/s larger than that calculated by TRAC. The RIGEL-calculated core flow reversal lasts until nearly 10 s, while the TRAC-calculated flow reversal ends shortly after 6 s. Because the flow reversal predicted by RIGEL lasts longer, the period of voiding in the core is also extended. Consequently, RIGEL calculates a dryout and heatup of the hot rod in the model. TRAC, with its shorter interval of core voiding, does not predict a core heatup. The later termination of the reversal in the RIGEL calculation is consistent with the reason for the termination of the core flow reversal, that the break flow has decreased to the point that the break can be supplied by the intact loop cold-leg flows. This occurs in the RIGEL calculation about 9 s after the LBLOCA initiation. Thus, the magnitude of the vessel-side break markedly affects the early details of the predicted LBLOCA transients. We conclude with the observation that both TRAC and RIGEL predicted the same major phenomena and processes, and both predict that the reactor reaches shutdown conditions without damage. There are important differences in details, particularly with respect to the magnitude of the vessel-side break flow. These early differences influence the predicted courses of the LBLOCA transient. Comparison of the RIGEL and TRAC critical flow models is recommended.

SUMMARY OBSERVATIONS

1. Reactor shutdown to decay heat levels is predicted for each of the five transient types. The active scram system effectively reduces core power to decay levels for reactor scram, MSLB, and SBLOCA events. The passive scram system effectively reduces core power to decay levels for transients in which the scram system is either unavailable (e.g., LOSP events) or inoperable (e.g., LBLOCA event after the pool water level declines below the scram line takeoff point).

2. The PIUS core, as presently designed, is characterized by compensating reactor shutdown mechanisms. When highly borated pool water enters the primary through either the scram lines or the lower density locks under baseline conditions, the negative reactivity associated with the boron is the primary mechanism for decreasing core power to decay heat levels. The moderator and fuel temperature contributions reactivity are positive in such circumstances. However, negative reactivities are inserted via the moderator temperature and the void when either the boron entering the core is not sufficient to prevent fuel and coolant temperature increases (e.g., blockage or dilution situations) or the accident is sufficiently severe to cause voiding and delay introduction of boron into the core (e.g., the LBLOCA).

3. The PIUS concept, as presently conceived, has multiple flow paths between the primary system and reactor pool. Following a LOSP initiator, for example, a natural circulation path would be established with reactor pool water entering the primary system through the lower density lock and reentering the pool through the upper density lock. However, alternate flow paths exist should even complete blockage of one or other of the density locks occur. Lower density lock blockage fractions as high as 75% are accommodated for low probability accident initiators such as the SBLOCA and LBLOCA. Neither operator nor active-system actions are needed to accomplish reactor shutdown, even for a spectrum of transient and accident initiators combined with very low probability flow path blockage occurrences.

4. Our confidence in the baseline simulations is enhanced by the assessment activity performed using ATLE data. The ATLE processes and phenomena were correctly predicted by TRAC. However, there are quantitative discrepancies between key TRAC-calculated parameter values and the ATLE data and we would like to better understand the reasons for these differences. More effort is required to identify whether the reasons for the discrepancies lie in our knowledge of the facility, modeling decisions made in preparing the TRAC input model of ATLE, or deficiencies in the TRAC models and correlations.

5. Our confidence in the predicted outcomes of the baseline simulations is enhanced by the code benchmark comparisons that were performed for the active-system scram, the SBLOCA, and the LBLOCA. The RIGEL and TRAC-calculated results display many areas of similarity and agreement. However, there are also differences in the details of the transients and accidents calculated by the two codes, and we would like to better understand the reasons for these differences. It is desirable that the reasons for these differences be explored if the PIUS reactor progresses to the design certification stage. Although it is desirable to understand the reasons for the differences, we have concluded that they affect the detailed course of the predicted sequences rather than the predicted end states of the transient and accident sequences.

6. Although the sensitivity calculations move beyond both the assessment activity using ATLE data and the code-to-code benchmark activity with RIGEL, the PIUS design appears to accommodate marked departures from the baseline transient and accident conditions, including very low probability combination events. The studies of extremely low pool boron concentrations and complete blockages of the lower density lock are characteristic of very low probability events, yet these events appear to be successfully accommodated. No phenomenological "cliffs" were encountered for the sensitivity studies conducted.

7. At the present time, it is not known whether coupled multidimensional core neutronic and thermal-hydraulic effects are important. We believe that it will be important to investigate such effects should the PIUS reactor progress to the design certification stage.

REFERENCES

1. T. J. Pederson, "PIUS-A New Generation of Power Plants," Second ASME/JSME International Conference on Nuclear Engineering, San Francisco, California (March 21-24, 1993).
2. ABB Atom, "PIUS Preliminary Safety Information Document," (December 1989).
3. C. B. Brinkman, "PIUS PSID Supplemental Material," ABB Combustion Engineering Power document LD-93-020, Enclosure I (February 12, 1993).

4. D. Babala, U. Bredolt, and J. Kemppainen, "A Study of the Dynamics of the SECURE Reactors: Comparison of Experiments and Computations," *Nuclear Engineering and Design* **122**, 387-399 (1990).

5. "TRAC-PF1/MOD2 Code Manual - Theory Manual," Los Alamos National Laboratory document LA-12031-M, NUREG/CR-5673, Vol. 1 (to be issued).

6. B. E. Boyack, "Assessment of the PIUS Physics and Thermal-Hydraulic Experimental Data Bases," Los Alamos National Laboratory document LA-UR-93-3564 (1993).

7. B. E. Boyack and J. S. Elson, "Assessment of TRAC-PF1/MOD3 Code Adequacy for NP-HWR Thermal-Hydraulic Analyses," Los Alamos National Laboratory New Production Reactor document LA-NPR-TN-010 (September 15, 1992).

8. H. J. Stumpf, "TRAC Calculations of a Pump-Trip Scram and Partial Loss of Heat Sink for the ATLE Test Facility," Los Alamos National Laboratory document (to be published).

9. B. E. Boyack, J. L. Steiner, S. C. Harmony, H. J. Stumpf, and J. F. Lime, "Reactor Scram Events for the Updated PIUS 600 Advanced Reactor Design," Los Alamos National Laboratory document (to be published).

10. B. E. Boyack, J. L. Steiner, S. C. Harmony, H. J. Stumpf, and J. F. Lime, "Loss of Offsite Power Events in the Updated PIUS 600 Advanced Reactor Design," Los Alamos National Laboratory document (to be published).

11. S. C. Harmony, J. L. Steiner, H. J. Stumpf, J. F. Lime, and B. E. Boyack, "Loss of Offsite Power Events in the Updated PIUS 600 Advanced Reactor Design," Los Alamos National Laboratory document (to be published).

12. B. E. Boyack, J. L. Steiner, S. C. Harmony, H. J. Stumpf, and J. F. Lime, "Small Break Loss-of-Coolant Accidents in the Updated PIUS 600 Advanced Reactor Design," Los Alamos National Laboratory document (to be published).

13. J. L. Steiner, S. C. Harmony, H. J. Stumpf, J. F. Lime, and B. E. Boyack, "Large Break Loss-of-Coolant Accidents in the Updated PIUS 600 Advanced Reactor Design," Los Alamos National Laboratory document (to be published).

14. H. Zhao and U. Bredolt, "A Cold Leg LOCA in PIUS," *Transactions of the American Nuclear Society* **68**, Part A, pp. 288-89 (1993).

15. H. Zhao and U. Bredolt, " A Cold Leg LOCA in PIUS," Asea Brown Boveri Atom document (undated).

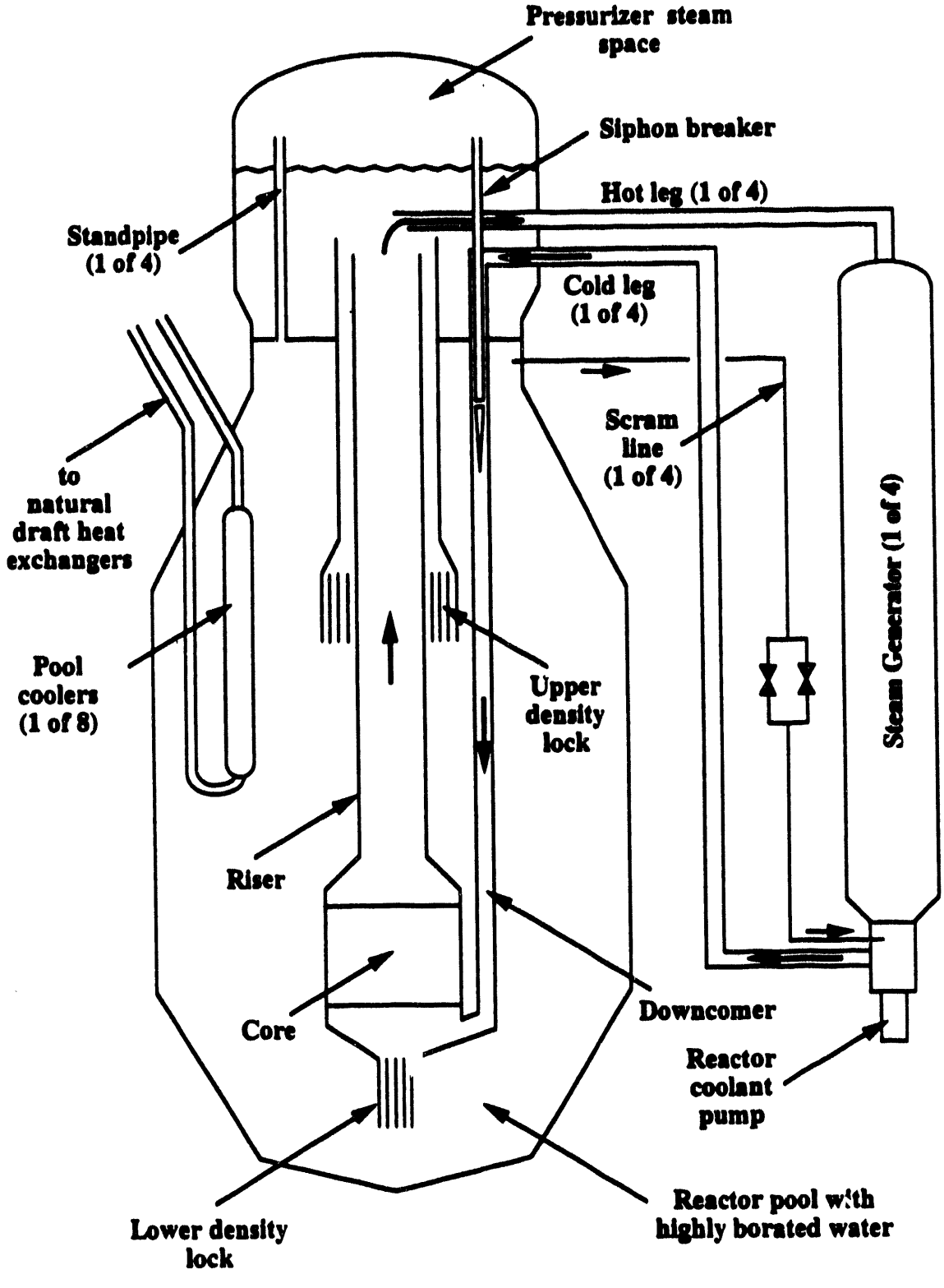


Fig. 1.
Schematic of the PIUS reactor.

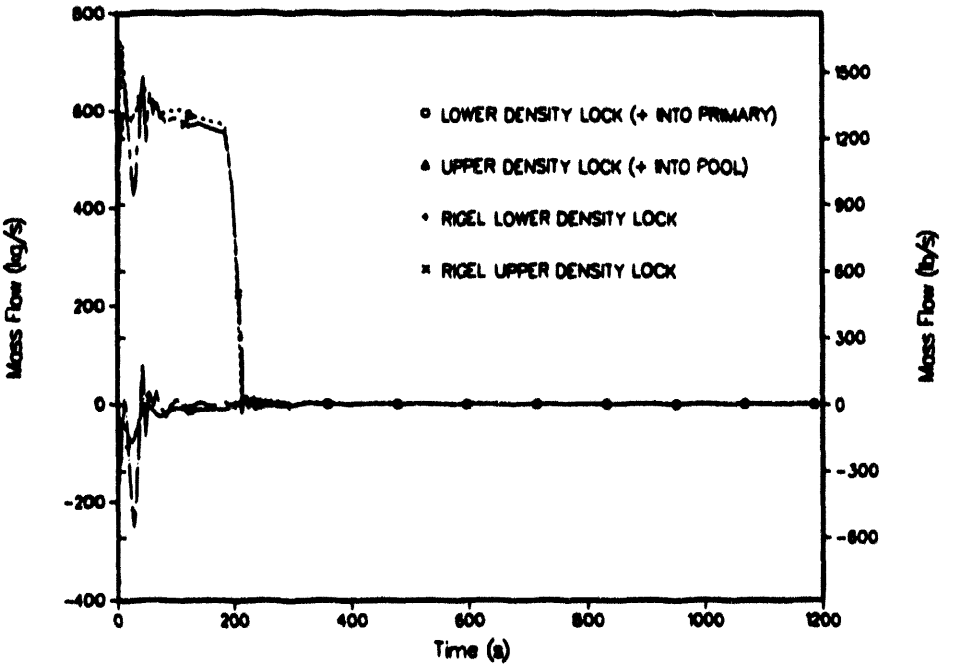


Fig. 2.
Density lock flows for active scram system baseline case.

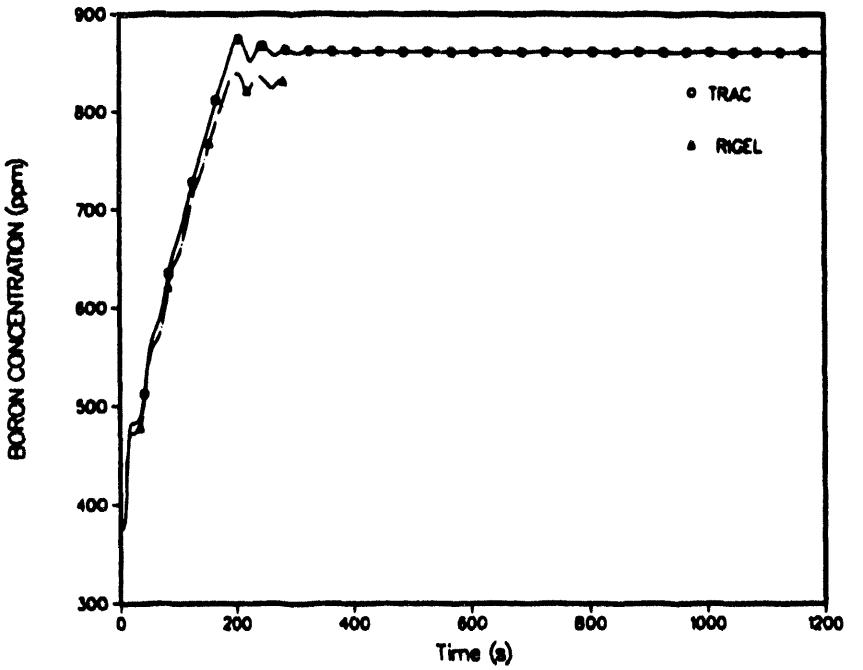


Fig. 3.
Primary boron concentration for active scram system baseline case.

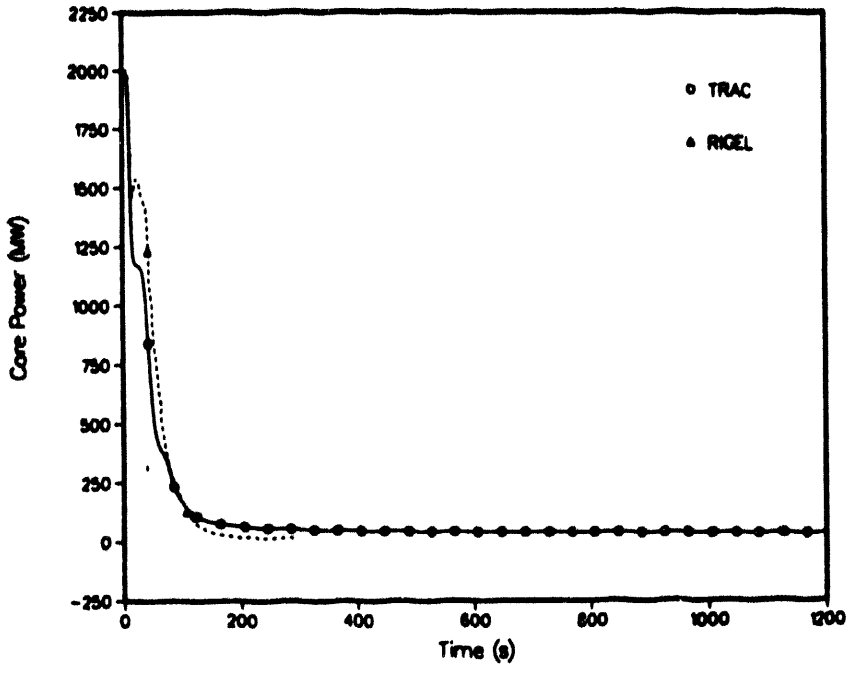


Fig. 4.
Core power for active scram system baseline case.

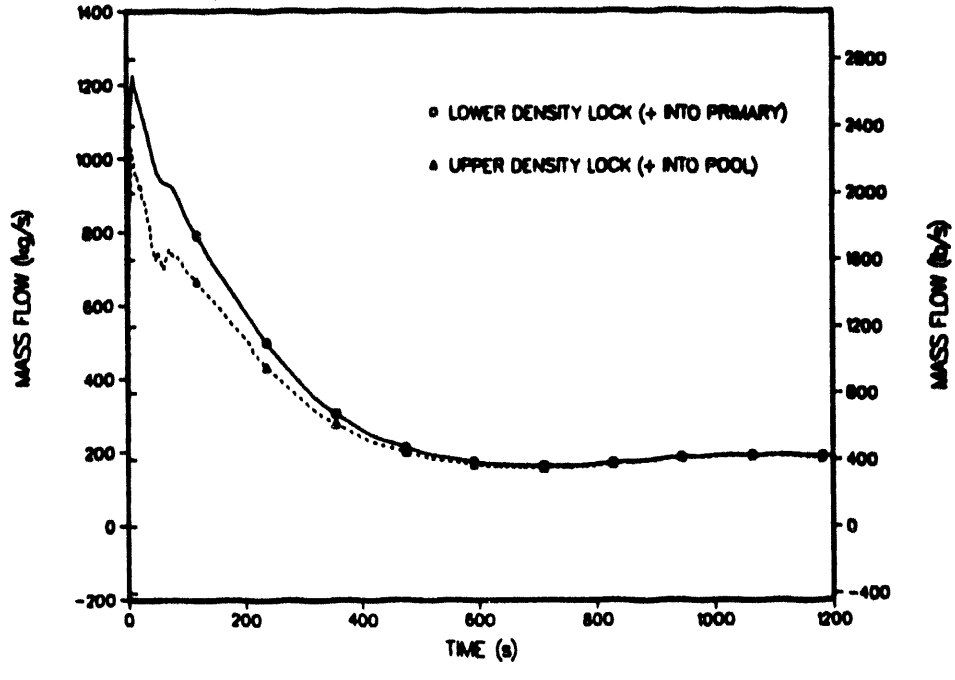


Fig. 5.
Density lock flows for LOSP baseline case.

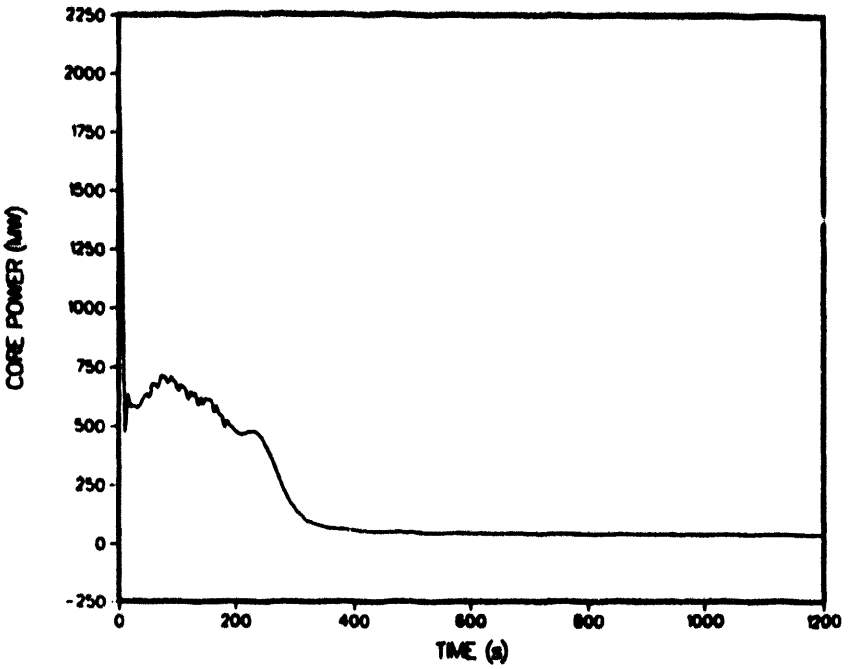


Fig. 6.
Core power for LOSP 100% blockage case.

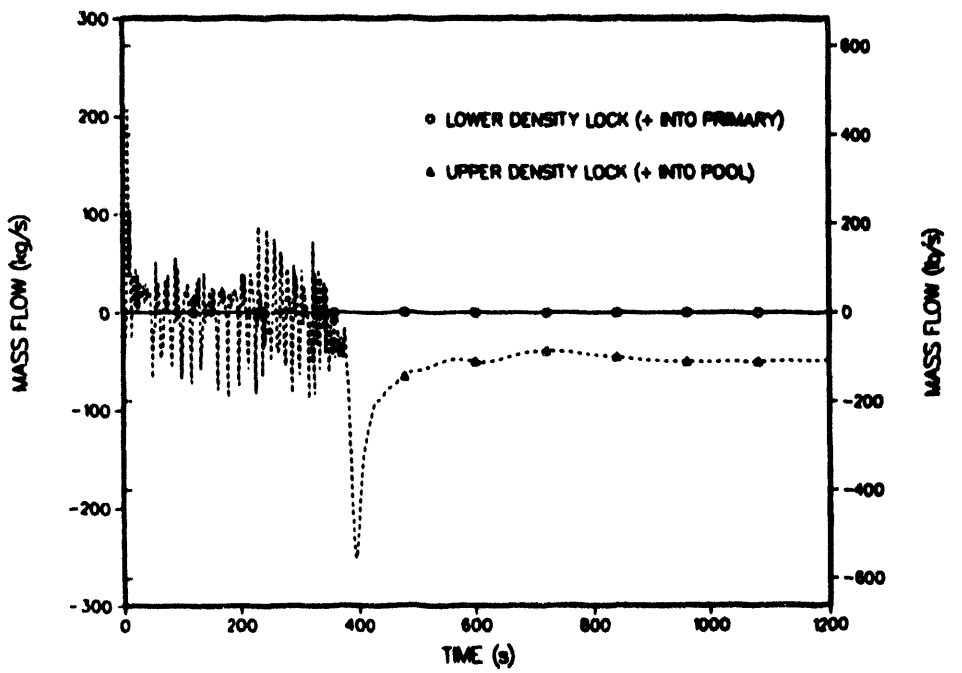


Fig. 7.
Density lock flows for LOSP 100% blockage case.

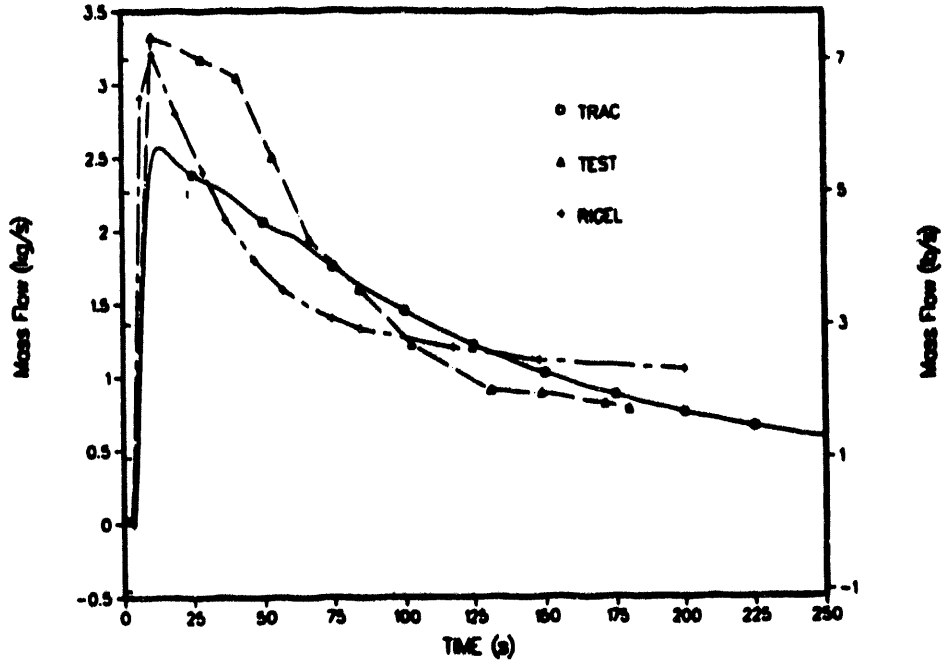


Fig. 8.
Comparison of code-calculated and ATLE lower density lock flows.

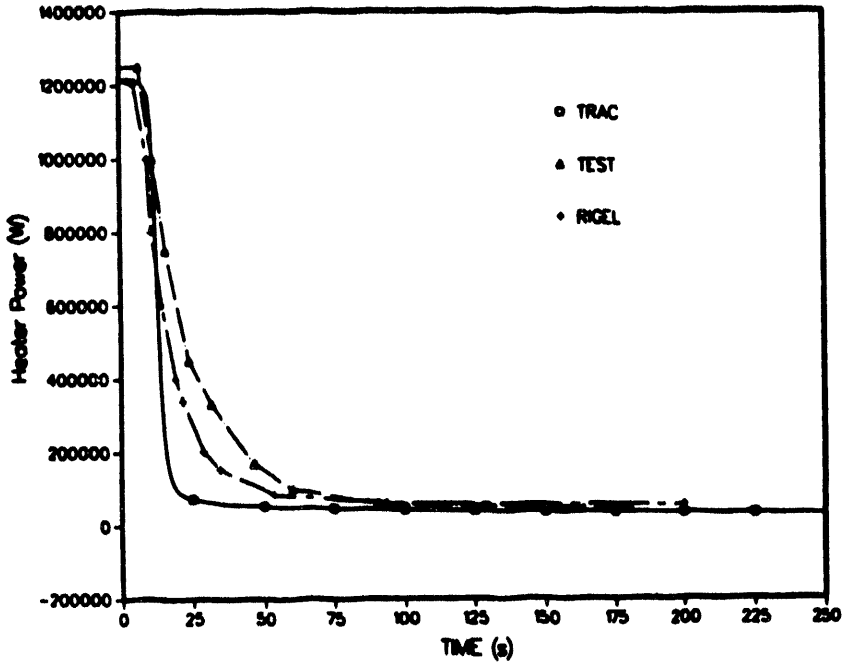


Fig. 9.
Comparison of code-calculated and ATLE heater rod powers.

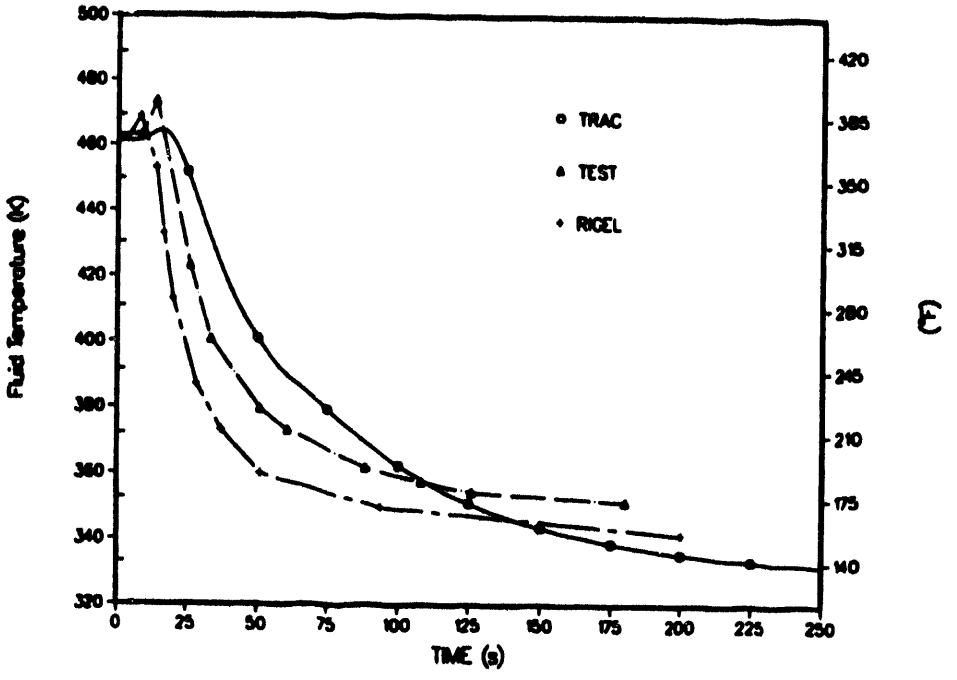


Fig. 10.
Comparison of code-calculated and ATLE core outlet temperatures.

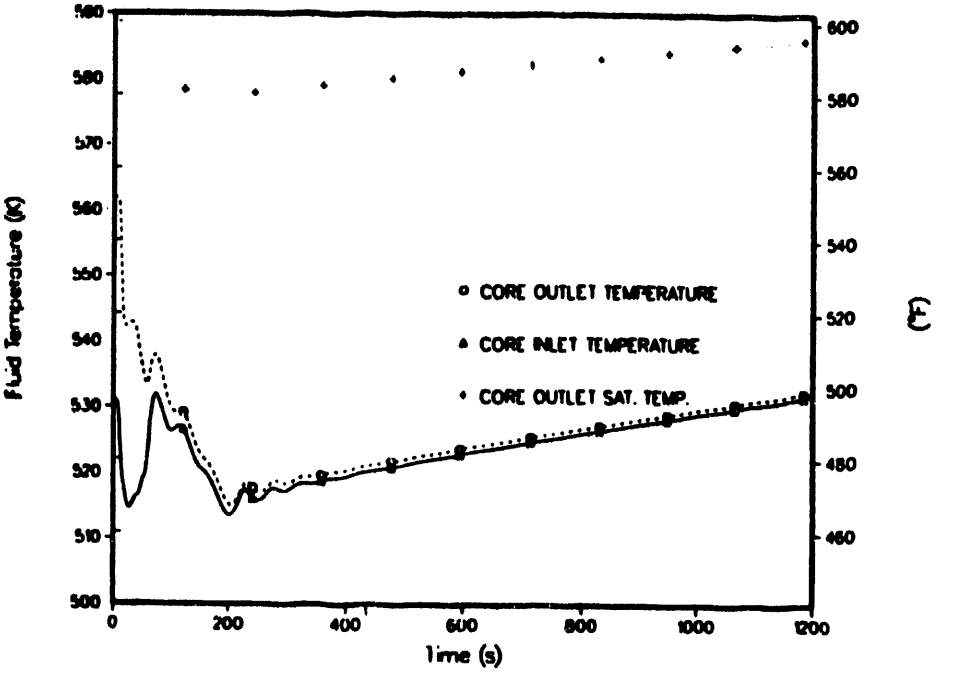


Fig. 11.
Core coolant temperatures for the MSLB baseline case.

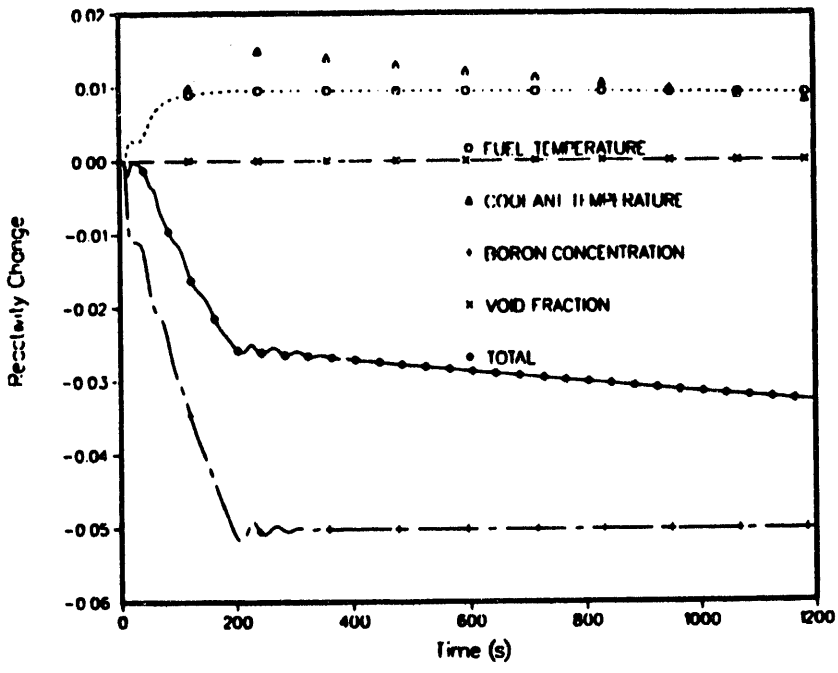


Fig. 12.
Core reactivity changes for the MSLB baseline case.

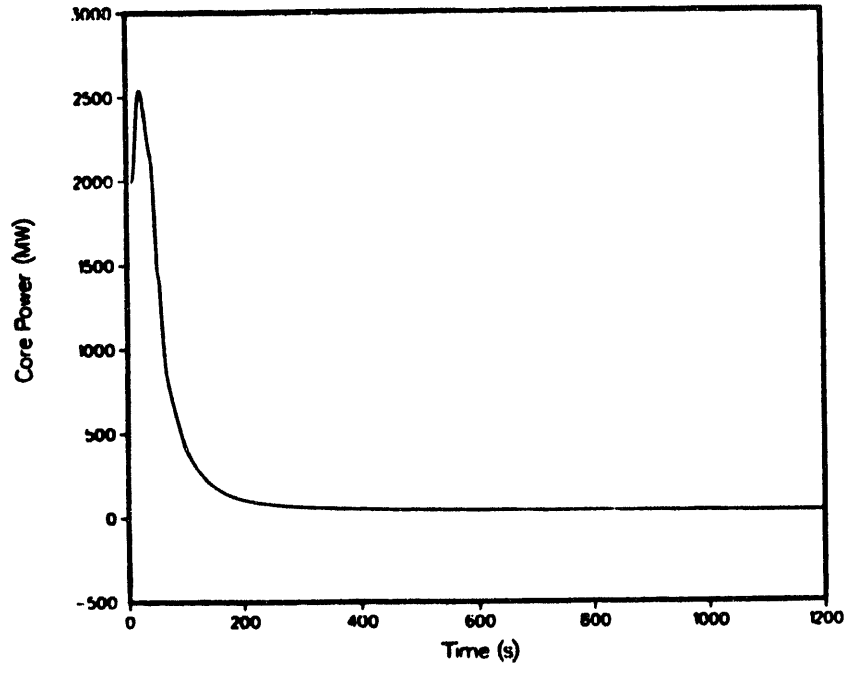


Fig. 13.
Core power for MSLB with failure of active scram system.

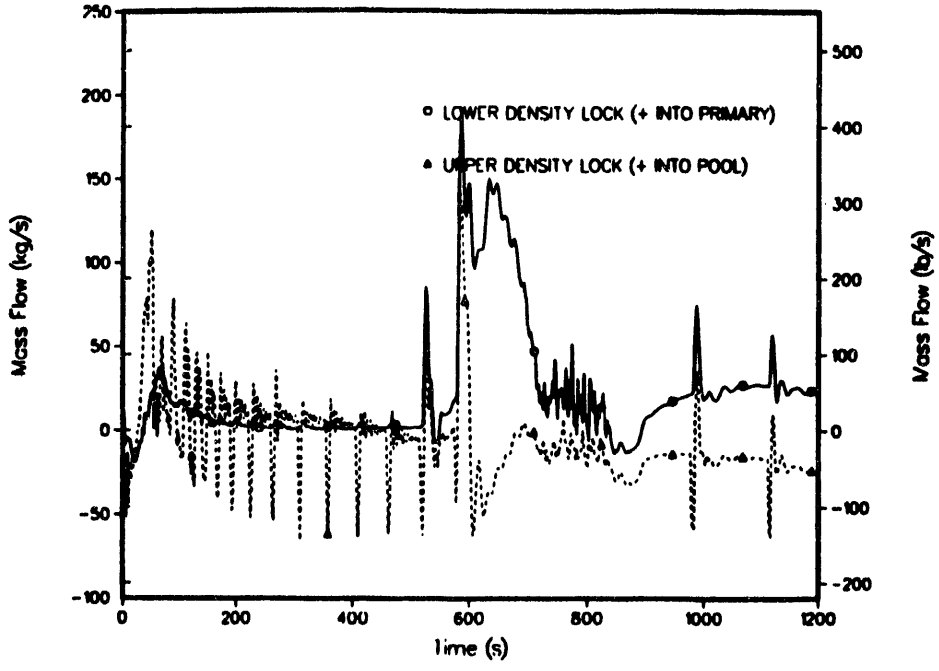


Fig. 14.
Density lock flows for MSLB with failure of active scram system.

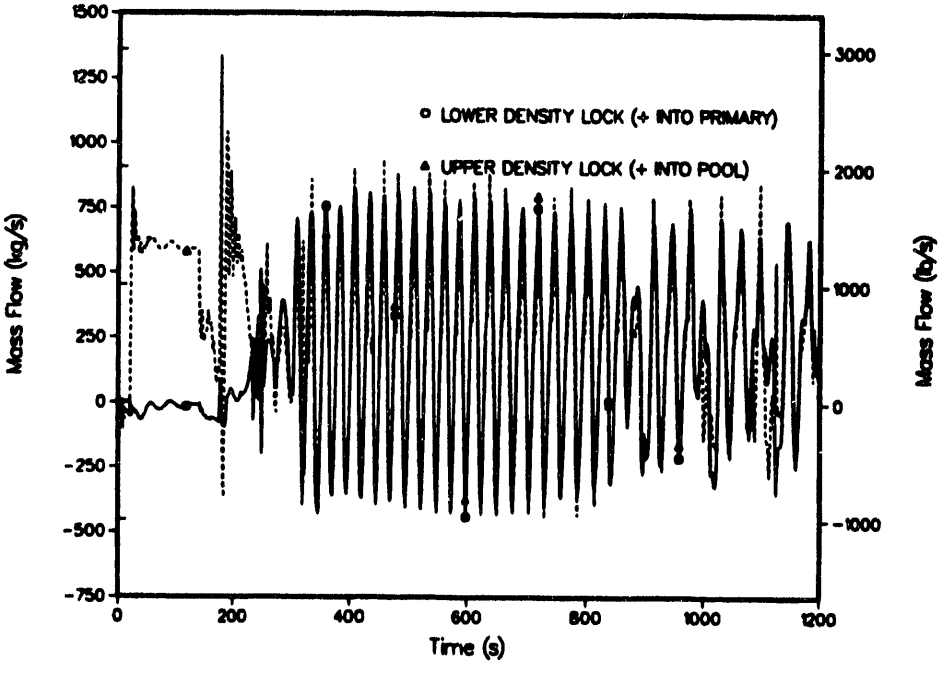


Fig. 15.
Density lock flows for SBLOCA baseline case.

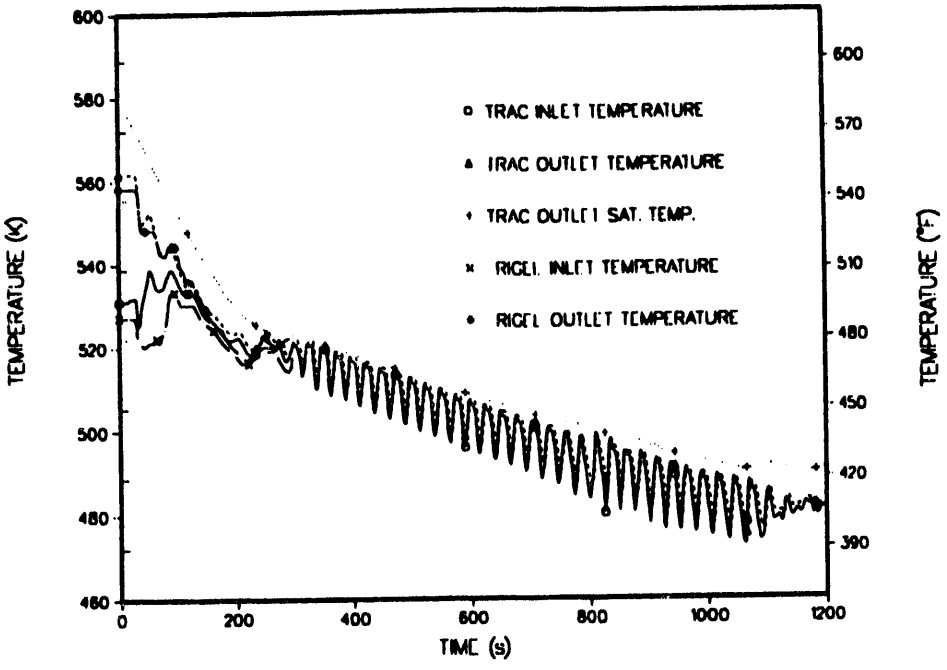


Fig. 16.
Coolant temperatures for SBLOCA baseline case.

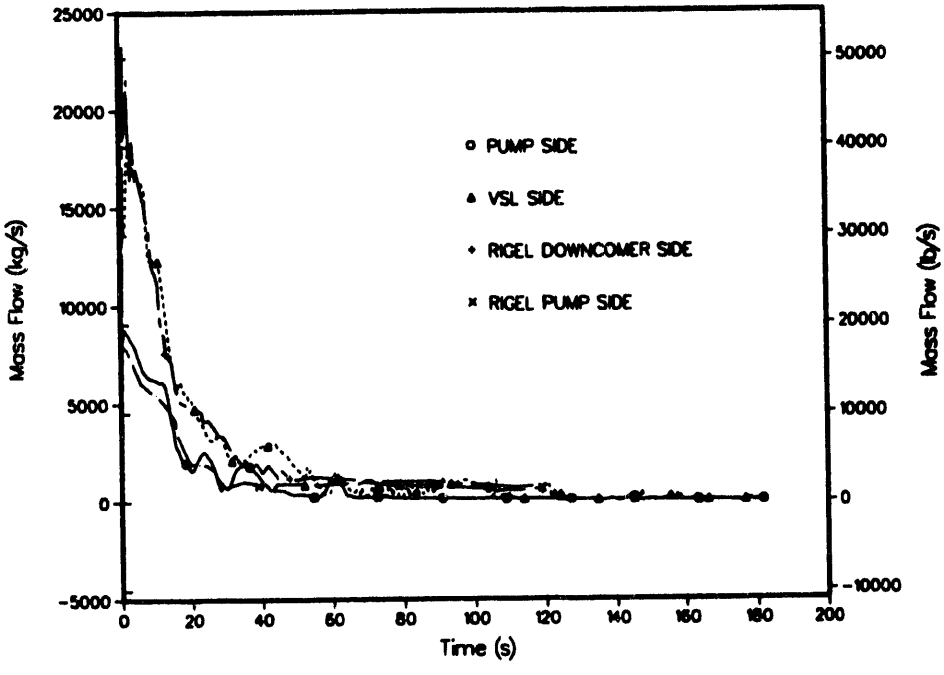


Fig. 17.
Break flows for LBLOCA baseline case.

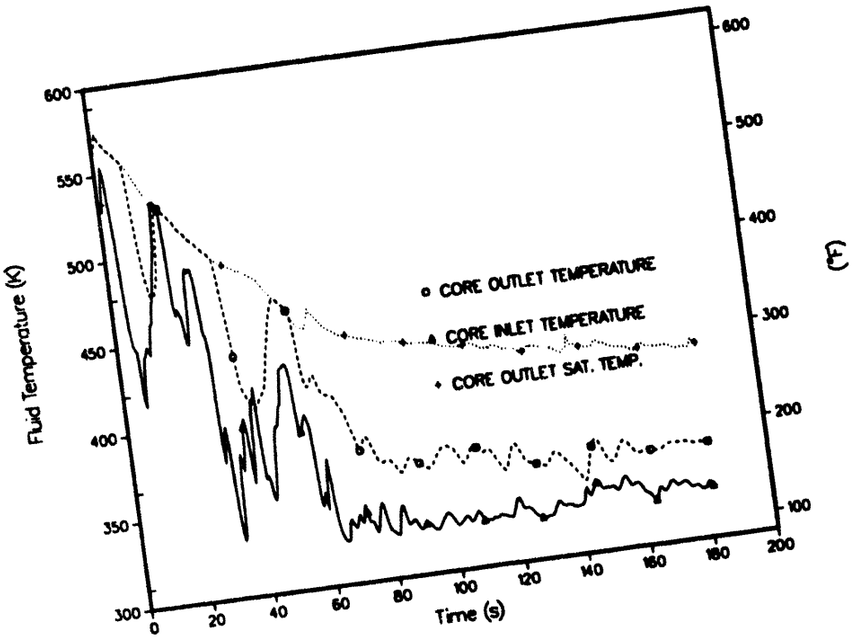


Fig. 18.
Core coolant temperatures for the LBLOCA baseline case.

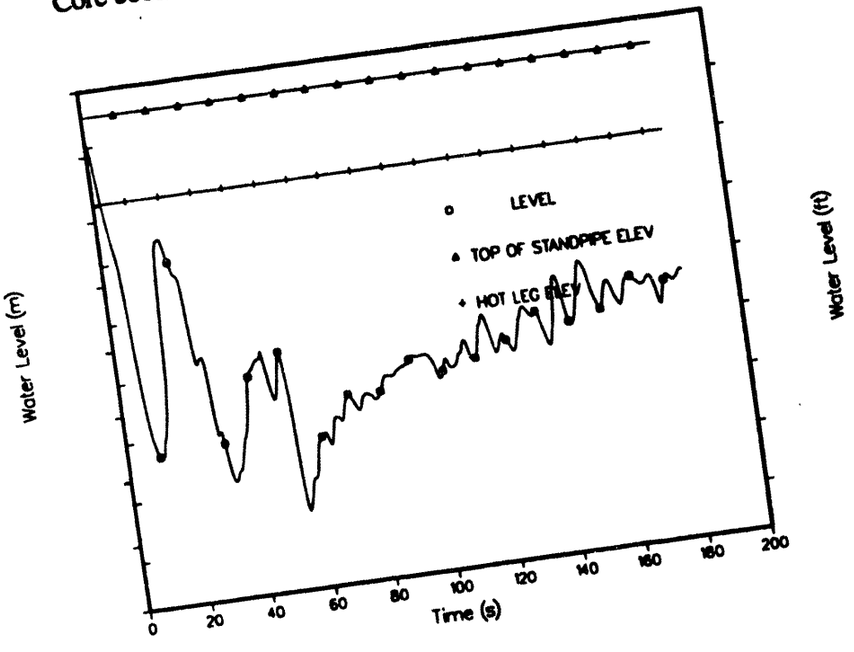


Fig. 19.
Collapsed coolant level for LBLOCA baseline case.

CANDU 3 TRANSIENT ANALYSIS USING AECL CODES[1]

Rex W. Shumway and Jerry L. Judd
Idaho National Engineering Laboratory
David D. Ebert
U.S. Nuclear Regulatory Commission

Abstract

A limited number of transient scenarios were calculated using a computer code suite and input modelling provided by the Atomic Energy of Canada Limited (AECL) for the CANDU 3 design. Emphasis was placed on a large-break loss-of-coolant accident with delays in actuation of the two independent shutdown systems (shutdown rods and liquid poison injection). Although this is expected to be an extremely unlikely scenario, it was studied because of the potential consequences which would result from a positive void coefficient of reactivity. Results indicate that a few second delay in shutdown would result in quickly reaching fuel or cladding melting temperatures, before the emergency core cooling system would be activated. Only small changes in the timing and consequences of the scenario result when several parameters, of potential importance to the progression of the accident, are varied. The severity of the accident is dramatically reduced when it is assumed that one of the two independent shutdown systems function as designed. The results presented in this paper are consistent with related studies performed by AECL[1] and others[2], and do not reveal any new characteristics or phenomena.

1. Background & Introduction

The CANDU 3 design was submitted to the NRC for preapplication design review by Atomic Energy of Canada Limited (AECL) through its U.S. affiliate, AECL Technologies. As part of this review, AECL extended an offer to the NRC and its contractor at the Idaho National Engineering Laboratory (INEL) to use the AECL thermal-hydraulic and neutronic-analysis computer code suite. We accepted this offer and undertook an analysis of a limited number of transient scenarios using DEC5000 workstations, both at the NRC and INEL. We received training in the use of the code suite at AECL facilities in Canada, and have run a variety of sensitivity

1.Work supported by the U.S. Nuclear Regulatory Commission under DOE Idaho Operations Office Contract DE-AC07-76IDO1570.

studies using base-case input decks supplied by AECL. The input model for the base case, a large-break loss-of-coolant accident (LOCA), was identical to that used by AECL in the "Power Pulse Break Survey Analysis" report[1].

The purpose of our analysis was to: (a) gain familiarity with CANDU 3 transient response, (b) look at a spectrum of accident scenarios, (c) look at sensitivity of these scenarios to delayed shutdown, and (d) assess modifications to NRC codes that will be needed in order to perform independent analysis of the CANDU 3 design. This study provides background information for the NRC's preapplication review and is not a licensing design review.

One of the accidents that we analyzed, namely a large break (100% break of an inlet header) LOCA with failure to shutdown, is an extremely unlikely scenario that involves (a) a low probability header break, (b) failure of the shutdown rods, and (c) failure of the liquid poison injection.

The positive void reactivity coefficient of CANDU 3 was raised as a policy issue in a formal Commission paper (SECY-93-092) dated April 8, 1993. This issue arose because General Design Criterion 11 in NRC's regulations requires that a reactor be designed so that, "the reactor core and associated coolant system shall be designed so that in the power operating range the net effect of the prompt inherent nuclear feedback characteristics tends to compensate for a rapid increase in reactivity." While the CANDU design may satisfy this criterion, because it has a slightly negative overall power coefficient during normal power operation, void reactivity increases dramatically during a large-break LOCA. A Staff Requirements Memorandum dated July 30, 1993, in response to SECY-93-092, stated that the presence of a positive void coefficient would not necessarily disqualify such a design, but the consequences of events which have the potential for rapid increases in reactivity, such as a large-break LOCA, should be analyzed. The calculations performed in this study provide some of the background needed to deal with this issue.

The AECL codes and input decks were used in this study with minor modifications although they were set up with conservative input to analyze postulated accidents of the type assessed in Chapter 15 of a FSAR. A lower probability accident, like a large-break LOCA with failure to shutdown, would be more appropriately analyzed using a best-estimate code input deck. However, such an input deck was not available and the base-case input deck was not changed for our analyses. The effect of the conservatively biased initial conditions is discussed within the paper.

Parameter variations were selected to provide a sensitivity study, and do not correspond to any postulated mechanisms. Also, the code output is assumed to be invalid beyond the time at which cladding or fuel melting temperatures are reached, so all the output has been truncated correspondingly. Any analysis beyond melting

temperatures would have to include severe accident treatment with fuel relocation. Thus we have performed only a partial analysis, up to the time where fuel or cladding melting occurs.

Section 2 presents a description of the suite of computer codes developed by AECL to perform thermal-hydraulic and neutronic analysis and the modelling of the CANDU 3 design. Calculational results of sensitivity studies of a large-break LOCA with failure to shutdown performed with the coupled thermal hydraulics and neutron kinetics are presented in Section 3. Section 3 also presents the results of a rod withdrawal transient with failure to shutdown (an anticipated transient without scram) performed with the coupled thermal hydraulics and neutron kinetics models. In Section 4, we also studied the large-break LOCA and small-break LOCA scenarios with successful shutdown and emergency core cooling system activation. Conclusions are drawn in Section 5 from the results of these calculations.

2. Code and Model Description

This section describes the computer codes and input models used to perform the calculations discussed in this paper. Two different models of the primary system were used. Comparisons of the two models for the long term large-break LOCA calculation are given in Section 4.

2.1 Computer Code Description

The computer codes used in these calculations are those developed by AECL to perform the design scoping analysis of the CANDU-3 reactor. The codes are given in **Table 1** along with a brief description of each code.

Table 1. AECL Computer Code Description

Code	Description
CATHENA[3]	A one-dimensional two-fluid six-equation thermal hydraulics code capable of modeling horizontal stratified flow.
KINGPIN	Extracts coolant temperature and density and fuel temperature from the CATHENA model and builds an input file for POWDERPUFS-V.
POWDERPUFS-V[4]	Cross section generation code. Calculates cross sections for each fuel channel axial segment for use in the CERBERUS code.
MATMAP[5]	Processes geometric information, material assignments, and cross section data from POWDERPUFS-V for use by CERBERUS.
CERBERUS[6]	Calculates the time-dependent three-dimensional neutron flux distribution using the Improved Quasi-static method.
CERBSPOW	Calculates the three-dimensional power distribution from the three-dimensional flux distribution calculated by CERBERUS.
INTREP	Calculates the instrument response of in-core and ex-core detectors from the CERBERUS flux distribution.
CATCERB	Constructs the CATHENA input file for the next time step based on the latest power distribution calculated by CERBSPOW.
TRIPDPG	Calculates the time at which the trip setpoints are reached from the instrument responses calculated by INTREP.

The calculations discussed in Section 3 were performed with all the codes listed in **Table 1** and are labeled as "Coupled" in this paper. These calculated the power during the transient with the full three-dimensional kinetics model with temperature and density effects on the cross section data explicitly taken into account. **Figure 1** shows the relationship between the different codes during a coupled transient calculation. The minimum communication time interval between CATHENA and CERBERUS calculations was 50 milliseconds for all the calculation discussed in this paper. A result of this coupling is that the power in the CATHENA is held constant over each 50 millisecond interval and the CERBERUS calculations are based on thermal-hydraulic conditions at the end of the 50 milli-second step.

Calculations were performed with a 10 millisecond communication time interval, and no discernible differences were found between the two calculations.

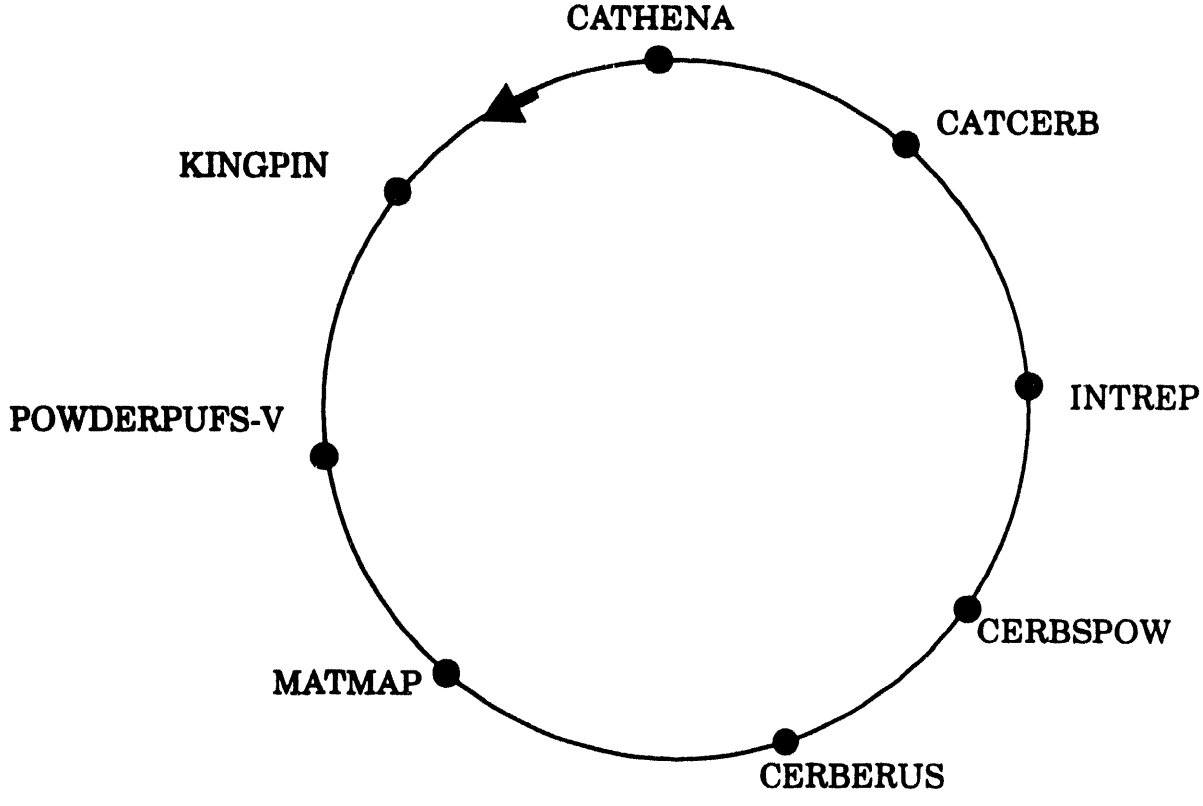


Figure 1 Sequence of codes used for the coupled calculations.

Calculations performed with CATHENA using an input power pulse are labeled as "Uncoupled" in this paper. Power during the transient was precalculated and input to the code. The power history used was that provided by AECL.

2.2 Ten-Channel CATHENA Primary Loop

CATHENA is a two-fluid six-equation code. The version of CATHENA used for these calculations is 3.4b Rev 6 with three additional updates to allow it to run on the INEL DEC 5000 workstations. **Figure 2** shows a CATHENA nodalization diagram of the primary loop. CANDU 3 reactors have two steam generators and four primary pumps. Consequently they have two headers at the core exit and four headers at the inlet. The primary loop is filled with heavy water and the secondary loop uses light water. The primary loop has a figure-8 type flow path since fluid goes through both steam generators during a complete loop through the system. The

numbers in the boxes in **Figure 2** represent the number of hydraulic cells for that component. Empty boxes represent one cell.

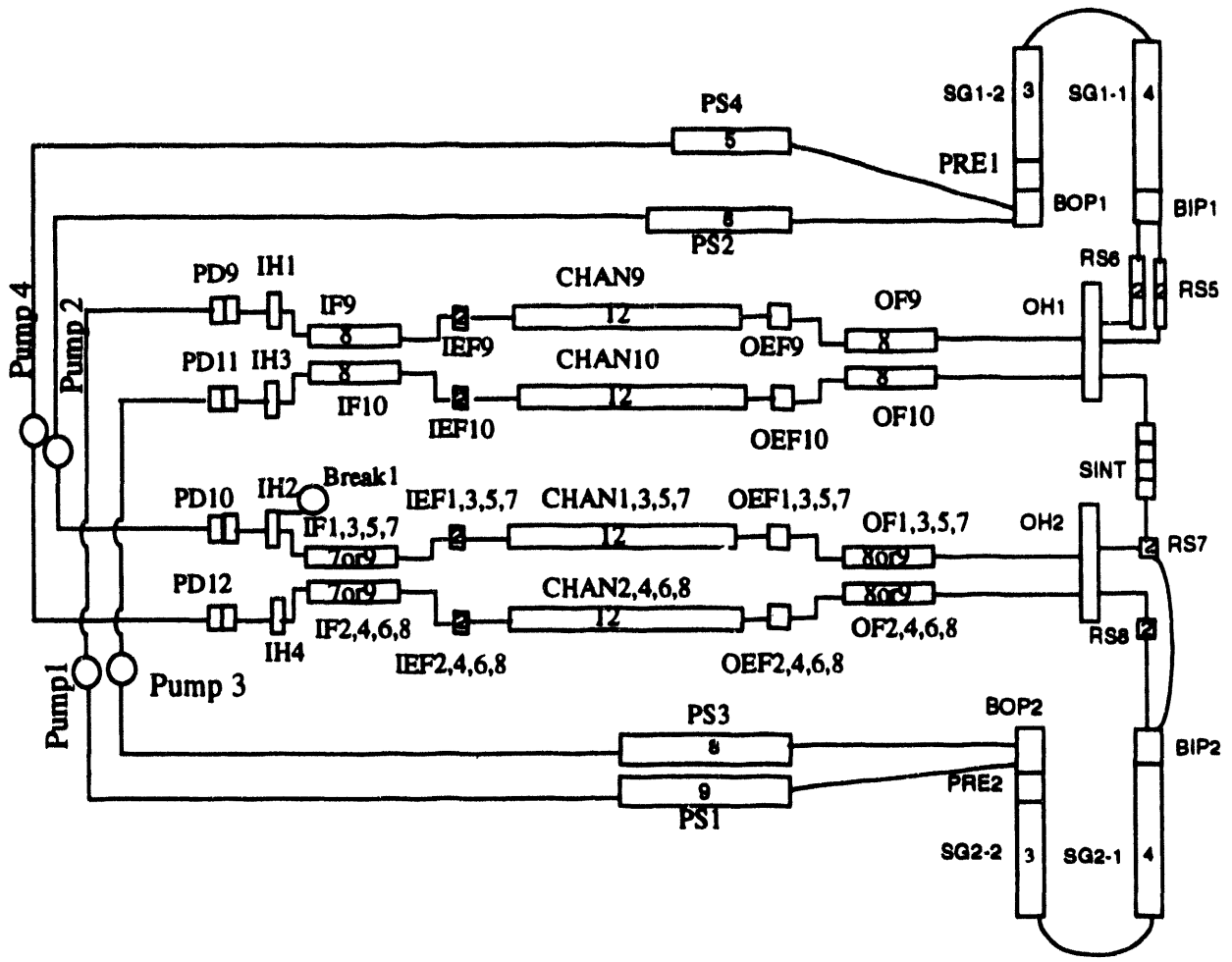


Figure 2 CANDU 3 Primary Loop Nodalization

The 232 core pressure tubes are modelled by ten CATHENA channels. Eight channels model half the core and two channels model the other half. **Figure 3** illustrates the channel groupings. This figure demonstrates that the 58 feeder pipes connected to each inlet header distribute liquid to a one-half core sector rather than to a one-quarter sector of the core. This is because the feeder pipes from each header delivers fluid to vertically alternating pressure tubes in each core half.

Table 2 gives the number of core pressure tubes each CATHENA channel represents. It also gives the power per channel and the power per unit flow. This

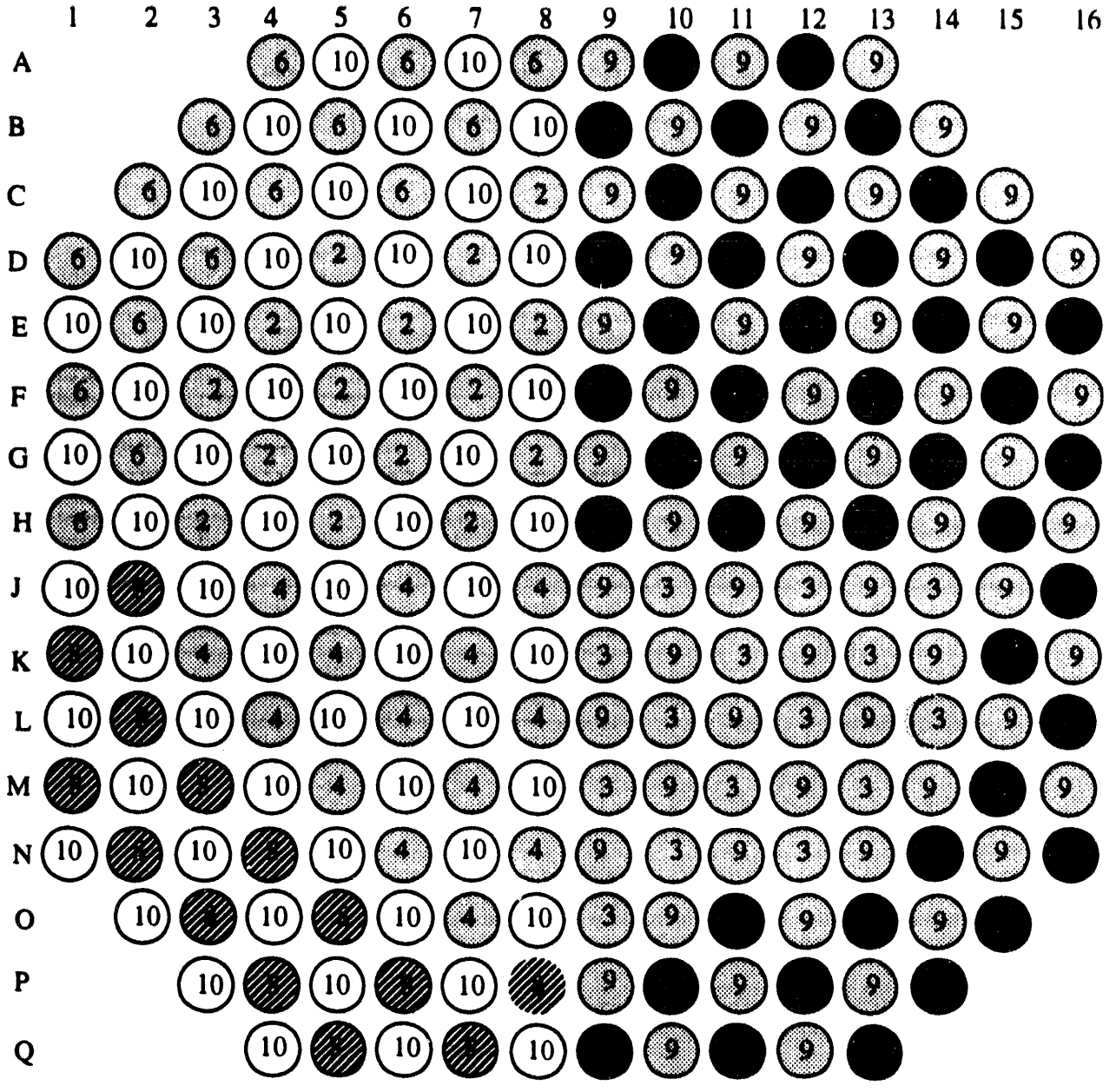


Figure 3 Core Cross-section Showing CATHENA Channel Groups

input file models a 6% power tilt which contributes to the mismatch in power per unit flow among the channels. Power is tilted toward the right hand side of the core.

Table 2: Channel Radial Power Profile

CATHENA Channel Number	Connected to Inlet Header	Power MW	Number CANDU Fuel Channels	MW/ Channel	Radial Peaking Factor	Flow per Channel kg/s	Power/ Flow MW/ kg/s
1	IH2	104.89	14	7.492	1.231	24.17	0.30997
2	IH4	99.37	15	6.625	1.089	25.02	0.26475
3	IH2	112.24	15	7.483	1.230	24.61	0.30406
4	IH4	94.67	14	6.762	1.111	25.23	0.26801
5	IH2	79.32	14	5.666	0.931	20.68	0.27399
6	IH4	67.84	15	4.523	0.743	21.63	0.20910
7	IH2	79.16	15	5.277	0.867	21.18	0.24915
8	IH4	68.27	14	4.876	0.802	21.39	0.22794
9	IH1	375.61	58	6.476	1.064	22.76	0.28459
10	IH2	330.12	58	5.692	0.936	23.36	0.24363
Total		1411.5	232	6.084			

The first eight channels have 19 fuel rod groups modelled in them while channels nine and ten have only one. A fuel rod group is a collection of fuel rods that are lumped together for the temperature calculations. The 19 rod group set assumes half bundle symmetry while the single rod group set lumps all fuel rods together. The reactor has 37 fuel rods per bundle and 12 fuel bundles per pressure tube.

The CANDU 3 steady-state core power is high enough to cause saturated boiling at the channel exit. During normal operation of the CANDU 3 core, the core exit flow quality is roughly 4% (equivalent to 30 to 40% void fraction). The initial void profile influences the transient power profile because it effects how much the void fraction can change during the transient. **Figure 4** shows the axial void profile for three of the ten channels. Notice that channel 9 has a higher exit void fraction than channel 2 even though power is lower (see **Table 2**). The input power and flow resistances are such that channel 9 has a higher power/flow than channel 2. **Table 2** gives the power per unit flow for each channel. Although the flow resistance values given in the input file for channels 2 and 9 are about the same, channels 6 and 8 have larger

resistances than 2. Since 2 is in parallel with 6 and 8 it gets a larger flow rate than does the average channel 9.

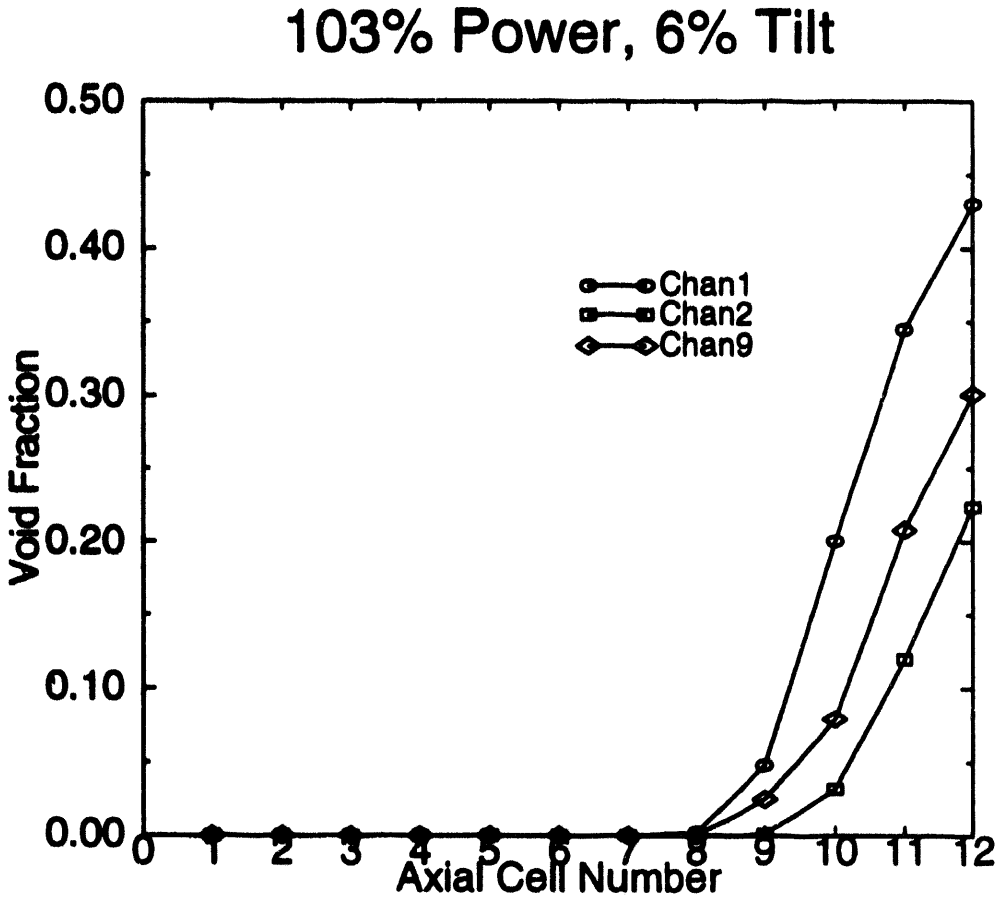


Figure 4 Steady-state axial void profile.

CANDU transients are sensitive to whether off-site power is available. When this power is available, all four primary loop pumps receive a LOCA signal trip delay of 15 minutes after the pressure in outlet header No. 1 drops below 6 MPa. This trip time delay is intended to allow the emergency core cooling system to bring the fuel temperature down. (A high reactor building pressure can also give a LOCA signal but the building is not modelled.) Outlet header 1 is used for this signal detection rather than outlet header 2 because it is hydraulically further from the pressurizer. In the event of a loss of off-site-power the pumps have no long term power source.

2.3 Secondary Loop

The secondary loop has a feedwater reservoir which supplies the secondary side of both steam generators. Separators at the top of the steam generators send steam to the turbine and water to the downcomer. The CATHENA nodalization is shown in **Figure 5**.

A LOCA signal causes the Emergency Core Cooling system to activate and allows the main steam safety valves to begin opening. Flow from these valves causes the secondary to blowdown and helps cool the primary water more rapidly (crash cooldown).

2.4 Emergency Core Cooling System

The emergency core cooling system was part of the input file for the long transient calculations and is not needed during the short time span of the power pulse calculations. However, since its nodalization diagram contains part of the primary loop, it is illustrated at this point (see **Figure 6**). The pressurizer is attached between ECO 11 and 12. All but ECO12 and the pressurizer were eliminated from the input file for the power pulse calculations to save computer time.

All six headers are fed by water from the Emergency Core Cooling system. ECO connects to the two outlet headers and ECI connects to the four inlet headers. Rupture discs in the Emergency Core Cooling lines burst when a differential rupture pressure of 0.35 MPa is reached. High pressure Emergency Core Cooling injection comes from an accumulator and low pressure injection is pumped from a grade level tank. The accumulator tank has 150 m^3 of air and 300 m^3 of light water at an initial pressure of 6.43 MPa and a temperature of 323 K. One control volume models the two tanks in the plant. One of two low pressure pumps cause water to flow in a circular path until low pressure loop check valves open. They open after the accumulator has dumped enough effluent to reduce the pressure downstream below the pump pressure. Low pressure water comes from a grade level tank at a temperature of 323 K.

2.5 Three-Dimensional Kinetics Model

The three-dimensional kinetics model is the same one described in **Reference 1** and only a brief description is given here. There are primarily three sets of input files used for the kinetics modeling and each is discussed below.

The POWDERPUFS-V[4] code is used to calculate the cross section data for the thermal-hydraulic conditions that exist in each axial segment of each of the ten fuel channels modeled in CATHENA. A basic input file is developed that contains input sections for each of the 120 fuel types used in the model. At each time point, coolant

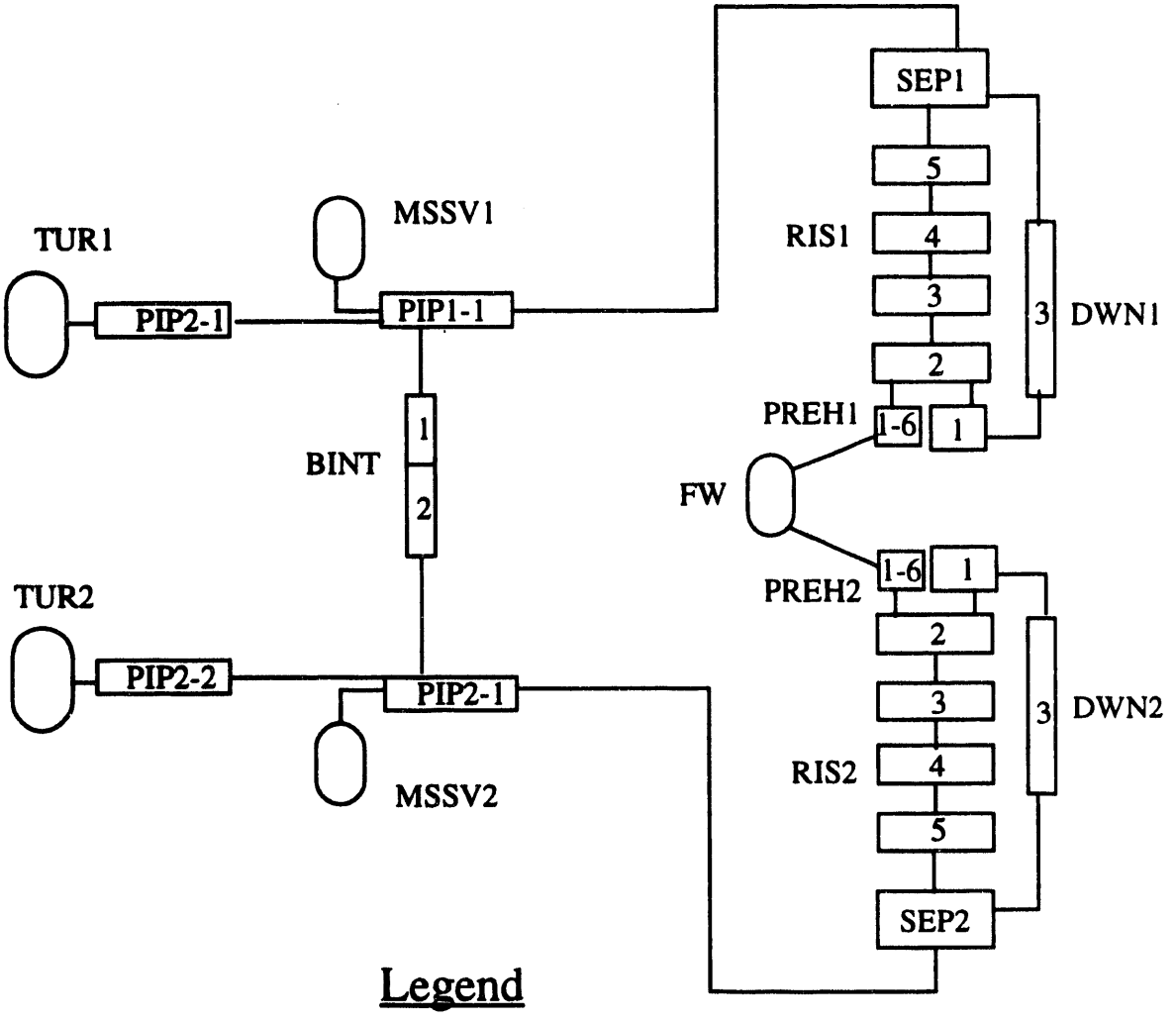


Figure 5 CANDU 3 Secondary Side Nodalization

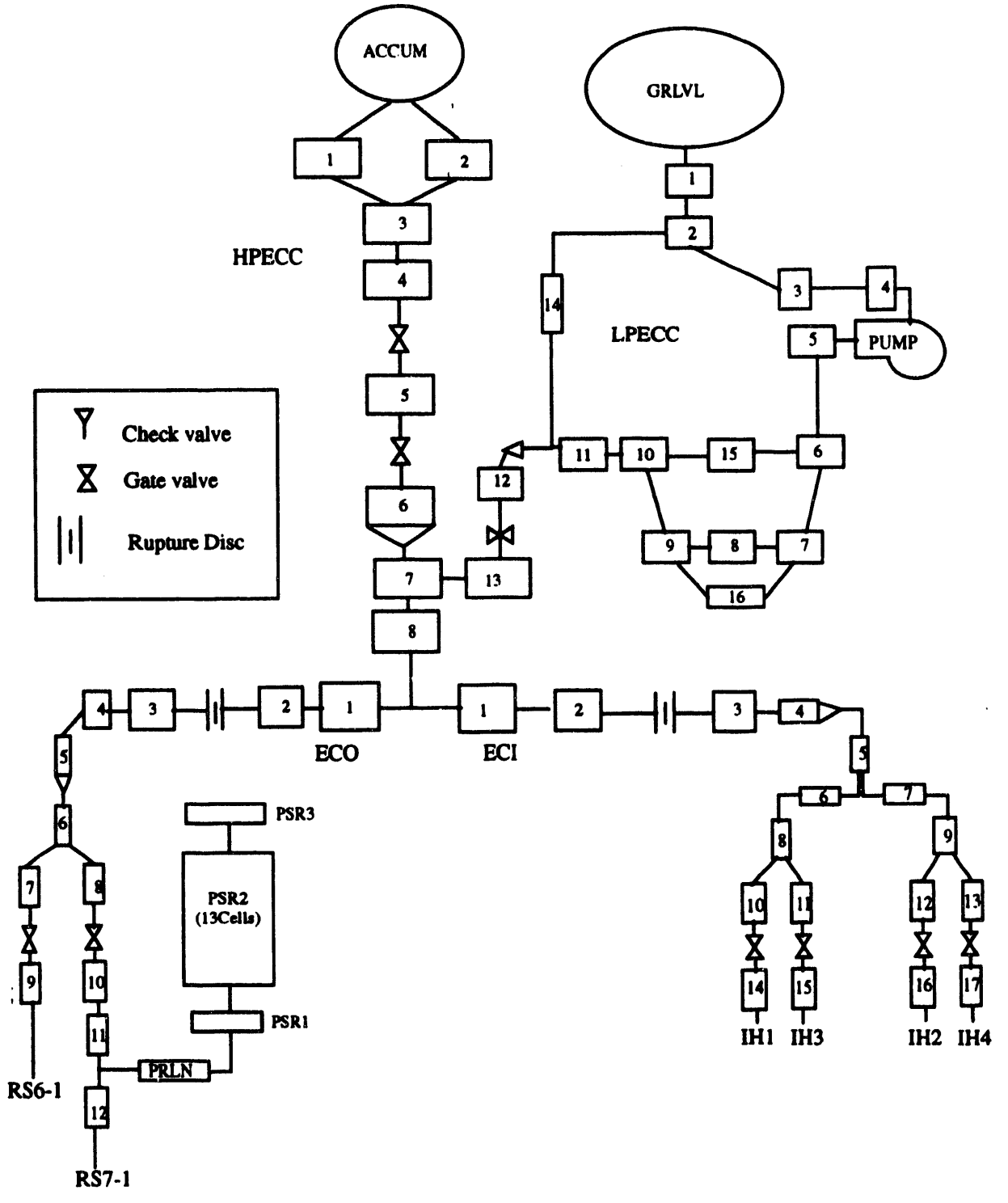


Figure 6 CANDU 3 Emergency Core Cooling System Nodalization Diagram

density, coolant temperature, and fuel temperature data are extracted from the CATHENA results and processed into a POWDERPUFS-V input file for the current time step.

The MATMAP code input consists of geometric information concerning mesh sizes, cross section set assigned to each mesh cell, and the location and type of all reactivity devices present in the core. Basically, the X-Y geometric model is as shown in **Figure 3**, with either one or two mesh intervals per pressure tube and additional mesh intervals for modeling the reactivity devices. These constraints result in 36 mesh intervals in the X-direction and 24 mesh intervals in the Y-direction. The axial model consists of fourteen mesh intervals, which is one per fuel bundle except for the bundle on each end which has two equal size mesh intervals.

The CERBERUS code solves the time-dependent diffusion equation using the improved quasi-static method with data calculated by MATMAP. The CERBERUS input includes information about the number of delayed neutron groups, the steady-state power, steady-state or transient solution, and flux shape re-calculation time interval.

3. Coupled Calculational Results

This section presents results of calculations performed with the coupled code system shown in **Figure 1** and the 10 channel CATHENA model described in Section 2.2 and Section 2.3 and the kinetics models described in Section 2.5. Section 3.1 describes the sensitivity calculations performed for the large-break LOCA and Section 3.2 describes the rod withdrawal without scram calculation.

3.1 Large-Break LOCA Sensitivity Calculations

The LOCA event for a CANDU-3 reactor results in a quick partial voiding of the core which causes a positive reactivity insertion due to the positive void coefficient of the reactor. For this reason, a significant change in the spatial flux distribution results from the non-symmetric voiding behavior and this requires a full three-dimensional kinetics capability. The coupling of the spatial kinetics was discussed in Section 2.1.

Core power is calculated by the kinetics code suite during the power pulse transient. Therefore, the core power changes with time because the fuel and fluid temperatures and channel void fractions change and affect the core reactivity. The power initially shifts to the outlet end of the channels because that is where the hot water is and where voiding begins. CANDU 3 reactors have a positive void feedback coefficient and are therefore designed with two redundant shutdown systems. They have a rod injection system with rods entering the moderator tank from the top and the have a poison liquid injection system with injectors entering the tank from the

side. Use of the phrase 'without scram' in this report means that both systems are assumed to fail.

The base-case input deck is labelled 100% reactor inlet header break at 103% of full power with a 6% tilt. The tilt is toward the side fed by inlet headers 1and 2. The break location is inlet header number 2. The break area is twice as large as the header cross-sectional area. The initial reactor power is 1411 MW. (**Reference 7** gives a value of 1420.782 as 103% of full power.)

A series of calculations were run to evaluate the effect of changing individual parameters on the core response. The steady-state conditions used to initiate the transient are a core at 103% full power with a 6% tilt imposed on the core. A 100% inlet header break was selected as the base case based on results given in **Reference 1** that state that the 100% inlet header break is the most limiting break for the CANDU-3 design. Sensitivity calculations were performed for cases with and without scram. Scram by the shutoff rods was simulated in the calculations using a scram, but the initiation of the scram was determined by the slowest trip signal from all SDS1 and SDS2 incore and excore instrumentation. **Table 3** presents the parameters varied and a brief summary of the peak values of power, reactivity, cladding surface temperature, and fuel centerline temperature achieved during the transients with scram.

Table 3. LBLOCA With Scram Sensitivity Cases

Scram	Parameter Varied	Parameter Value	Peak Relative Power	Peak Reactivity ($)	Peak Clad Surface Temperature (K)	Peak Fuel Centerline Temperature (K)
Nominal	Base Case	96.36% Purity	2.1327	0.586	1380	2790
Nominal	Coolant Purity	99.722% Nominal	1.8022	0.478	1340	2750
Nominal	Coolant Purity	93% Worst	2.5782	0.690	1380	2790
Delayed	Scram Time	Delayed 1 second	4.9321	0.797	1720	3010

Figure 7 shows the normalized power behavior for all the cases with scram. The coolant purity variation results in different void reactivity worth (see **Figure 8**) and yields a higher peak power (approximately 15%) than the base case. The delayed scram results in a significant rise in peak power which results from the increased voiding in other channels as seen in **Figure 9**. The effect of these variations on the

peak fuel centerline and peak cladding surface temperature is shown in **Figure 10**. The gap conductance value used in the CATHENA model was 10 kW/m^2-K. Since the cladding is thin compared to U.S. reactors the AECL believes this to be a conservative value and calculated peak fuel temperatures may be as much as 500 K too high. Since none of the cases shown in **Table 3** reach fuel melt, this conservative assumption has no significant effect on the results of the transient. The change in temperature is small for the coolant purity variation and significant for the delayed scram, but temperature values are still below melting temperatures.

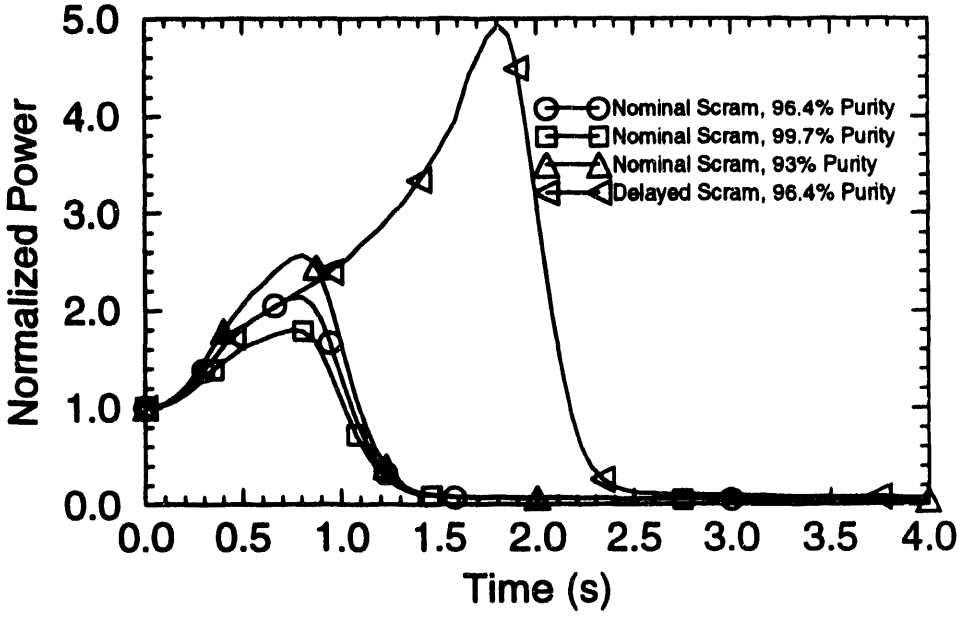


Figure 7 Normalized power for coupled calculations with scram.

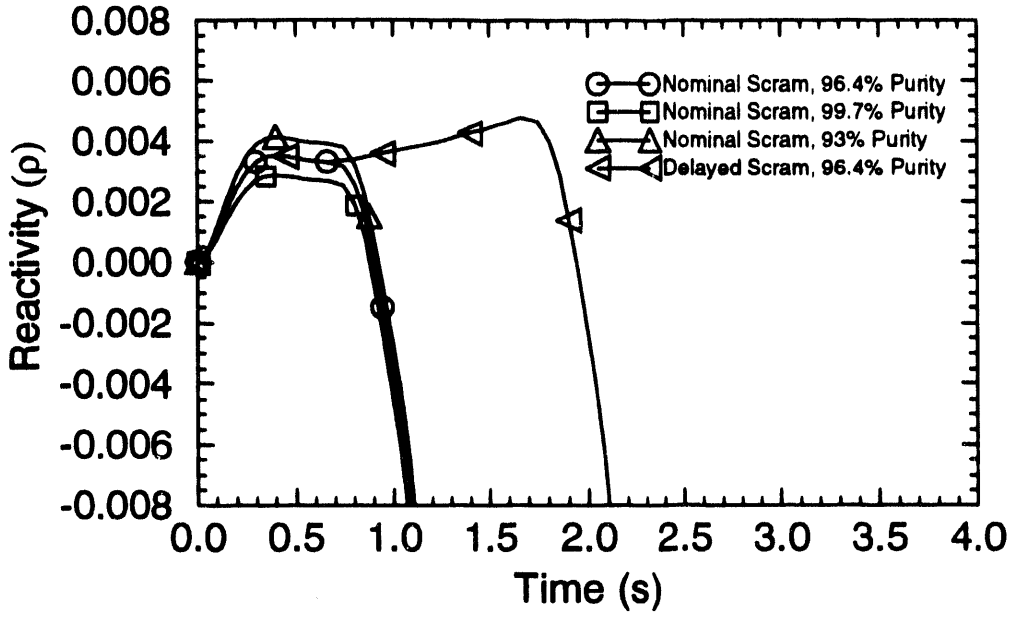


Figure 8 Reactivity for coupled calculations with scram.

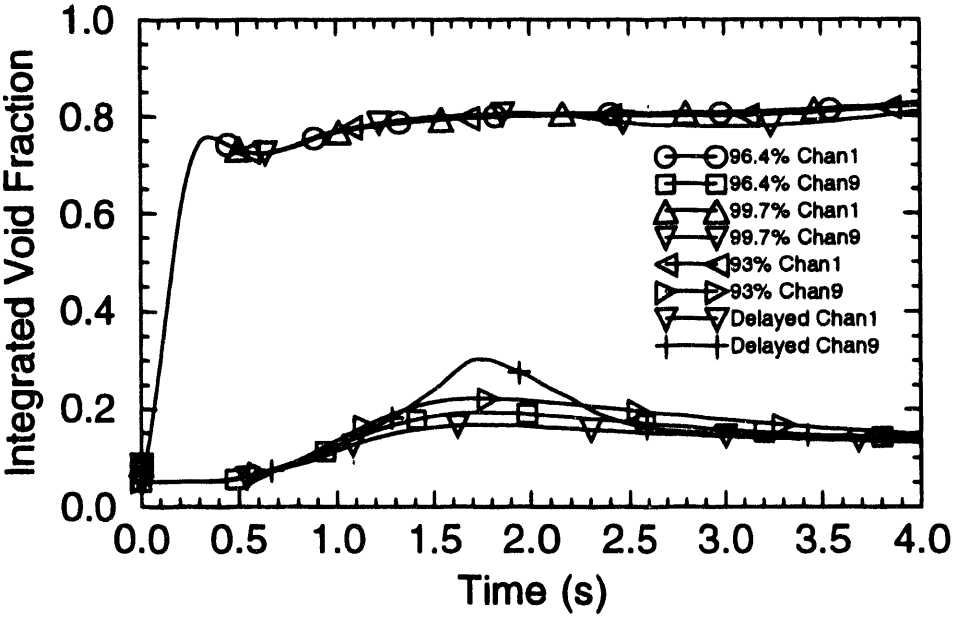


Figure 9 Integrated void fraction for coupled calculations with scram.

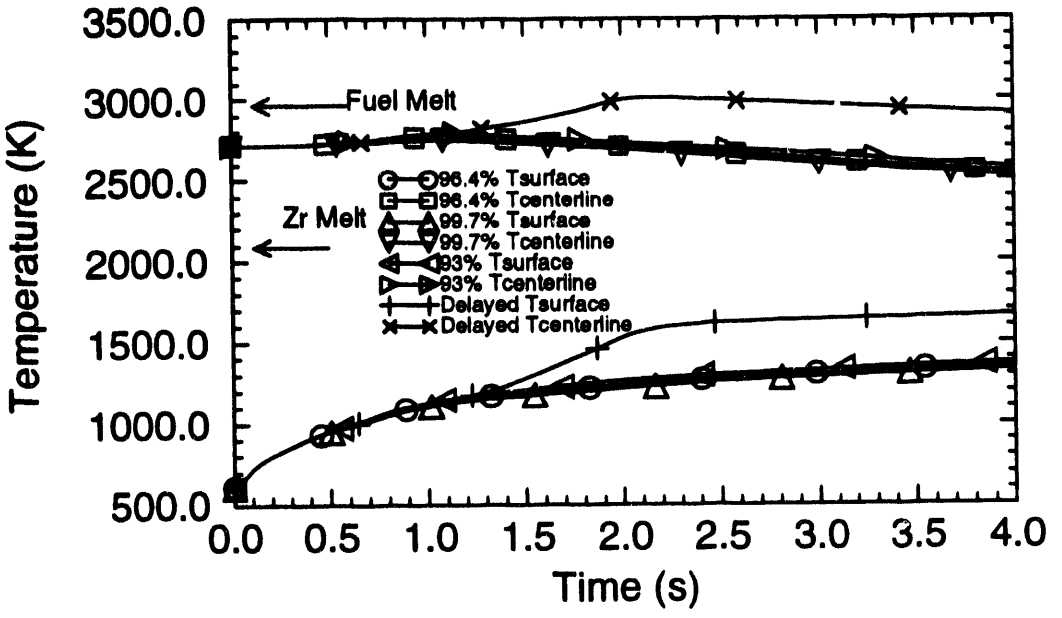


Figure 10 Peak fuel centerline and peak cladding surface temperatures for coupled calculations with scram.

Table 4 presents the parameters varied for the transient without scram and a brief summary of the values of power and reactivity when either the cladding or fuel melting temperatures are reached during the transient. The conservative gap conductance only affects the time at which fuel melt occurs for the cases without scram.

Table 4. LBLOCA Without Scram Sensitivity Cases

Parameter Varied	Parameter Value	Relative Power[a]	Reactivity ($)[a.]	Time to Reach Clad Melt[b] (s)	Time to Reach Fuel Melt[c] (s)
Base Case	96.36% Purity	7.20	0.60	3.005	3.105
Coolant Purity	99.722%	4.55	0.47	3.845	> 4.25
Coolant Purity	93%	12.22	0.77	2.425	2.385
Heat Transfer Coefficient	+20%	9.51	0.65	2.814	2.844
Heat Transfer Coefficient	-20%	1.92	0.54	0.602	Above melt in steady-state
CHF	+20%	7.21	0.61	3.005	3.105
CHF	-20%	7.30	0.60	2.994	3.104
Initial Power	70%	7.13	0.48	3.782	> 4.25
Initial Power	30%	8.40	0.32	5.822	6.757

a. Value at time the first melting point is reached
b. Clad melting temperature is 2100 K.
c. Fuel melting temperature is 3100 K. 500 K is subtracted from the CATHENA fuel temperature to correct for the conservative gap conductance.

The normalized power for the cases without scram is shown in **Figure 11**. Only those cases for which there is a significant difference from the base case are shown. **Figure 11** shows that one of the cases results in a rapid runaway of the power (93% coolant purity). **Figure 12** shows the reactivity during the transient for each case. The effect of the variations on the voiding rate is shown in **Figure 13** and **Figure 14**. The voiding rate in CHAN1 (connected to the broken inlet header) is essentially the same in all the cases. The significant changes in voiding rate occur in the channels connected to the intact inlet headers as shown in **Figure 14**. **Figure 15**

shows the behavior of the peak cladding surface temperature for the different cases and **Figure 16** shows the behavior of the peak fuel centerline temperature.

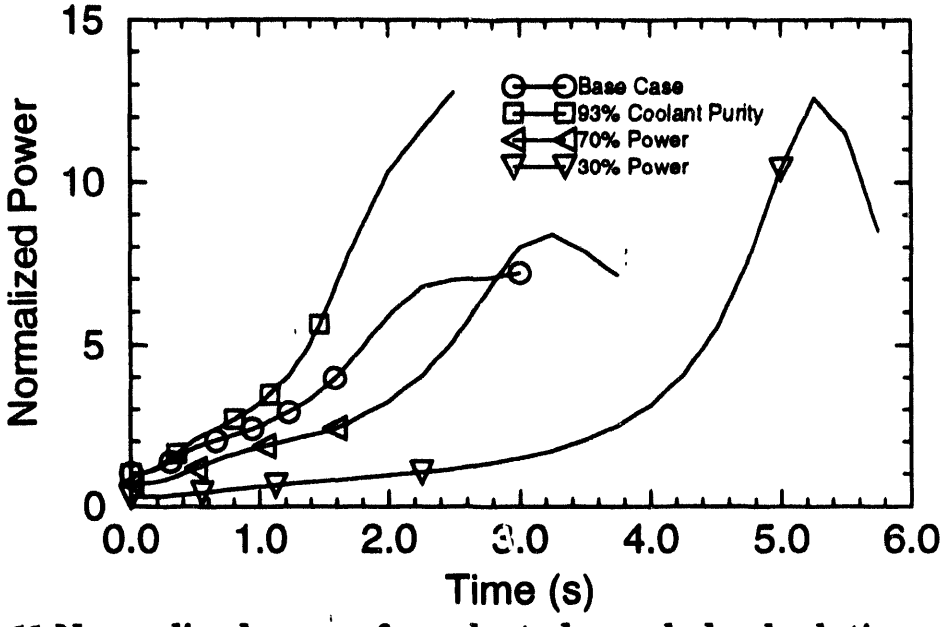


Figure 11 Normalized power for selected coupled calculations without scram.

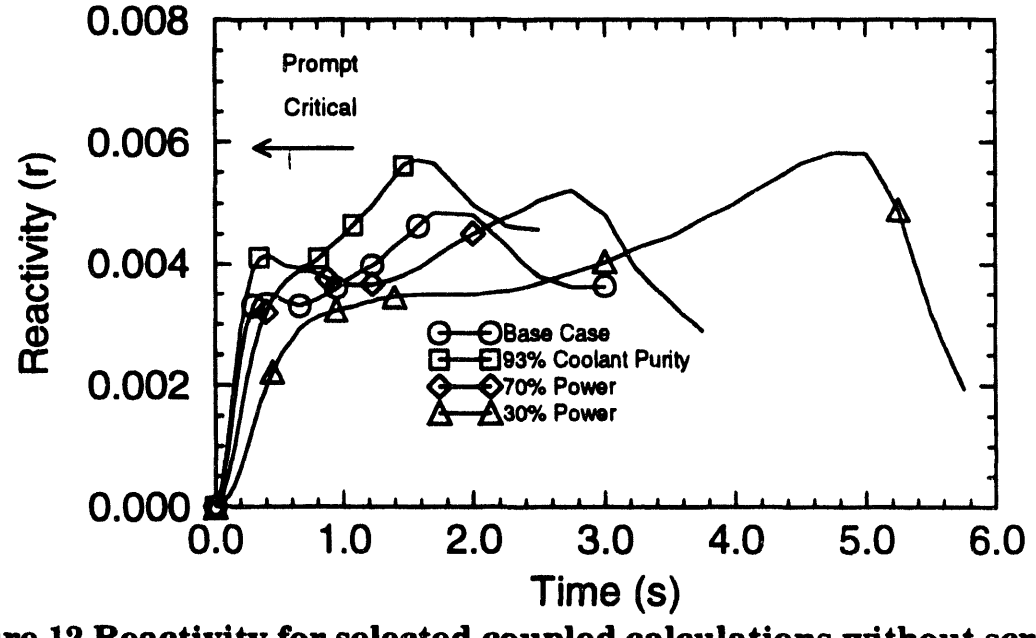


Figure 12 Reactivity for selected coupled calculations without scram.

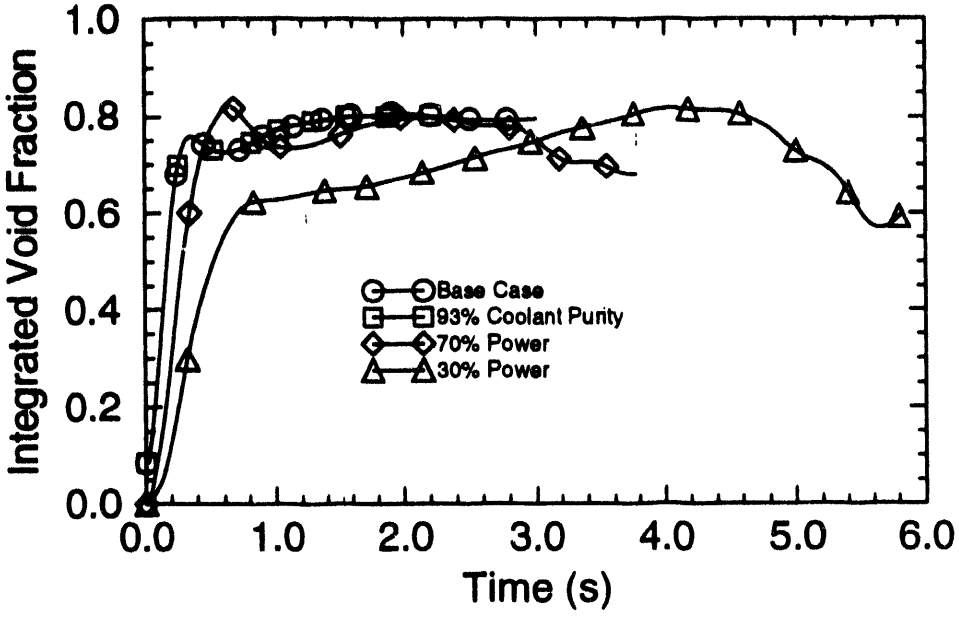


Figure 13 Integrated void fraction in CHAN1 for selected coupled calculations without scram.

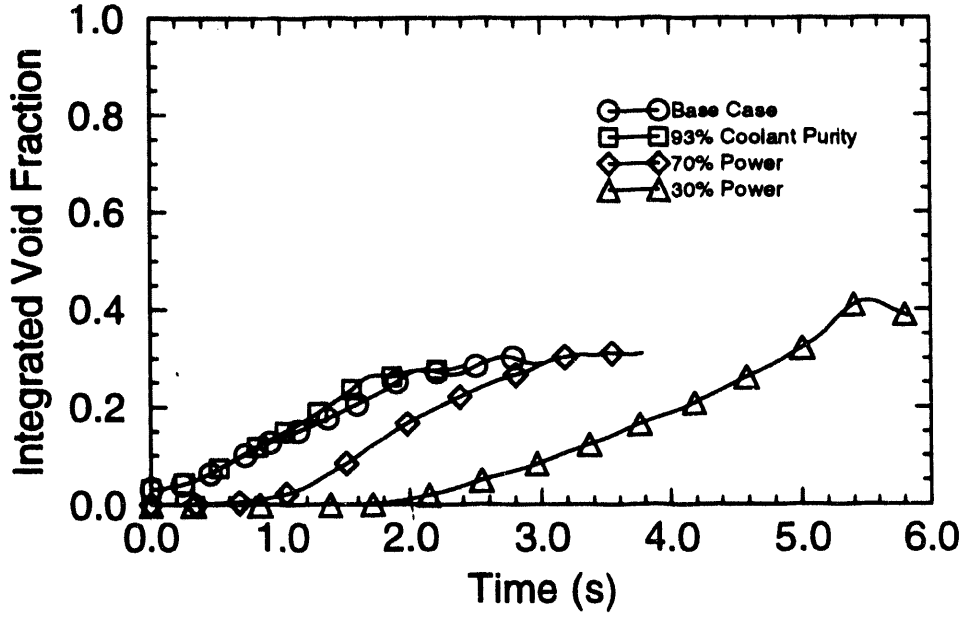


Figure 14 Integrated void fraction in CHAN2 for selected coupled calculations without scram.

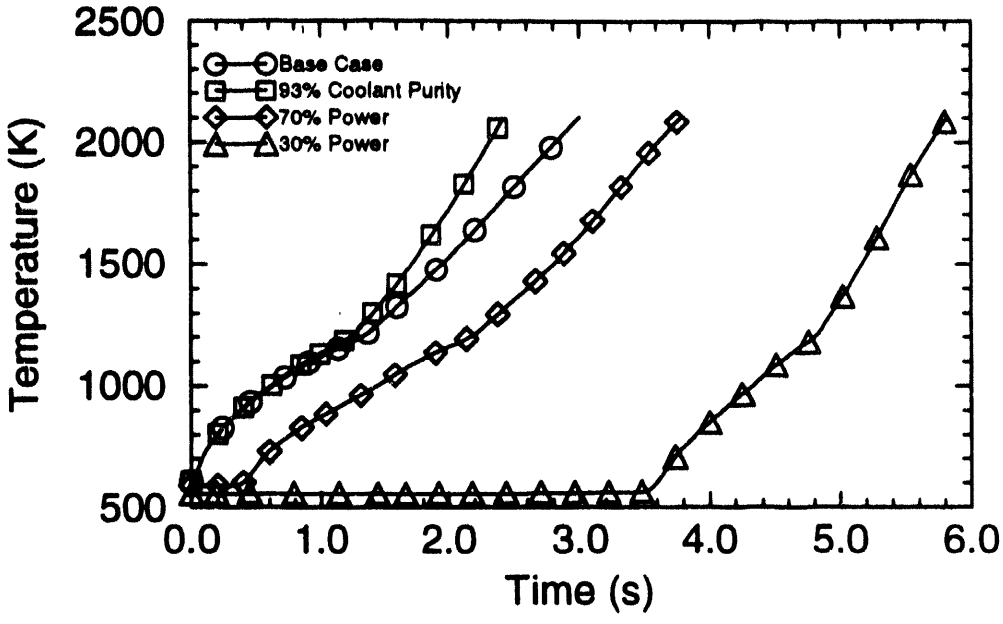


Figure 15 Peak cladding surface temperatures for selected coupled calculations without scram.

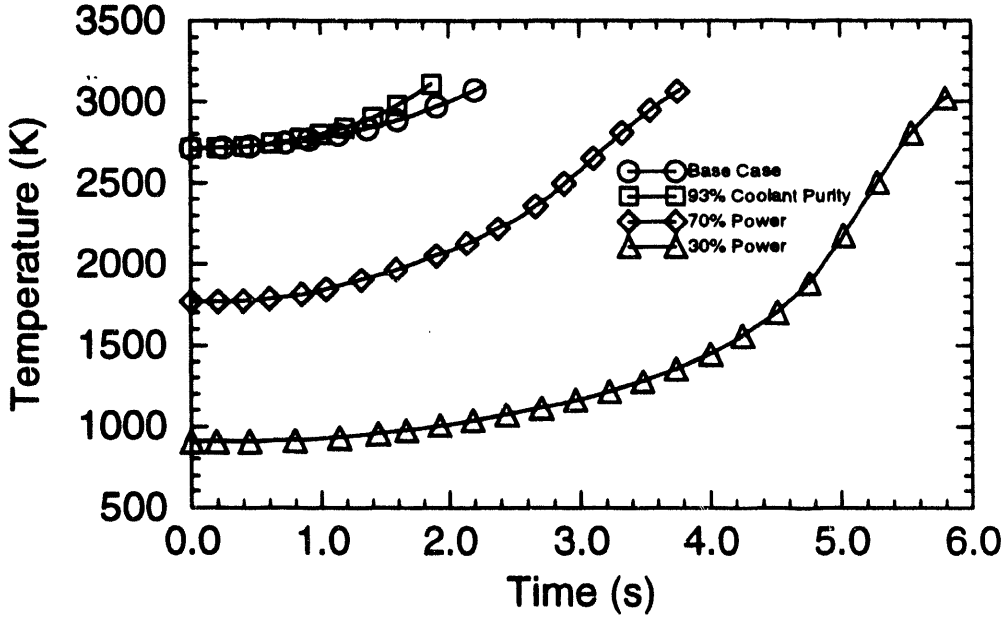


Figure 16 Peak fuel centerline temperatures for selected coupled calculations without scram.

3.2 Rod Withdrawal Calculation

The models and calculational sequence described in Section 2 were used to perform an anticipated transient without scram calculation and assess the performance of the core during this type of event. The reactor is initially at 103% full power with a 6% power tilt. The event was initiated with an instantaneous withdrawal of a single adjuster rod worth approximately 3 cents of reactivity. The calculation stopped at 32.5 seconds.

Figure 17 shows the normalized power of the core during the calculation. The power is still increasing at 32.5 seconds and this is due to the fact that reactivity is still positive as shown in **Figure 18**. Reactivity is still positive due to the positive void reactivity. The reduction in reactivity from 3 to 15 seconds appears to be primarily due to the reduction in void fraction over that period and secondarily due to the increase in fuel temperature. The void fraction increases initially due to the rapid power rise resulting from the rod withdrawal. The reactivity is essentially constant after 15 seconds even though fuel temperature continues to rise because the doppler reactivity feedback is small compared to the void reactivity. This calculation was performed, assuming no reactor trips, to investigate the response of the core to small positive reactivity insertions at full power. Additionally, the reactivity insertion was performed instantaneously for this calculation, but in reality would have taken a second or so in the real reactor. If trips were allowed, the reactor would have tripped on overpower.

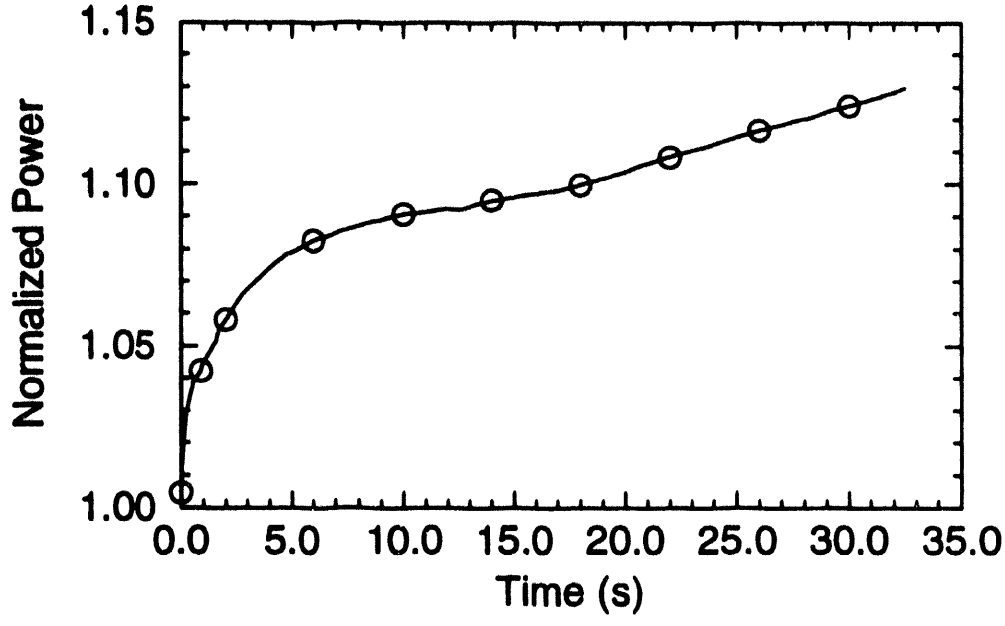


Figure 17 Normalized power versus time for the ATWS calculation.

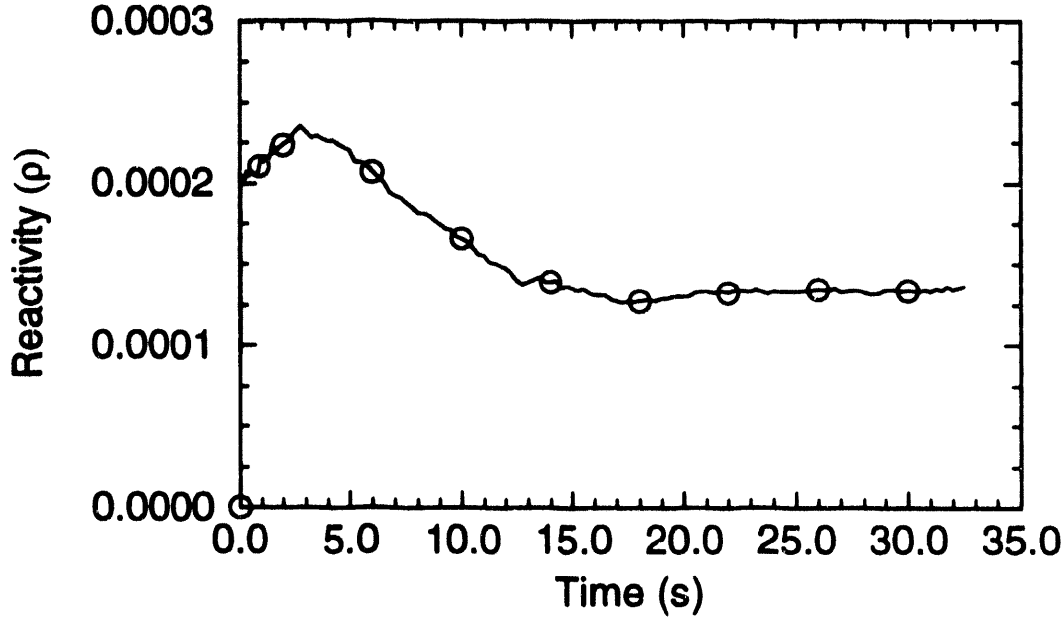


Figure 18 Reactivity versus time for the ATWS calculation.

4. Uncoupled Calculational Results

Calculations were performed with CATHENA only by using an input power history curve. The large-break LOCA was run with both the four and ten channel core models with the Emergency Core Cooling system described in Section 2.4. In addition, the small-break LOCA was run with a 0.76% inlet header break with the four channel core model.

4.1 Break with the Four Channel Model

A 100% large-break LOCA and 0.76% small-break LOCA calculation were undertaken with CATHENA. The input power rise for the large-break LOCA was similar to the previously large-break LOCA base case with scram, but the peak was higher. There was no power rise for the small-break LOCA since voiding occurs slowly. The small-break LOCA was assumed to occur during a loss of off-site power. When the outlet header pressure falls to 6 MPa, a LOCA signal trip occurs which results in turbine unloading, steam dump valves opening and activation of the Emergency Core Cooling system. Turbine unloading is modeled by ramping up the flow resistance in the steam line. The main steam safety valve opening lowers the saturation temperature of the secondary side of the two steam generators and causes more rapid cooling of the primary fluid. The main steam safety valve opening time is 30 seconds. Low primary pressure causes rupture discs to break in the Emergency Core Cooling lines. The discs are modeled between cells 2 and 3 in both the inlet and outlet header Emergency Core Cooling lines. When the pressure in cell 3 is 0.35 MPa less than the pressure in cell 2 the rupture discs fail. Emergency Core Cooling enters the primary loop just prior to 20 seconds for the large-break LOCA and 500 seconds for the small-break LOCA. In both cases the fuel cladding heats up. It rises by less than 100 degrees Kelvin before the Emergency Core Cooling is able to quench the fuel. **Figure 19** shows the large-break LOCA cladding temperature results. Because the break is in inlet header 2, channel 2 has a strong negative flow and kept cool. The flow in its companion channel, channel 4, stagnated and a temperature rise results.

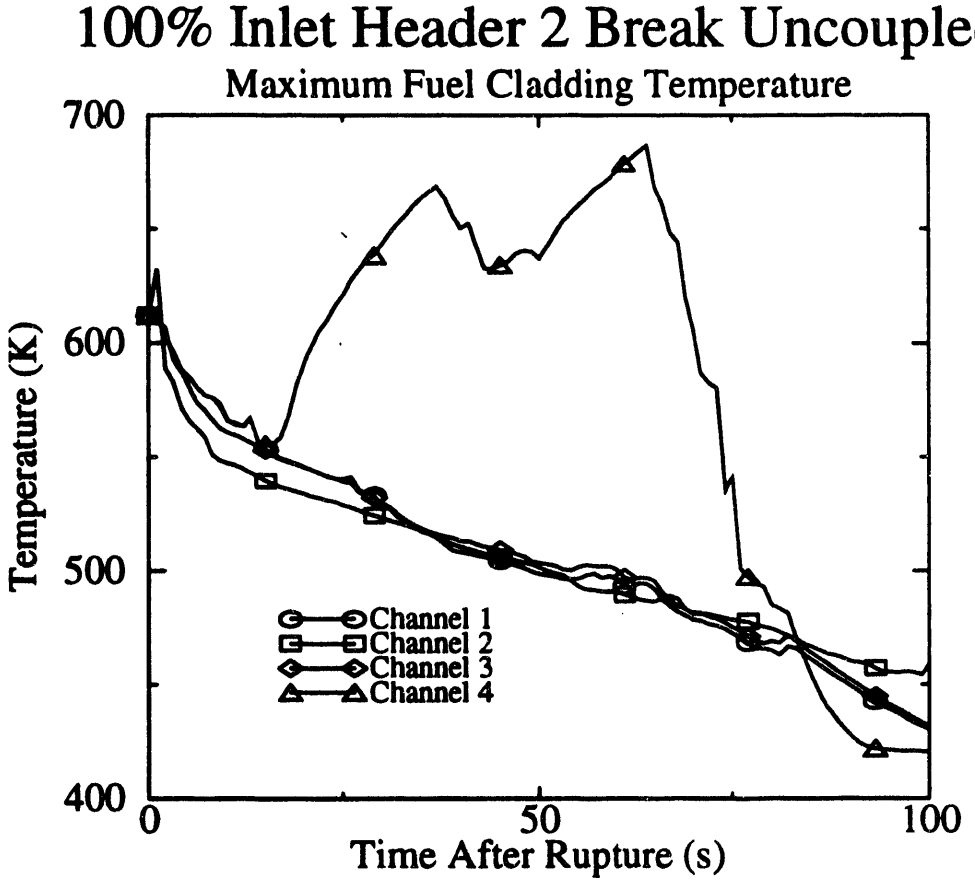


Figure 19 Four Channel Model LBLOCA Maximum Cladding Temperature

4.2 Large-Break LOCA with the Ten Channel Model

The ten channel model had a non-flat radial power profile which affected the cladding temperature heatup differently than the four channel model. The highest powered channel had a departure from nucleate boiling shortly after the break. A temperature rise of about 900 degrees Kelvin occurred as shown in **Figure 20**. By the time Emergency Core Cooling entered the channels, the cladding is in stable film boiling and it is difficult to re-wet. The temperature rise would be large enough to make the cladding go through the alpha-beta phase change, thereby lowering the strength of the cladding.

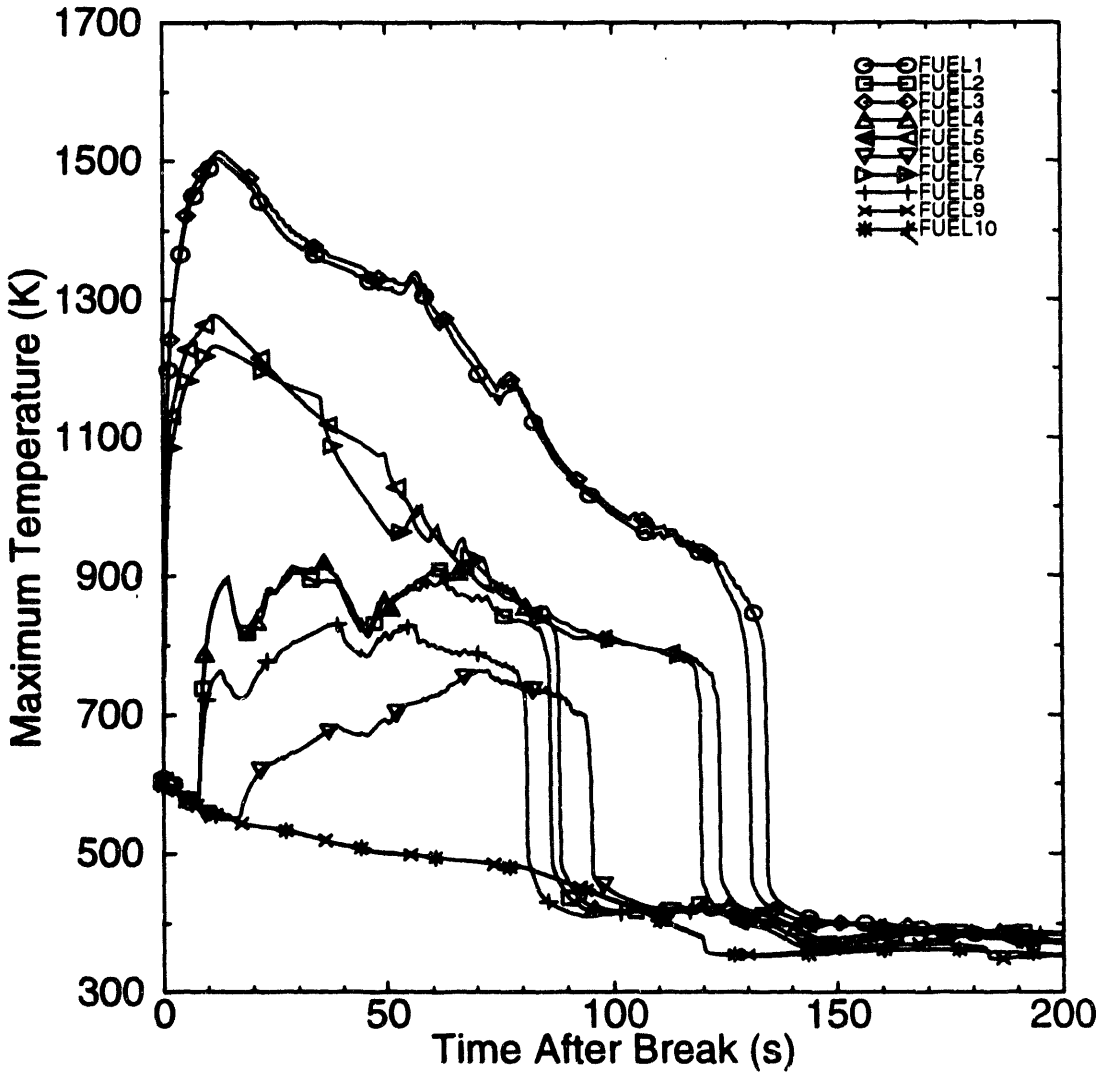


Figure 20 Ten Channel Model LBLOCA Maximum Cladding Temperature

5. Conclusions

All the calculations that invoke the actuation of the Emergency Core Cooling System were performed using CATHENA as a stand-alone code. That is, precalculated (by AECL) power evolutions were input to CATHENA rather than coupling it to the other codes in the code suite (e.g., CERBERUS). The power evolution is similar to that given in Reference 2 for a large-break LOCA with shutdown on rods only. Calculations performed for the large-break LOCA with shutdown show that the Emergency Core Cooling System is actuated after about 20 seconds. The large-break LOCA transients were run using two different input models: a four-channel and a ten-channel model. Significant calculational differences were produced by the two input models because of radial peaking and differences in power to flow. For the four-channel model, there is a 100 K increase in the maximum cladding surface temperature, whereas for the ten-channel model there was a 900 K rise. These results demonstrate the need for additional side calculations when the four-channel model is used (these are called 'slave model' calculations by AECL.

Calculations of a small-break LOCA (0.76% break in inlet header No.2) with shutdown were made using the four-channel model only. Results show that the Emergency Core Cooling System is actuated prior to 500 seconds in this case. Even though the scram signal is actuated later, there is a negligible power rise before scram and only a small increase in the maximum cladding surface temperature. Based on the results cited above for a large-break LOCA, the ten-channel small-break model may result in larger increases in the maximum temperature rise. The adequacy of the four-channel model for this class of accidents should also be assessed.

A rod withdrawal calculation with failure to shutdown shows that the CANDU 3 reactor may have a positive power coefficient above 105% because the power is continuing to increase beyond this level. Negative Doppler feedback compensates for about half of the positive reactivity inserted by the rod and other positive feedbacks. Reactivity feedback mechanisms have different magnitudes and time responses in the CANDU 3 design than in light water reactors.

The base-case large-break LOCA with failure to shutdown leads to fuel or cladding melting temperatures within a few seconds due to the positive void coefficient of reactivity. This is true even when lower, more realistic initial fuel temperatures are taken into account, delaying the time to melt by only about one to two seconds. Beyond this time, the calculations were not considered to be valid because the core geometry would begin to change and the code models would not apply. A severe accident analysis of this degraded-core scenario is beyond our capability at this time. NRC codes like MELCOR have not yet been modified for CANDU reactor analysis.

A sensitivity analysis with delayed shutdowns of up to about one second in the scram initiation, shows that there is negligible fuel melting and cladding failure. Also for nominal shutdown times, but with very degraded coolant purity (most positive-void reactivity), there is negligible fuel melting and cladding failure. For cases with failure to shutdown, the analysis shows that the end result of fuel or cladding melting is the same, and variations in parameters yield only small changes in the timing of the events.

The severity of the accident is dramatically reduced when it is assumed that one of the two independent shutdown systems function as designed. The results presented in this paper are consistent with related studies performed by AECL[1] and others[2], and do not reveal any new characteristics or phenomena.

6. References

1 "EXTERNAL ANALYSIS REPORT - Power Pulse Break Survey Analysis," AECL 74-03310-AR-001, Revision 0, October 10, 1991.

2 "Analysis of the Consequences of Failure to Shutdown Following a Large Loss of Coolant Accident in a Pickering NGS A Unit", Prepared by the Nuclear Studies and Safety Department and Civil Design Department of Ontario Hydro, October 1987, and "Assessment of Early Disruption Events during a Postulated Power Excursion Accident in Pickering a CANDU Reactor", ANL/RAS-OH-1, September 1987.

3 B. N. Hanna, "CATHENA MOD3.2n Theoretical Manual," AECL Research, THB-CD-002, November 1989.

4 E.S.Y. Tin and D.B. Miller, "Powderpufs-V Physics Manual," TDAI-31 Part 1 of 3, July 1979.

5 B. Rouben, "MATMAP Program Description," TDAI-318, October 1984

6 A.R. Dastur, B. Rouben and D.B. Buss, "CERBERUS - A Code for Solving the Space-Dependent Neutron Kinetics Equations in Three Dimensions," TTR-392, February 1992.

7 "ECCS Performance Analysis for Breaks in Large HTS Piping", Project 74 CANDU 3, AECL 74-68500-AR-001, Revision 1, March 3, 1993.

DATABASE AND MODELING ASSESSMENTS OF THE CANDU 3, PIUS, ALMR, AND MHTGR DESIGNS

Donald E. Carlson and Ralph O. Meyer
U. S. Nuclear Regulatory Commission

ABSTRACT

As part of the research program to support the preapplication reviews of the CANDU 3, PIUS, ALMR, and MHTGR designs, the NRC has completed preliminary assessments of databases and modeling capabilities. To ensure full coverage of all four designs, a detailed assessment methodology was developed that follows the broad logic of the NRC's Code Scaling, Applicability, and Uncertainty (CSAU) methodology. This paper describes the methodology of the database assessments and presents examples of the assessment process using preliminary results for the ALMR design.

INTRODUCTION

The Nuclear Regulatory Commission (NRC) has been conducting preapplication reviews of the CANDU 3, PIUS, ALMR, and MHTGR designs. CANDU 3 (Canadian Deuterium Uranium Model 3) is an evolutionary heavy water reactor design submitted by Atomic Energy of Canada Limited through its U.S. affiliate, AECL Technologies; PIUS (Process Inherent Ultimate Safety) is an innovative pressurized water reactor design submitted by ABB Combustion Engineering; ALMR (Advanced Liquid Metal Reactor), also called PRISM (Power Reactor Innovative Small Module), is a metal-fueled, sodium-cooled fast reactor design submitted by the U.S. Department of Energy; and MHTGR (Modular High-Temperature Gas-Cooled Reactor) is a graphite-moderated, helium-cooled reactor design also submitted by the U.S. Department of Energy.

The preapplication reviews of the four designs are aimed at identifying key technical areas and policy issues that will have to be addressed for standard design certification. Among the research tasks associated with these preliminary reviews is the assessment of databases and modeling capabilities needed for design confirmation. To ensure full coverage of all four designs, a detailed assessment methodology has been developed. This paper describes the database assessment methodology that has been applied to all four designs.

OBJECTIVE

The objective of the assessment work for each design is to provide an early identification and prioritization of areas where further development of databases and computational models may be desirable in preparing for NRC's confirmatory analyses. Early planning can be especially important where establishment of a confirmatory database entails constructing or modifying a major test facility. In addition, the preliminary assessment work provides

background information for NRC's future design certification review activities. Such background information is most directly useful for evaluating the licensing adequacy of the vendor's databases and models.

The essential question addressed by the database and modeling assessments is:

> "What additional work is needed to have databases and computational models for these advanced reactors comparable to those for current light water reactors?"

The question regarding databases encompasses data available to the applicant as well as to the NRC. Should any major gaps be found in the databases for licensing analysis, these would generally have to be filled by the applicant. Areas where database coverage is sparse or where additional confidence is needed may warrant confirmatory work by the NRC. This assessment does not attempt to determine who should bear responsibility for generating any additional data. The question regarding computational models, however, addresses only the NRC's independent audit codes. Information from the modeling assessments will be used to plan NRC's code development efforts.

ASSESSMENT METHODOLOGY

Because database development potentially requires longer term planning than does the development of computational models, the major emphasis of this work is placed on providing an early assessment of databases. A rather formalized process is therefore used in assessing databases, whereas potential areas for modeling enhancements are assessed in a more ad hoc manner for this preliminary review stage.

The structure of the database assessment process follows the broad logic of the NRC's CSAU (Code Scaling, Applicability, and Uncertainty) methodology, which is described in Reference 1. Accordingly, the assessment process addresses *designs*, *scenarios*, *phenomena*, and *data* in that order. In contrast to the CSAU methodology itself, however, the database assessment process is not linked to particular codes or models. While most data are ultimately used for validating the models and methods of code-aided analyses, important exceptions exist, such as certain data used directly for ECCS (Emergency Core Cooling System) criteria and SAFDLs (Specified Acceptable Fuel Design Limits).

The database assessment process is designed to ensure that all important phenomena are covered. It is applied to each of the four designs as described in the following five steps:

1. Select and list, for each reactor design, a set of representative event scenarios that exercises a broad range of important phenomena for that design.

2. For each representative event sequence, identify the important phenomena that should be modeled to predict the scenario's progression and consequences.

3. Generate a list of data types and ranges that, if available, would be useful for confirming the modeling of phenomena identified in the previous step.

4. Generate a set of tables indicating whether, and to what extent, the types and ranges of data identified in the previous step are included in the existing and planned databases identified by the vendor.

5. List and comment on those data types not covered by existing or planned databases where additional data would be most helpful toward confirming important safety characteristics of the design.

The above five-step process is described in greater detail in the following subsections. Preliminary assessment results for the ALMR design are presented to provide examples of the assessment process.

Step 1. Selection of Representative Scenarios

Once a reactor design has been defined, the first step in the database assessment process is to select a set of representative scenarios that exercises a broad range of important phenomena for that design. These representative scenarios are selected from event sequences identified in the NRC's draft preliminary safety evaluation reports (PSERs) for the ALMR (Reference 2) and MHTGR (Reference 3) and in the recently completed NRC systems studies for CANDU 3 (Reference 4) and PIUS (Reference 5).

During the evolution of the CANDU 3 and PIUS systems studies, a scheme of scenario categories was developed by the NRC research staff. In addition to initiating frequencies, this scheme also considers failures of components or systems, as well as operator errors. References 4 and 5 provide further details of the scheme. Using this scheme, event scenarios are grouped into the four event categories (ECs) described below:

EC-I	Event sequences that would be expected to occur one or more times during the life of a plant.
EC-II	Event sequences that would be expected to occur once over the lifetime of a population of reactors.
EC-III	Less likely event sequences that would be analyzed for source terms and containment challenges.
EC-IV	Extremely unlikely event sequences which nevertheless may have potential consequences that merit their consideration in the design.

Such categories are important in evaluating the nature and relative importance of associated data and modeling needs. The above frequency categories also have some bearing on whether conservative or best-estimate calculations are to be used in the safety analyses.

The PSERs for the ALMR and MHTGR used a somewhat different categorization scheme that closely parallels the four event categories described above. For the database assessment process, it is not essential which of the scenario classification schemes is used, as long as the broad spectrum of phenomena to be modeled is covered.

Table 1 lists a preliminary set of representative scenarios for the ALMR design. In this example, representative scenarios are identified for EC-II, EC-III, and EC-IV. EC-I scenarios would generally be included as well, but are not present in this case because their key phenomena were found to be bracketed by those of EC-II. This case is also somewhat atypical in that the contractor performing the preliminary assessment for the ALMR listed ten representative scenarios in EC-III. For the other three reactor designs, it was more typically found that two to five scenarios per category suffice to represent the broad range of key phenomena for the important sequences in that category.

As an intermediate step, it is often helpful to cross-reference the relative importance of phenomena and components with scenarios. Table 2 shows an example of such a cross-referencing for the ALMR design in the phenomenological area of reactor physics.

Step 2. Identification of Key Phenomena and Parameter Ranges

The second step in the assessment process is to identify and list, for each representative scenario, the major phenomena that must be modeled to predict the scenario's progression and consequences. Where appropriate, the ranges of important state variables and other parameters (e.g., dimensions, material characteristics, etc.) that affect each phenomenon are also specified.

The key phenomena are grouped in up to ten phenomenological areas, with one list being generated for each area. For water-cooled reactors, the ten areas would be:

1. Reactor Physics
2. Thermal Hydraulics
3. Fuel Behavior and Core Melt Progression
4. Fuel-Coolant Interactions
5. Reactor Vessel Failure
6. High-Pressure Melt Ejection
7. Core-Concrete Interactions
8. Hydrogen Combustion
9. Fission Product Release and Transport
10. Containment Failure.

In general, no more than four of these areas (1, 2, 3, and 9) may come into play in scenarios of EC-I or EC-II, whereas all ten may arise in EC-III or EC-IV scenarios.

Table 3 is a preliminary listing of important phenomena for the ALMR design in the five phenomenological areas of Reactor Physics, Thermal Hydraulics, Fuel Behavior and Core Melt Progression, Fission Product Release and Transport, and Containment Failure.

Step 3. Identification of Hypothetical Data Types Useful for Confirming Key Phenomena

The third step in the assessment process is to identify data types or measurements that, if available, would be useful for confirming the modeling of the important phenomena. These hypothetical data types should consist of separate-effects data for "bottom-up" confirmation of individual key phenomena as well as integral data for "top-down" confirmation of important interactions between phenomena. Where possible, the data types should be described in terms of specific measurements, indicating the types of facilities that would be needed for conducting such measurements. The listing of these data types is incorporated in the table for Step 4.

Step 4. Existence of Data Types for Key Phenomena and Phenomena Interactions

Once the useful types of separate-effects and integral data have been identified, the forth step in the assessment process is to generate a set of tables indicating whether, and to what extent, the data types are included in the existing and planned databases identified by the vendor. Table 4 provides a preliminary example of such a table for the ALMR design in the area of reactor physics.

Step 5. Listing of Data Types Not Covered by Existing or Planned Databases

The final step in the database assessment process is to list and prioritize those data types not covered by existing or planned databases where additional data would be most helpful toward confirming important safety characteristics of the design. An example is shown in Table 5, which is a listing of high-priority data types not covered by existing or planned data for the ALMR. This example reflects the contractor's preliminary assessment that, while certain interactions of phenomena may be adequately addressed by the applicant's plans for integral testing of the prototype, there appears to be a shortage of separate effects tests for modeling individual phenomena.

DISCUSSION

Application of the database assessment methodology has been completed in draft form for all four reactor designs. The assessment work was comprised of tasks in six NRC research contracts at five national laboratories. Major contributors from the laboratories and the areas of their assessment contributions are indicated in the Appendix.

In addition to database assessments, the completed draft reports for the four designs also include preliminary assessments of NRC modeling capabilities. An example of the modeling assessment results is shown in Table 6, which is a listing of suggested areas where NRC code enhancements would be useful in modeling important ALMR phenomena.

The draft database and modeling assessment reports for PIUS, MHTGR, and ALMR are being maintained in the respective NRC project files for future reference. The research contracts for those three designs were recently curtailed in accordance with SECY-93-104 (Reference 6).

The vendor of the CANDU 3 design, on the other hand, has announced its intention to proceed with a formal application for design certification in 1994. Database and modeling assessment results for CANDU 3 will be finalized and published in the near future.

REFERENCES

1. B. Boyack, R. Duffey, et. al., "Quantifying Reactor Safety Margins: Application of the Code Scaling, Applicability, and Uncertainty Methodology to a Large Break Loss of Coolant Accident," NUREG/CR-5249, EGG-2552, October 1989.

2. R. R. Landry, T. L. King, J. N. Wilson, "Draft Preapplication Safety Evaluation Report for the Power Reactor Inherently Safe Module Liquid Metal Reactor," U. S. Nuclear Regulatory Commission Report, NUREG-1368, September 1989.

3. P. M. Williams, T. L. King, J. N. Wilson, "Draft Preapplication Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor," U. S. Nuclear Regulatory Commission Report, NUREG-1338, March 1989.

4. J. R. Wolfgong, M. A. Linn, A. L. Wright, M. Olszewski, M. H. Fontana, "Systems Analysis of the CANDU 3 Reactor," NUREG/CR-6065, ORNL/TM-12396, Oak Ridge National Laboratory, July 1993.

5. R. Fullwood, P. Kroeger, J. Higgins, R. Youngblood, H. Cheng, G. Martinez-Guridi, G. Van Tuyle, W. Shier, R. Morante, P. Soo, "Integrated Systems Analysis of the PIUS Reactor," NUREG/CR-6111, BNL-NUREG-52393, Brookhaven National Laboratory, November 1993.

6. J. M. Taylor, paper for the NRC Commissioners, "Program Analysis and Recommendations Concerning the Nuclear Regulatory Commission (NRC) Reviews of the Advanced Reactor (PRISM, MHTGR, and PIUS) and CANDU 3 Designs," SECY-93-104, April 20, 1993.

Table 1. Representative Scenarios for ALMR Database Assessment

EVENT CATEGORY	SCENARIO DESCRIPTION
EC-II	Uncontrolled single rod withdrawal at 100% power
	Loss of normal shutdown cooling
EC-III	Unprotected loss of primary flow and IHTS cooling (ULOF)
	Unprotected control rod withdrawal (UTOP)
	Unprotected loss of IHTS cooling (ULOHS)
	Inadvertent withdrawal of all control rods without scram for 36 hr (one module) with normal cooling
	Inadvertent withdrawal of all control rods without scram for 36 hr with RVACS cooling only
	Station blackout (all modules) for 36 hr with scram
	Complete loss of decay heat removal for 12 hr, followed by 25% unblockage of RVACS
	Unprotected loss of flow, loss of heat sink, with seizure of one EM pump
	Rupture of steam generator tubes with failure to isolate or dump water from steam generator
	Flow blockage of a single fuel assembly
EC-IV	Unprotected loss of primary flow with loss of coast down on all EM pumps
	Major core flow blockage

Table 2. Representative Cross Referencing of Phenomena and Components in the Area of ALMR Reactor Physics

PHENOMENA AND COMPONENTS	SCENARIO													
	EC-II		EC-III										EC-IV	
	1	2	1	2	3	4	5	6	7	8	9	10	1	2
Reactor Physics														
1. Passive Shutdown	4	1	5	5	5	5	5	1	1	5	1	5	5	5
2. Bowing	3	2	3	5	4	5	5	1	1	5	1	4	5	5
3. Control Drive Line Expansion	3	1	5	5	5	5	5	1	1	5	1	4	5	5
4. Excess Reactivity	3	0	4	4	4	4	4	1	1	4	1	4	4	4
5. GEM Reactivity Worth	0	1	5	2	3	2	5	1	1	5	1	3	5	3
6. Sodium Void Worth	0	0	2	2	2	2	2	1	1	2	1	5	5	5
7. Spatial Kinetics	pt	pt	pt	pt	pt	pt	pt	pt	pt	pt	pt	3D	3D	3D

pt - Point kinetics
3D - Three-dimensional spatial kinetics needed
0 - Not required
1 - Possibly required, but expect minor contribution
2 - Potentially of interest, depending on scenario details
3 - Component should be modeled or phenomena understood
4 - Important component or phenomenon
5 - Dominant component or phenomenon

Table 3. Representative List of Important ALMR Phenomena

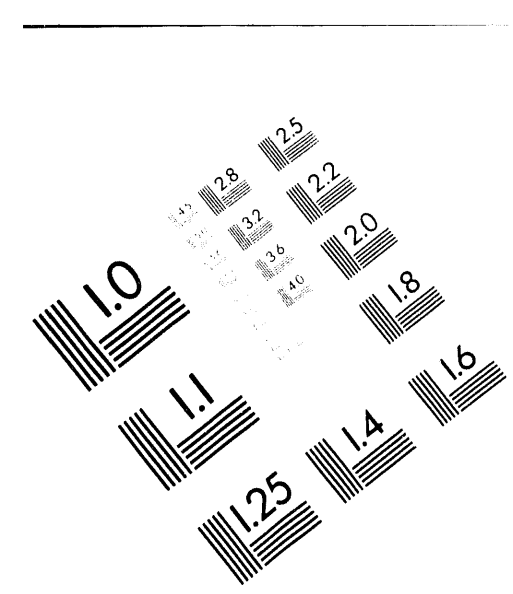
REACTOR PHYSICS
- Passive Shutdown Worths
- Bowing Worth
- Control Drive Line Expansion Worth
- Excess Reactivity
- GEM Reactivity Worth
- Sodium Void Worth
- Spatial Kinetics

THERMAL HYDRAULICS
- Sodium and Water Mixing
- Two-Phase Sodium
- Electromagnetic Pumps
- Multi-Dimensional Upper Plenum
- Reactor Vessel Auxiliary Cooling
- Upper Plenum Level Tracking
- Auxiliary Cooling System
- Gas Expansion Modules
- Thermal Expansion of Structures
- Natural Circulation Model
- Forced Circulation Model
- Balance of Plant Model
- Fuel Assembly Heat Transfer
- Intermediate Heat Transport System

FUEL BEHAVIOR AND CORE MELT PROGRESSION
- Ternary Fuel Properties
- Fuel Swelling
- In-Pin Fuel Melting
- Fuel Melt Dispersal
- Fuel-Clad Mechanical Interaction
- Fuel-Clad Chemical Interaction
- Clad Eutectic Penetration
- Fuel Axial Conduction
- Fuel Length Effects
- Core Melt Composition
- Clad and Duct Performance
- Fuel Failure Non-Propagation
- In-Vessel Debris Coolability

FISSION PRODUCT RELEASE AND TRANSPORT
- Fission Product Retention in Na Pool
- Fission Product Retention in Burning Na Pool

CONTAINMENT FAILURE
- Containment Loading
- Containment Integrity



Association for Information and Image Management

1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910
301/587-8202

2 of 7

Table 4. Representative Tabulation of Existing and Planned Databases for ALMR Reactor Physics Phenomena

PHENOMENA	EXISTING DATA	PLANNED	COMMENTS
Passive Shutdown Worths	1. EBR-II Demonstration test (1986)[1] 2. ZPPR-15 (April 1985)[2] 3. FFTF behavior for oxide core[3]	1. EBR-II Demonstration with Recycled Fuel in Phase III 2. Demonstrated in the Prototype Tests	ZPPR test not prototypical of ALMR, but used metal fuel.
Control Rod Drive Line Thermal Expansion Worth	No direct data. Inferred from EBR-II and FFTF transients, and SASSYS analysis	Overall Effect to be demonstrated in the Prototype	The exact drive line and UIS for the ALMR not chosen. Function of control rod position.
Bowing Worth	No direct data.	Unknown	The extent of this effect should be quantified by a test program.
Excess Reactivity	No data	1. EBR-II demonstration with Recycled fuel in Phase III 2. Prototype control stop setting would supply data	Recycled actinides and fuel length (strain) swelling increases TOP initiator.
GEM Reactivity Worth	1. FFTF proof of principle Tests (1986)[4] 2. FFTF Pump Restart Test (1989)[3] 3. ZPPR-15 Test (April 1985)[2]	1. Prototype operation	Enough data have been collected for the Proof of Principle. Reliability Issues remain.
Void Worth	1. ZPPR-15 Test (April 1985)[2]		Probably could estimate from code predictions. Coherent and incoherent sodium boiling issues remain.

[1] H. P. Planchon, et al., 1987; [2] H. F. McFarlane, et al., 5/88; [3] R. A. Harris, et al., 4/92; [4] L. R. Campbell, et al., 6/87

Table 5. Representative Listing of ALMR Data Missing and Not Planned for Reactor-Physics and Thermal-Hydraulics Phenomena

MISSING DATA	COMMENTS
Doppler Reactivity	Critical experiments in ZPPR could isolate the worth of this phenomenon, which is crucial to the passive shutdown mechanism.
Axial Expansion Reactivity	Critical experiments in ZPPR could isolate worth as a function of burnup, recycled material content, and with/without clad lockup.
Channel Bowing Reactivity	Critical experiments in ZPPR could isolate worth as a function of diameter increase at several axial positions for the BOL and EOL equilibrium fuel cycle.
Ch. Bowing Mechanical Interaction	Separate effects test to determine the mechanical interaction of several channel ducts with electrical heaters. GEM impact evaluated. Qualification for the NUBOW-3 code.
Sodium Void Worth	ZPPR critical experiments to quantify the sodium void worth at BOL and EOL for the equilibrium fuel cycle. A bubble tube could be placed in the lower plenum of the Prototype to bubble gas through the core.
Fuel Full-Length Effect	FFTF experiments with prototypical fuel to evaluate fuel slumping (before clad lockup), porosity link development to the gas plenum, and difference in fuel/mechanical interactions for the equilibrium life cycle.
GEM Reliability	Out-of-reactor aging experiments for GEM reliability data and potential failure mechanisms.
Synchronous Motor Variations	Determine range of V-A delivered by hardware and its impact on the coast down. Evaluate aging effects.
Control Drive Th. Expansion	Out-of-reactor tests to validate the thermal expansion of the control rod drive.
Upper Internal Structure	Separate effects tests to demonstrate the flow patterns and temperature profiles along the control rod drive lines during off-normal conditions.

Table 6. Representative Listing of Areas for Enhancement of ALMR Modeling by NRC Audit Codes

MODEL	COMMENT
RVACS	The SSC code has been iterating with the MINET (sub code of SSC) code to model this effect. A model should be added to SSC for the design certification review.
EM Pump	The coast down effect has been determined in the MINET model and programmed in SSC. An EM pump should be added to SSC to increase the range of transients that the code can model.
Two EM Pump Loops	For core inlet pipe breaks and the sudden loss of a single EM pump, two loops are required to be modeled.
Sodium Level Tracking	A model to describe the upper plenum sodium overflow of vessel liner should be added to evaluate long term heatup cases.
Two-Phase Sodium	A two-phase sodium model is needed in the core region to evaluate the effects of sodium voiding during several scenarios.
Bowing Reactivity Feedback	A model to represent the bowing feedback in the limited free bowing arrangement of the ALMR is required for analysis of ATWS events.
Multi-Dimensional Upper Plenum	The upper plenum of the ALMR needs an accurate upper plenum model to determine thermal expansion of the vessel, control rod drive lines, and sodium.
Fuel Axial Conduction	The high thermal conductivity of metal fuel requires that axial conduction be considered.
3-D Spatial Kinetics	A 3D kinetics model is needed in several scenarios to determine the local feedback power levels associated with voids.
Auxiliary Cooling System	The heat rejection of the steam generator should be added to model operational events.
Source Term	VICTORIA would have to add additional elements and chemical species to cover the ALMR.

APPENDIX

Application of the database assessment methodology described in this paper has been completed in draft form for all four reactor designs. The assessment work was comprised of tasks in six NRC research contracts at five national laboratories. Major contributors from the laboratories and the areas of their assessment contributions are indicated below:

- Peter G. Kroeger; Reactor Physics, Thermal Hydraulics, Fuel and Fission Product Behavior, and Severe Accidents for the MHTGR design; Contract L2213 at Brookhaven National Laboratory.
- Gregory C. Slovik; Reactor Physics, Thermal Hydraulics, Fuel and Fission Product Behavior, and Severe Accidents for the ALMR design; Contract L2205 at Brookhaven National Laboratory.
- Jerry L. Judd; Reactor Physics for the CANDU 3 design; Contract L2445 at Idaho National Engineering Laboratory.
- Rex W. Shumway and Calvin E. Slater; Thermal Hydraulics for the CANDU 3 design; Contract L2445 at Idaho National Engineering Laboratory.
- Donald L. Hagrman; Fuel and Fission Product Behavior for the CANDU 3 design; Contract L2445 at Idaho National Engineering Laboratory.
- Brent E. Boyack; Reactor Physics and Thermal Hydraulics for the PIUS design; Contract L2447 at Los Alamos National Laboratory.
- Anthony L. Wright; Severe Accidents for the CANDU 3 design; Contract L2225 at Oak Ridge National Laboratory.
- Brian S. Cowell; Severe Accidents for the PIUS design; Contract L2225 at Oak Ridge National Laboratory.
- Terence J. Heames; Source Terms for the CANDU 3 design; Contract L2227 at Sandia National Laboratories.
- Nathan E. Bixler; Source Terms for the MHTGR and ALMR designs; Contract L2227 at Sandia National Laboratories.
- Richard M. Elrick; Source Terms for the PIUS design; Contract L2227 at Sandia National Laboratories.

Assessing Functional Diversity by Program Slicing

Dolores R. Wallace James R. Lyle Keith B. Gallagher* Laura M. Ippolito

U.S. Department of Commerce
Technology Administration
National Institute of Standards and Technology
Computer Systems Laboratory
Gaithersburg, MD 20899

Abstract

A responsibility of the Nuclear Regulatory Commission auditors is to provide assessments of the quality of the safety systems. For software, the audit process as currently implemented is a slow, tedious, manual process prone to human errors. While auditors cannot possibly examine all components of the system in complete detail, they do check for implementation of specific principles like functional diversity. This paper describes an experimental prototype Computer Aided Software Engineering (CASE) tool, unravel, designed to enable auditors to check for functional diversity and aid an auditor in examining software by extracting all code relevant to a computation identified for detailed inspection.

1 Overview

The United States Nuclear Regulatory Commission (NRC) is responsible for licensing the use of safety systems for nuclear power plants in the United States. The safety systems in nuclear power plants are used to detect and mitigate unsafe operating conditions. As nuclear power plants are modernized, replacement of some analog components with digital components and software introduces new safety concerns.

New technology that is dependent on the use of programmed digital computers is being proposed for use in nuclear power plants. These components are proposed for both new construction and replacement of obsolete or worn out systems in older plants. Modern digital systems have many features that suggest their use in safety systems: self-diagnostic aids, on-line testing, high accuracy, drift-free operation, signal multiplexing, and the use of fiber optics. The use of computer software (programs) in these digital systems is a new and untested technological area. The nuclear power industry is facing the same problems in the development and assurance of software as other industries (e.g., avionics, medical devices) which rely on high integrity software. High integrity software is software that can and must be trusted to operate dependably in some critical function[18].

A responsibility of NRC auditors is to provide assessments of the quality of the safety systems. For software, the audit process as currently implemented is a slow, tedious, manual process prone to human errors. Guidance developed for NRC on software quality assurance provides some checklists that may be used during audits[17]. While these checklists apply to all software products, (e.g. the software requirements document, the software design specifications, user documentation, code, test, and other software assurance documentation), complete standards for producing and auditing high integrity software are not yet available. Draft standards and guidelines vary in their selection of best practices[15]. An investigation of software error analysis has shown that in general industry-wide error data (for any industry) is not sufficient to assist developers nor to alert auditors to the types of problems that may exist in the safety system under audit[13].

While auditors cannot possibly examine all components of the system in complete detail, they do check for implementation of specific principles like functional diversity and for absence of specific features like the capability for unintended functions to

*also at Loyola College in Maryland

occur. One approach for checking is to perform a thread audit, that is, to follow a selected set of inputs throughout the system.

Auditors need a mechanism to check software code for functional diversity. Section 2 describes the use of functional diversity in computer software and the need for automation for auditors to examine software for functional diversity and the absence of unintended functions. Section 3 describes a technique, program slicing, that may be used to examine code for functional diversity. Section 4 describes the technical basis supporting development of a prototype tool using slicing for NRC auditors. Sections 5 and 6 provide suggestions for potential applications of slicing to other software issues and summarizes the effort on the prototype.

2 Auditing for Diversity

While the commercial world is developing some tools and standards organizations are attempting to codify best practices for development and assurance, these tools and evolving standards may not be addressing the needs of auditors. Auditors have a difficult task in assessing software in safety systems. One partial solution may be to provide automated assistance to the auditors to assess software relative to one of the nuclear industry's principal concerns: functional diversity.

Functional diversity is a solution to protect against potential design faults. Categories of diversity include hardware diversity, process safety function diversity, and diversity of the internals of software computation. Often in safety systems a critical decision can be made from multiple criteria, calculated from several physical measurements. The NRC auditor needs to verify that each criterion is calculated independently and hence a single software fault can not corrupt more than one criterion. Functional diversity may also be employed by a single programmer or by different teams who code the same algorithm[6]. Within a software system, the same function may be programmed in more than one way, but eventually a voting mechanism within the system decides what output to accept. The value of functional diversity for computer software is debated in technical literature and various experiments have been conducted in attempts to find a valid approach. For software, the approach appears to be more to ensure that no two safety functions use the same paths from the input to a function to its output. Hence, an error for one critical function can in no way impact the output of another critical function. Auditor capability to verify functional diversity of critical software functions would be an asset in the licensing process of safety functions. In some instances, safety functions must share low level algorithms or code that is a potential source of common mode failure. The NRC auditor needs the ability to identify such practices so that attention can be focused on both the vendor's process and product.

As part of the licensing process, NRC auditors examine a safety system to ensure that it meets its functional and performance requirements and does not perform any other functions. For any input (e.g., pressure reading, temperature value) used by the software safety system, it is important to track the path of that input's value throughout the system and to demonstrate that common software does not exist for two computations whose functions are to be diverse. The tracking process enables a developer or auditor to observe precisely the behavior of a specific input. The observer can detect usage of code that was not anticipated for that input. This type of examination is referred to as a string check or thread audit. The auditors may manually apply this technique to examine the software. This manual audit process is slow, tedious, and prone to human errors. It is possible to build automated tools to aid NRC auditors so that they can avoid tedious, error prone, manual examination of source code.

The state of the art of software tools is such that NRC auditors should already have tools to help examine software. The National Institute of Standards and Technology (NIST) examined the status of commercially-available Computer-Aided Software Engineering (CASE) tools for the NRC and found that few of the CASE tools currently commercially available are suitable for use by auditors and that in general the functionality provided by CASE tools is generic, rather than specific, in analytic capability. In the first instance auditors would usually need the same tool and all the products of the developer. In the second instance, the user of the tool needs to do additional work to apply the tool's capability to conduct the specific type of analysis.

NRC auditors presently lack CASE capability for the support of safety evaluations including functional

diversity and string checks. Lack of such support means that some aspects of the evaluations are manually laborious and possibly inaccurate. Automation to support the auditors may relieve them of the error-prone, tedious effort and enable them to concentrate on the analytic aspects of safety evaluation.

3 Program Slicing

NIST is exploring a concept, called program slicing[19, 21], to provide support for the auditor tasks. The purpose is to allow auditors to examine source code and collect data about specific properties. While some tools allow study of program properties, these tools require extensive and time-consuming execution of the code; such a process is an unreasonable burden for an auditor.

Program slicing is a family of program decomposition techniques based on extracting statements relevant to a computation in a program. Program slicing produces a smaller program that reproduces a subset of the original program's behavior[21]. This is advantageous since the slice, by excluding irrelevant statements, can collect an algorithm for a calculation that may be scattered throughout a program. Program slices fit in with the way programmers understand programs since after trying to understand an unfamiliar program, programmers recognize slices from the program better than other chunks of code from a program[19]. It should be easier for a programmer interested in a subset of the program's behavior to understand the corresponding slice than to deal with the entire program. The utility and power of program slicing comes from the potential automation of tedious and error prone tasks. Program slicing has applications in program debugging[12, 19], program testing[5, 8, 9], program integration[4], software safety analysis[3], parallel program execution[20], and software maintenance[2]. Several variations on this theme have been developed, including program dicing[11], dynamic slicing[1, 7] and decomposition slicing[2].

3.1 Computing Program Slices

A program slicing algorithm must locate all statements relevant to a computation, specified by a program variable and a program location (statement). Together, the given statement and the given variable are known as the slicing criterion. A *slicing criterion* for a program slice is a tuple $< i, v >$ where i is a statement in the program and v is a subset of the program variables. A *program slice* of a program P for a given slicing criterion, $< i, v >$, is an executable program obtained by deleting zero or more statements from P such that the values of the variables in v are the same just before execution reaches statement i for both P and the slice on P.

The essence of a slicing algorithm is the following: starting with the statement specified in the slicing criterion, search the possible program flow backward, including in the slice any statement that assigns a value to a variable in the slicing criterion. When a statement is added to a slice, generate a new slicing criterion for the statement just added to the slice by deleting the variables that are changed by executing the statement from the original slicing criterion and adding any variables referenced by the included statement. A slicing algorithm must handle the following issues:

1. Expression statements
2. Compound control statements
3. Declared structures
4. Pointers
5. Dynamic structures
6. References to Structure Members by Pointer
7. Assignment to Structure Members by Pointer
8. Procedure Calls
9. Arrays
10. Unions
11. Goto statements
12. Multiple source files

By way of an example, this paper discusses the first two issues. Discussion of the other issues can be found in many sources.

To compute program slices on a source program it is first transformed into the more readily usable form of a flow-graph with nodes and directed edges. Nodes correspond to source program statements and edges represent execution flow. For a node corresponding to an assignment statement there is a single edge directed from the assignment statement node to the node corresponding to the statement that is executed next. For control statements, such as **if**, **while** or **switch**, there is an edge to each statement that could be executed next. The set of statements that could be executed after a statement is called the *successor set*. Each node of the flow-graph is annotated

```
 1  main()
 2  {
 3      int red, green, blue, yellow;
 4      int sweet,sour,salty,bitter;
 5      int i;
 6
 7      red = 1;
 8      blue = 5;
 9      green = 8;
10      yellow = 2;
11
12      red = 2*red;
13      sweet = red*green;
14      sour = 0;
15      i = 0;
16      while ( i < red) {
17          sour = sour + green;
18          i = i + 1;
19      }
20      salty = blue + yellow;
21      yellow = sour + 1;
22      bitter = yellow + green;
23
24      printf ("%d %d %d %d\n",
25          sweet,sour,salty,bitter);
26      exit(0);
27  }
```

Figure 1: Slicing Example Program

by a *def* set, the variables that may receive a new value when the statement is executed and a *ref* set, the variables whose values are used during execution of that statement.

To locate the statements that influence the value of variable v just before execution reaches statement m we would compute a program slice for the criterion $< m, v >$. For expression statement n, where m is a successor of n, the *defs(n)* set and the slicing criterion determines if an expression statement is included in a slice.

$$S_{<m,v>} = \begin{cases} S_{<n,v>} & \text{if } v \notin \text{defs(n)} \\ \{n\} \cup S_{<n,x>} \forall x \in \text{refs(n)} & \text{otherwise} \end{cases}$$

Figure 2 presents the data-flow sets used in computing program slices for the program of figure 1. For example, suppose we want to know how the value of the variable sweet printed at line 25 was computed. The specification of a slicing criterion requires a variable and a node in the flow-graph. Node 18 corresponds to the **printf** statement at line 25 so, the criterion would be $S_{<18,sweet>}$. Applying this criterion generates the sequence of criteria presented in figure 3. Nodes 9 through 18 do not assign a value to sweet and are not included in the slice. Node 8 assigns a value to sweet based on red and green and so node 8 (line 13) is included in the slice along with slices on red and green at node 8. The slice on red consists of nodes 7 and 3; the slice on green consists of node 5. The slice is now complete except for except for some syntactic dependencies (nodes 1, 2 and 20) that are captured by the *requires set*, explained below.

3.1.1 Compound control statements

A compound control statement is a statement that has a condition directly controlling the execution of another statement (possibly also a compound statement). Control statements such as **if, switch, while, for** and **do ... while** should be included in a program slice whenever any statement governed by the control statement is included in a slice. When control statement n is added to a program slice, the slice on the criterion $< n, \text{refs(n)} >$ is added to the original slice computation. For each statement, n, associate a set, *requires(n)*, of statements that must be included in a slice containing statement n. The requires set is a general mechanism for capturing dependencies. A control statement is in the requires set of each statement governed by that control statement. The requires can also be used to capture syntactic dependencies such as the closing brace on line 19 matching the while statement on line 16 in the example of figure 1. The slicing rule for $v \in$ defs(n) becomes:

$$S_{<m,v>} = \{n\} \cup S_{<n,x>} \forall x \in \text{refs(n)} \cup S_{<y,x>} \quad \forall x \in \text{refs(y)} \forall y \in \text{requires(n)}$$

4 Unravel Project

Unravel is a prototype program slicing tool being developed for NRC as part of the High Integrity Software Assurance Project at NIST. **Unravel** is intended to be used to supplement NRC software audits. The basis for the decision to develop the prototype tool **Unravel** was based on two principal criteria:

Line	Statement	Node	Succ	Req	Defs	Refs
1	`main()`	1	2	—	—	—
2	`{`	2	3	1, 20	—	—
7	`red = 1;`	3	4	2	red	—
8	`blue = 5;`	4	5	2	blue	—
9	`green = 8;`	5	6	2	green	—
10	`yellow = 2;`	6	7	2	yellow	—
12	`red = 2*red;`	7	8	2	red	red
13	`sweet = red*green;`	8	9	2	sweet	red, green
14	`sour = 0;`	9	10	2	sour	—
15	`i = 0;`	10	11	2	i	—
16	`while ( i < red) {`	11	12, 14	2, 14	—	i, red
17	`sour = sour + green;`	12	13	11	sour	sour, green
18	`i = i + 1;`	13	11	11	i	i
19	`}`	14	15	—	—	—
20	`salty = blue + yellow;`	15	16	2	salty	blue, yellow
21	`yellow = sour + 1;`	16	17	2	yellow	sour
22	`bitter = yellow + green;`	17	18	2	bitter	yellow, green
24 25	`printf ("%d %d %d %d\n",` `sweet,sour,salty,bitter);`	18	19	2	—	sweet, sour salty, bitter
26	`exit(0);`	19	—	2	—	—
27	`}`	20	—	—	—	—

Figure 2: Slicing Example Data-Flow Sets

$$S_{<18,sweet>} = S_{<17,sweet>} = \cdots = S_{<9,sweet>} = \{8\} \bigcup S_{<8,red>} \bigcup S_{<8,green>}$$

Figure 3: Criteria for $S_{<18,sweet>}$

1. no tool with similar functionality and performance capability exists, and

2. the tool is technically feasible.

Before beginning work on **unravel**, NIST conducted a literature study to identify any commercial tools that may have similar functionality to **unravel**. **Unravel** is a static program analyzer that examines source code directly but does not require execution of the program. The tool search focussed on tools that could aid an NRC auditor conducting string checks or examining functional diversity during evaluation of software safety systems in nuclear power plants. Several CASE tools (table 1) were compared to **unravel**, a program slicer[19], being developed by NIST. Of the CASE tools identified in Table 1, only those were selected for additional study if they were described with terminology such as data flow analysis, control flow analysis, and traceability. In each instance, the tools were unsuitable because of their need for execution time or very sophisticated interpretation of results or because they provide no analysis of the source code and only find errors.

4.1 Language issues

Several computer languages are used within the nuclear industry. **Unravel** must be able to accommodate the languages prevalently used in this industry. Many existing systems of one major vendor have software written in PLM-86, proprietary to INTEL; however, vendors tend to be moving toward ANSI C, Ada, and C++ for the work they plan to do in the future[15]. Since FORTRAN has been a widely used programming language among engineers for many years, some safety systems may have been written in some dialect of FORTRAN.

The following languages used for safety system implementation have been identified as potential targets of the slicing tool: ANSI C, C++, Ada, PLM-86, and FORTRAN.

The slicing tool eventually should be able to handle either Ada, C++ or ANSI C. However, the prototype tool should concentrate on ANSI C for the following reasons:

- ANSI C is a stable standard not likely to have significant changes in the near future.

- C++ does not have an ANSI standard and is still evolving with several major features incorporated into the language since 1985 (e.g. templates and exceptions).

- ANSI C is a subset of C++ and any work on a slicer for ANSI C could be later applied to an extension for C++.

- Ada is a much larger and more complex language than C++ or ANSI C and would require the most effort to build a prototype slicer.

- A slicer for PLM-86 would be of limited utility since it is only used by one contractor.

- A slicer for FORTRAN would be of limited utility since FORTRAN is being abandoned in favor of modern programming languages[15].

The main consideration when evaluating feasibility of using program slicing on a given programming language is the difficulty of tracking data-flow through the program. The following language features potentially present some difficulties:

Tasking Any language or system that supports communicating independent processes cannot be sliced across tasks in a meaningful way. Some languages such as Ada have tasking built into the language while other languages such as ANSI C use system calls (e.g. fork()) to the host operating system to create independently executing tasks.

Exceptions Slicing code using exception handling routines is not well defined. The exception handler can be invoked at any time and therefore the state of program variables is unknown at the time the exception handler is invoked. Exceptions are called signals in ANSI C.

Generics Ada generics and C++ templates should be investigated in more detail in a since templates are a new feature to C++ that might change in the near future.

Aliases Aliases, more than one name for a memory address, are introduced by a number of language features such as unions in ANSI C, common blocks in FORTRAN and passing the same parameter more than once in the same function call.

List of Tools and Vendors	
Tool	**Vendor**
Auto-G	RJO, Enterprises, Inc.
BugFinder	Software System Design
Cohesion Environment	Digital Equipment Corporation
Design Family	META Software Co.
EasyCASE	Evergreen CASE Tools Inc.
ERwin	Logic Works Inc.
Excelerator	Intersolv
ForeSight	NuThena Systems
Mantis	CINCOM System Inc.
McCabe Slice Tool	McCabe & Associates
Object Maker	Mark V Systems Ltd.
Requirements Tracer	Teledyne Brown Engineering
StateMate	i-Logix, Inc.
Test-Gen	Software Systems Design

Table 1: List of Tools and Vendors

Pointers and Dynamic Memory The problems with pointers are similar to aliases. It is difficult to keep track of the exact memory location pointed to, especially if the location could be one of several that have been dynamically allocated. A conservative solution of keeping all locations that might be pointed to must be used. Using such a conservative algorithm produces larger slices than necessary.

Multiple Source Files A system divided into multiple source files must have some method for defining the files that link together into each executable program.

GOTO statements The presence of Goto statements requires an extra pass over the program being analyzed to identify all statements influenced by branch (if or loop) statements[14].

NRC has identified several language features that vendors are not likely to use in safety software. These features include tasking and exceptions that are dependent on an underlying operating system. Without these features, there are no relevant technical obstacles to construct a tool that would be useful during a safety audit of code written in ANSI C. For software using these features program slicing can still be useful. For example, while slices can not be computed across two tasks, program slicing can be used within a single task.

4.2 Implementation Status

We currently have a demonstration version of unravel that can be used on simple (pre-ANSI) C programs. We are currently developing a more complete version to slice ANSI C for evaluation by NRC auditors in 1994.

Unravel runs on a laptop UNIX workstation with an X Window System interface. The menu driven interface is designed to be easy for the auditor to use with a minimum of training.

5 Future Developments

There are several possible future developments that are outside the scope of this implementation plan that should be considered.

Other Languages To extend unravel to other languages a new implementation from the beginning is not required. Unravel is designed so that source language dependent information is in a single component that can be replaced for analysis of a language other than ANSI C. This component is built with the compiler writing tools

lex and yacc that simplify the task of extending unravel to a new language.

Influence Tracking The information collected by unravel could also aid NRC auditors in other safety audit activities, such as tracing a sensor signal through the code. This can be accomplished by reversing the direction of the slice computation and following data-flow of an input forward through the code rather than backward from an output as in program slicing.

Coding Standard Adherence With some small changes to unravel, adherence to coding standards intended to avoid error prone programming constructs such as usage of pointers, or deeply nested loops could be easily checked.

Fault Tree Analysis The analyser component could be used to build a tool to aid an NRC auditor in constructing fault trees.

Within the nuclear power industry, the use of systems hazard analysis as a mechanism for mitigation of potential faults, is recommended in many standards and guidelines[16]. Once the hazards have been identified, the objective is to mitigate the risk that a hazard will occur. One approach to achieve this objective is to use system fault tree analysis. Under the assumption that there are relatively few unacceptable system states and that each of these hazards has been determined, the analysis procedure is as follows. First, assume that the hazard has occurred. Then an analyst constructs a tree with the hazardous condition as the root. The next level of the tree is an enumeration of all the necessary preconditions for the hazard to occur. These conditions are combined with logical and and or as appropriate. Then each new node is expanded "similarly until all leaves have calculable probability or cannot be expanded for some reason." [10]

The results of system hazard analysis must be examined for their impact on software. The level of detail available at the software requirements or software design phases may not be sufficient to fully understand potential hazards and some critical information may be overlooked in the development of the design and code. Once code is available, it is very useful to be able to apply the equivalent of system fault tree analysis on the software. Software hazard analysis is the subject of a current study by NIST under contract RES-92-005 for the NRC.

"Software fault-tree analysis works backward from the critical control faults through the program code or the design to the software inputs. In other words, it starts from the outputs that would indicate a hazardous state (or lack of them) and traces backward to find paths through the code from particular inputs to these outputs or to demonstrate that such paths do not exist."[10] The use of software fault tree analysis for software can aid developers and auditors in performing safety evaluations to ensure potential hazards have been appropriately addressed in the software.

6 Status and Summary

NRC auditors need automated capability to evaluate software used in safety systems of nuclear power plants. The auditors need to examine source code for functional diversity and to perform string checks. Manually examining source code is a tedious and error prone task. In a search for commercial tools to assist auditors, NIST surveyed the availability of commercial tools that support program slicing and found that none existed. The McCabe Slice Tool required that the source code be executed to extract its slice. Use of executions to find slices of code is known as dynamic slicing. Most other tools assisted with the design of software but not debugging or maintaining software. Since no tool existed, NIST conducted a feasibility study on the development of such a CASE tool.

The CASE tool unravel uses program slicing to evaluate source code for functional diversity and to support string checks. Program slicing extracts code that influences a chosen variable. The automation of such a process will save time and money. It will also be less error prone than by use of human resources. Program slices need not be found by program execution, but do show all execution paths that can be taken by the program.

References

[1] H. Agrawal, R. DeMillo, and E. Spafford. Debugging with dynamic slicing and backtracking.

Software-Practice and Experience, 26(6):589–616, June 1993.

[2] K. B. Gallagher and J. R. Lyle. Using program slicing in software maintenance. *IEEE Transactions on Software Engineering*, 17(8):751–761, August 1991.

[3] K. B. Gallagher and J. R. Lyle. Program slicing and software safety. In *Proceedings of the Eight Annual Conference on Computer Assurance*, pages 71–80, June 1993. COMPASS '93.

[4] S. Horwitz, J. Prins, and T. Reps. Integrating non-interfering versions of programs. *ACM Transactions on Programming Languages and Systems*, 11(3):345–387, July 1989.

[5] M. Kamkar, P. Fritzson, and N. Shahmehri. Interprocedural dynamic slicing applied to interprocedural data flow testing. In *Proceeding of the Conference on Software Maintenance -93*, pages 386–395, 1993.

[6] J. Knight and N. Leveson. An experimental evaluation of the assumption of independence in multiversion programming. *IEEE Transactions on Software Engineering*, 12:96–109, 1986.

[7] B. Korel and J. Laski. Dynamic program slicing. *Information Processing Letters*, 29(3):155–163, October 1988.

[8] B. Korel and J. Laski. STAD - A system for testing and debugging: User perspective. In *Proceedings of the Second Workshop on Software Testing, Verification and Analysis*, pages 13–20, Banff, Alberta, Canada, July 1988.

[9] J. Laski. Data flow testing in STAD. *The Journal of Systems and Software*, 1989.

[10] N. Leveson, S. Cha, and T. Shimeall. Safety verification of Ada programs using software fault trees. *IEEE Computer*, 8(4):48–59, May 1991.

[11] J. R. Lyle and M. D. Weiser. Experiments in slicing-based debugging aids. In Elliot Soloway and Sitharama Iyengar, editors, *Empirical Studies of Programmers*. Ablex Publishing Corporation, Norwood, New Jersey, 1986.

[12] J. R. Lyle and M. D. Weiser. Automatic program bug location by program slicing. In *Proceeding of the Second International Conference on Computers and Applications*, pages 877–882, Peking; China, June 1987.

[13] W. W. Peng and D. R. Wallace. Software error analysis. Technical report, National Institute of Standards and Technology, Gaithersburg, MD 20899, 1993. NIST Special Publication 500-209.

[14] R. E. Tarjan and T. Lengauer. A fast algorithm for finding dominators in a flowgraph. *ACM Transactions on Programming Languages and Systems*, pages 121–141, July 1979.

[15] U. S. Nuclear Regulatory Commission, Washington, DC 20555. *Class 1E Digital System Studies*. (to be published as) NUREG/CR-6113.

[16] D. R. Wallace, L. M. Ippolito, and D. R. Kuhn. *High Integrity Software Standards and Guidelines*. U. S. Nuclear Regulatory Commission, Washington, D.C. 20555, 1992. NIST Special Publication 500-204 and NUREG/CR-5930.

[17] D. R. Wallace, W. W. Peng, and L. M. Ippolito. *Software Quality Assurance: Documentation and Reviews*. National Institute of Standards and Technology, Gaithersburg, MD 20899, 1992. NIST-IR 4909.

[18] Dolores R. Wallace, D. Richard Kuhn, and John C. Cherniavsky. Proceedings of the Workshop on High Integrity Software; Gaithersburg, MD; Jan. 22-23, 1991. Technical Report NIST Special Publication 500-190, National Institute of Standards and Technology, 1991.

[19] M. Weiser. Programmers use slices when debugging. *CACM*, 25(7):446–452, July 1982.

[20] M. Weiser. Reconstructing sequential behavior from parallel behavior projections. *Information Processing Letters*, 17(5):129–135, October 1983.

[21] M. Weiser. Program slicing. *IEEE Transactions on Software Engineering*, 10:352–357, July 1984.

"SOFTWARE RELIABILITY ASSESSMENT"

M Barnes, P A Bradley, M A Brewer

AEA Technology
Consultancy Services

ABSTRACT: The increased usage and sophistication of computers applied to real time safety-related systems in the United Kingdom has spurred on the desire to provide a standard framework within which to assess dependable computing systems. Recent accidents and ensuing legislation have acted as a catalyst in this area. One particular aspect of dependable computing systems is that of software, which is usually designed to reduce risk at the system level, but which can increase risk if it is unreliable.

Various organisations have recognised the problem of assessing the risk imposed to the system by unreliable software, and have taken initial steps to develop and use such assessment frameworks. This paper relates the approach of Consultancy Services of AEA Technology in developing a framework to assess the risk imposed by unreliable software.

In addition, the paper discusses the experiences gained by Consultancy Services in applying the assessment framework to commercial and research projects. The framework is applicable to software used in safety applications, including proprietary software. Although the paper is written with Nuclear Reactor Safety applications in mind, the principles discussed can be applied to safety applications in all industries.

INTRODUCTION

Programmable Electronic Systems (PES) are being increasingly depended upon in systems which have the potential for unacceptable hazards to individuals, society, and the environment - for example, in industries such as nuclear, defence, oil & gas, and chemical process. There are also increasing pressures from the general public, regulatory authorities, professional institutes, and governments to ensure that systems with such large potential hazards exhibit tolerable levels of risk.

One aspect of this risk is that from unreliable software - but software is neither unreliable or unsafe on its own - it needs other components of a system to make it function as part of that system, and thus software cannot function in isolation. As a result, it is important to stress that software should not be assessed in isolation, but in a systems context, since there are other components of the system which are interrelated, eg sensors, actuators, processing hardware, interfaces, human operators/maintainers, and procedures. Failures of such components may dominate the total system risk, and hence it is necessary to determine where the risk assessment effort should be best targeted, in order to make risk assessment cost effective.

This paper focuses on software reliability from an assessment viewpoint, but in the context of risk to a system. In particular it relates to the experience of AEA Technology, Consultancy Services (CS), in carrying out assessments of software. Before assessing software risk, it is necessary to consider system risk.

THE CONCEPT OF SYSTEM RISK

The terms ***reliability*** and ***safety*** are often interchanged or confused. Reliability applies to all specified functions of a system, ie that the specified functions perform under specified conditions, for a specified time period, and reliability is usually associated with economic loss. Safety, on the other hand, is usually associated with quality of human health, ie disease, injury, or death, either immediately, or over longer term, eg via environmental effects. However, there are occasions when phrases such as "plant safety" are used to mean economic loss due to plant damage (as opposed to undesired shut down).

Safety can therefore be regarded as a subset of reliability, ie those functions which are designed to protect against injury/death are safety functions, and hence safety assessment would be aimed at a subset of all the system functions (but not restricted to this subset, unless such safety functions could be shown to be isolated from other system functions). However, the common factor in both safety and reliability assessment is the concept of ***risk***; either economic risk, risk to human life, or environmental risk.

System (eg plant) risk is a function of two components: the frequency (or probability) of a hazard occurring, and the consequences of that hazard occurring,ie:

RISK = HAZARD RATE x CONSEQUENCES OF HAZARD

The advantage of using the concept of system risk is that it enables the correct amount of attention to be afforded to the hazards being considered in the assessment. For example, for software, it informs the assessor of how much attention should be paid to the assessment of the software, based upon the consequences of the software failures considered. The assessment of system risk attempts to answer the following fundamental questions:

- what can go wrong?
- how often can it go wrong?
- how bad will it be?
- what are the implications?

The responses to these questions will determine the amount of effort and rigour needed to justify the usage of the software, whether it be on economic grounds (eg to a plant operations manager), or on safety grounds (eg to a regulatory body). The above questions form the basis for the assessment of tolerable risk, which is now discussed.

RISK ASSESSMENT

Risk assessment is aimed at demonstrating that risk is reduced to tolerable levels - risk cannot be eliminated completely; however there are:

- risks which cannot be accepted under any circumstances because the risks are intolerable;
- risks which are tolerable, but which should be reduced to as low as reasonably practical (ALARP);
- risks which can be broadly accepted without the need for detailed analysis to demonstrate ALARP

This is shown graphically in figure 1. One aspect of risk assessment is to determine the amount of trust required for systems which are designed to control the plant within defined operational boundaries to prevent hazards occurring, and to protect the plant should the control system fail. The factors which are driving the need for the risk assessment of PES are now discussed.

DRIVERS FOR RISK ASSESSMENT OF PES

There are many factors which are contributing to the increased requirement for risk assessment of PES. These interrelated factors are considered under the headings of sociological drivers, technological drivers, economic drivers, and political drivers.

Sociological Drivers

There have been many sociological changes which have effected the procurement of dependable

systems:

- The general public, through newspapers/television, are more aware of the daily risks to which they are exposed. This is highlighted by increasing press coverage on major incidents eg: coverage of the Chernobyl nuclear reactor and Bhopal accidents. Within the UK a number of disasters have lead to specific regulatory pressure, eg the Piper Alpha Oil off-shore installation explosion was followed by the Lord Cullen report, which stressed the need for system safety cases [ATOM].

- The general public is reluctant to accept these risks, hence society is moving into a 'blame culture' when incidents occur.

- In response to the perceived increase in risk and the reduced tolerance to these risks there has been an increase in the number of pressure groups which are influencing the acceptability of safety critical systems.

- Increased environmental awareness of the general public is creating a demand for new assessment services.

These sociological changes have resulted in a culture which is less tolerant to serious disasters and which calls for increasingly higher levels of safety.

Technological Drivers

Technological change has been the major driving force in the widespread application of programmable technology.

- The rapid growth in software/microelectronics technology has meant that programmable systems are pervading many areas of society.

- Technological developments have enabled the design of more complex systems, which were not previously attempted. These systems are being increasingly used to control and protect against safety related/critical hazards.

- New technology is continually being developed (eg, expert systems, neural networks, virtual reality) requiring different approaches to development and assessment.

- The technology within the workplace (eg, degree of tool support) is continually increasing (reflecting the move towards the mature stage of the product lifecycle).

- Not surprisingly, there is little commonality in the approach to regulating the development of programmable systems [EUR 1147].

This technological expansion has brought with it many challenges and potentially increased risks.

A set of illustrative risks to the public stemming from the use of computer systems is maintained by the Risks Forum [NEUMANN]. This list is growing at a rate of approximately 240 incidents per year.

Economic Drivers

There are many economic pressures on the development and assessment of dependable systems:

- Programmable systems are seen as an effective way of providing a competitive edge to many organisations based upon more functionality and lower prices. This demand, within an increasingly competitive environment, has resulted in the need for more complex systems without sacrifices of safety, reliability and availability, and at a cheaper price.

- The requirement to produce and demonstrate the dependability of complex programmable systems has inevitably resulted in increasing prices for systems.

- Organisations are also becoming more aware of the financial impact of major incidents and are more aware of the dependence upon programmable systems for ensuring survival.

- The removal of many world trade barriers has resulted in an increasingly international market which is subject to fluctuations in the exchange rate. This has a direct impact on the return from commercial work and the amount of research funding from European agencies.

Increasing demands for dependable systems, the move to a more international market and increasing development/assessment costs have resulted in a competitive economic environment.

Political Drivers

Political pressures are increasing, generally as a result of the sociological, technological and economic pressures:

- Legal liability is becoming clearer with criminal and civil liabilities eg, the Health and Safety at Work Act 1974, Consumer Protection Act 1987 and the concept of strict product liability having an impact of the development and assessment of programmable systems. Increasingly strict legal liability has resulted in the IEE providing guidance for its members which includes a definition of competence and a code of practice for the development of safety critical systems [IEE/BCS].

- National and international standards are under development [MOD 0055], [MOD 0056], [IEC 65A/9], [IEC 65A/10], which provide guidelines for the safety assessment of systems. It is believed that these standards, to varying degrees, will be mandated for the

assessment of programmable systems.

THE SOFTWARE RELIABILITY ASSESSMENT TASK

The above factors are promoting system risk assessment, and in turn, for PES, software risk assessment. Assessment is a necessary pre-cursor to granting licences to operate systems; the objective of licensing software for safety systems is to provide a judgement on the adequacy of the safety aspects based on documentary information submitted by the developers. This judgement is "live" issue, and will be influenced by approaches to licensing in other industries, emerging and established standards/guidelines, and research [NUCENG].

Fundamentally, the software safety assessor's task is to provide evidence of the strengths and weaknesses of the software, so that the regulator can:

- the correct safety functions have been specified in the software requirements
- these functions have been correctly implemented in the design and development
- safety will continue to be maintained in operational life, via the integrity of the software maintenance and change mechanisms

Hence the requirements specification, and in particular the specification of the safety functions, are vital to the licensing and assessment process.

These safety functions are intended to control risks inherent in the system (ie plant), and hence it is vital that a "top-down" approach to managing this risk in a systems context is adopted, rather than a bottom up approach of assessing the software reliability in isolation. A framework for assessment is thus needed.

A FRAMEWORK FOR SOFTWARE RISK ASSESSMENT

Consultancy Services has derived the following framework in response to the "drivers" for risk assessment. The framework has considered the key points from interim and emerging standards, and enables new and existing assessment practices to be incorporated.

Sources of Risk

Since software is a significant functional part of a PES system, then clearly, it too should be subjected to risk assessment, as part of an overall system risk assessment. In assessing software, the assessor addresses two main sources of risk:

- the plant hazards which the software system is required to control or protect against; ie do the specified safety functions address the plant hazards?
- the hazards imposed by the development of the software system itself; ie assuming that the safety functions have been correctly specified, have they been implemented correctly?

The framework described in this paper addresses both of these sources of risk.

Fundamental Elements of the Framework

The framework is based upon 3 fundamental activities, ie:

- Risk Identification (what can go wrong?)
- Risk Analysis (do defensive measures exist?)
- Risk Control (are the measures adequately controlled?)

Central to this framework is the concept of the "Hazard Log", which is a systematic means for documenting and managing the hazards identified in a system. The Hazards Log is a register which is used to log all hazards occurring throughout system development, ie from systems preliminary hazards analysis onward; it is living document which exists throughout the life of the system, and is updated as changes are made to the system. The Hazard Log is the focal point of safety assurance, and:

- all hazards resulting from all risk analysis activities
- the defences used against these hazards

are entered in the Hazard Log, which is then used to demonstrate that these hazards have been adequately dealt with, ie that the risk from the hazards has been reduced to a tolerable level.

Hazards analysis at the system level will lead to initial hazards being documented in the Hazards Log; requirements will have been specified for a defensive system to control or protect against these hazards, and a decision will have been made to divide the safety functions of the system into hardware and software functions. This forms the starting point for applying the software risk assessment framework (see figure 2).

Activities in the Framework

Risk Identification Activities:
The first activity is Risk Identification, and is aimed at identifying any new hazards and their impact. Systematic and structured "bottom-up" analysis techniques are applied to the products of the software development (eg specification, design, code), in order to identify any new hazards which might be inherent in the proposed system.

CS has used the Software HAZOPS technique for this activity. It is a structured and systematic "brainstorming" technique, and involves the following steps:

- a model of the system is created using Structured Analysis techniques;

- the system is then divided into logical and manageable units;

- relevant people with differing system viewpoints/needs, eg:
  - the customer;
  - the user/operator;
  - the maintainer;
  - the software developer;

  are gathered together to carry out the structured brainstorming, together with a chairman to control the brainstorming session, and a scribe to record the findings;

- "guidewords" and "deviations" are applied to the functions within the logically divided units, to determine the consequences of these deviations;

- any new hazards discovered, and any claimed defences against them, are entered in the Hazards Log, which will then form the input to the next activity (Risk Analysis);

- any new safety functions required, as a result of the new hazards discovered, will also be entered into the Hazards Log;

- if new safety functions are required, the system requirements (and design, etc) will be modified to include these functions.

This iterative process is applied at all stages of the software lifecycle.

Risk Analysis Activities:
This activity is aimed at analyzing the hazards entered into the Hazards Log and their respective defences (proposed safety functions), to determine if the defences have addressed the all hazards listed in the Hazards Log. During this detailed analysis activity, the assessor might well encounter new hazards which were not discovered in the Risk Identification activity; these hazards will also be entered into the Hazard Log. New defences will be required for:

- these newly discovered hazards, and
- known hazards where the claimed defences were inadequate

Systematic and structured "top-down" techniques are applied to the products of the software development (eg specification, design, code), in order to determine the root causes which lead to the failure of the safety functions, ie root causes which result in a failure to deal with the identified hazards adequately.

CS has used the technique of Software Fault Tree Analysis (SFTA). This is similar to Fault Tree Analysis as applied to electronic hardware analyses, except that it is used in a qualitative sense only. A number of "top events" are defined, based on the failure of each safety function. The products of the software development are then analyzed and a Fault Tree is then constructed based upon the structure of the product in question. The Fault Tree is then used to determine the root causes (base events) of the failures of these safety function top events.

The product is then analyzed against the base events to determine if and how the base events can happen. Usually the probability of the base event is either 0 or 1 (ie completely true, or false); for example, if the base event from a segment of code were "variable TEMPERATURE < 0", the assessor would analyze the code to determine if the TEMPERATURE variable could ever have a negative value. The defences for all hazards listed in the Hazard Log are input to the next activity (Risk Control).

Risk Control Activities:
This activity is aimed at determining the adequacy of the engineering practices and techniques used to control the software risk. Assessment of software risk control is aided by the assessor asking the following basic questions:

- what practices have been used to get the software "correct first time"?
- how is it known that the software is "correct"?
- what if it is not "correct"?

Hence the CS approach is based upon the assessment of the techniques (and their efficacy) used in the software development relating to:

- Fault Avoidance
- Fault Detection and Removal
- Fault Tolerance

(Note: the word "fault" in the context used here is intended to mean the concrete manifestation of an abstract human error. For example, a software developer might type the name of a constant incorrectly; the error is somewhere in the interface between the developer's thought process and finger control, but the fault is a new and erroneous constant embedded in the code).

Fault Avoidance: If the software developer can avoid making faults in the software, then the software would be fault-free and life would be very simple. However, history demonstrates that this is not the case, and that in spite of the fact that standards and guidelines abound, the same mistakes are made by generations of software developers, and more especially, their organisational management. Hence this part of the assessment addresses, amongst others, a correct specification, the choice of development techniques, the software quality assurance and verification aspects, the organisation and management structure, software standards, etc.

Fault Detection & Removal: Human beings find it difficult to avoid creating faults, which makes it necessary for the software developer to detect and remove the faults which were not avoided. This removal process also requires that the developer does not introduce further faults, since the risks imposed by these faults might well exceed the risks of those faults which were removed. This part of the assessment addresses aspects such as dynamic testing strategy, static analysis, reliability prediction, and software maintenance procedures.

Fault Tolerance: It should be noted that software faults are systematic faults, ie they are due

to errors made in the software design, and make system failure susceptible to a single fault, which will be replicated in redundant units. In addition, software does not deteriorate in service (like electronic hardware), but its performance might deteriorate if it is exercised by a set of different input sequences; this is because software provides true "high-fidelity" in that its behaviour is repeatable for repeatable input sequences.

Just as human beings cannot avoid creating faults, they cannot guarantee to detect and satisfactorily remove those residual faults, and hence these software faults will ultimately lead to system failure. This part of the assessment addresses the efficacy of the techniques used to either eliminate failures due to single faults, or reduce the impact of single fault failures to a tolerable level (defence in depth).

It is a well-established regulatory principle that system failure should not be vulnerable to a single fault. Consequently, this single fault criterion requires that the system is tolerant to faults which can lead to system failure. For residual software faults, these can be dealt with by fault tolerant aspects either by using techniques at the system level (eg functional diversity) or the software level. Fault tolerance requires two mechanisms:

- the detection of software failures
- a failure management strategy

The assessment techniques for Fault Avoidance, Fault Detection/Removal, and Fault Tolerance form a structured approach to the assessment of Software Risk Control, and can be applied in all parts of the software development lifecycle, including maintenance. The techniques are aimed at assessing either or both:

- the software development process, to determine if the techniques used during development are commensurate with the consequence of failure; this is primarily achieved by determining compliance with codes of practice, guidelines, standards, using tick lists;

- the products of the software development, to determine how effective the techniques have been; this is carried out by techniques such as complexity metrics, software reliability models, bug seeding, etc.

MANAGING THE FRAMEWORK

The model of the framework presented makes it appear as a static sequential procedure, ie where one activity is completed before the outputs are fed to the next activity, etc. In reality, it is quite different; it is a complex dynamic process, with many interrelated tasks with many interconnecting paths, involving many iterations of these paths. This means the framework is not easy to manage.

The framework can be applied at all phases of the software lifecycle. However, quite often distinct software lifecycle "phases" do not exist; instead several successive levels of refinement

are used, from abstract requirements, through to the concrete code. These can form many "indistinct" lifecycle phases, and this too can complicate the management of the framework.

Hence it is important that the administrative arrangements for producing:

- the input information required by the assessor,
- the findings of the assessment,

are well defined, planned, scheduled, monitored, and controlled. This is especially true where the relevant evidence has to be furnished to a regulatory authority.

EXPERIENCE IN APPLYING THE ABOVE FRAMEWORK

CS has applied the above framework for software risk assessment to a large number of commercial projects of various sizes and risk categories. These projects have been from a wide range of industries, including, defence, transport, medical, oil & gas, water, regulatory, process, manufacturing, and nuclear, and were for clients in the UK, the rest of Europe, Australia, and the USA. Non-disclosure agreements between CS and our clients prevent these project from being explicitly identified without prior permission, and so the following discussion on CS experience is presented in general terms rather than project-specific terms.

The practical application of the above framework has resulted in the exposure of a number of problem issues. Some of the lessons learned from our experience in applying the above framework to commercial and research projects, are now discussed, together with the approach that CS used to address the issues.

ISSUES ARISING FROM RISK ANALYSIS ACTIVITIES

A major question arising from the software risk analysis activity is "How can I quantify the software reliability?". In attempting to answer this question a number of further issues arise:

- Why can I quantify hardware systems but not software?
- Can I test my system to demonstrate a reliability figure?
- Can I use software metrics to demonstrate a reliability figure?
- Can I use software reliability models to demonstrate a reliability figure?

Why can I quantify hardware systems reliability but not software?

Our practical experience has highlighted that the distinction between hardware and software systems is becoming increasingly blurred. This blurring can be seen from the use of the Programmable Logic Device (PLD) which may have traditionally been considered to be hardware but is now providing levels of functionality to challenge "software" solutions. An illustration of the convergence of these two technologies is the increasing use of hardware

description languages, which are very similar to procedural programming languages, to "program" the "hardware" devices.

An increasingly more useful distinction, particularly with respect to the risk analysis, is that between the systematic (or design) failures and random failures of a "system". Random failures are failures which occur at random times due to degradation mechanisms in hardware components. Systematic failures are due to faults in the design of the system. Design faults could be due to an error in implementing defined requirements or a fault within the requirements. Using this distinction it can be seen that hardware systems consist of both random and systematic failures and software systems consist of purely systematic failures (since software doesn't suffer from mechanical degradation).

When quantifying hardware components a constant mean failure rate is assumed, based upon past experience of using a similar component within a similar environment. This constant failure rate represents the random failure of the hardware component. Systematic failures are considered as part of the development of fault trees, however as hardware systems become more complex (as illustrated by the use of PLDs) they have an increasingly large systematic component and hence the quantification of hardware components will become more prone to the difficulties currently being exhibited by purely software components.

In answer to above question it would seem that hardware systems have been quantified in the past because their limited complexity enabled risk analysts to represent this complexity within a structured technique (eg: fault tree) and use a knowledge of common hardware failure rates to predict the reliability of the system. The increased complexity possibly with software (and increasingly hardware) intensive systems means that modelling this complexity is far more difficult and requires new approaches.

Can I test my system to demonstrate a reliability figure?

As has been discussed above, software is high fidelity in that for given input values (over a history) it will always give the same outputs. Demonstrating that software meets reliability requirements would therefore seem to be a matter of testing the software with desired inputs to ensure that the correct systems outputs resulted. In order to provide a high degree of confidence in a high reliability figure the software testing would need to be exhaustive. It is widely recognised that, for a system of any complexity (both hardware and software), exhaustive testing is impractical [IEEE].

Practical experience has demonstrated that different testing techniques can be used to identify different types of fault and that some techniques are more useful than others. For example, a uniform random testing strategy using back-to-back testing techniques is a cost effective means of finding faults in programs [INF ST]. Further practical experience has illustrated that even though testing cannot be used to demonstrate a definitive reliability target it can be used to complement other techniques in putting forward a safety case. Further to this, testing has been used to demonstrate the integrity of small, safety-critical, parts of a system through exhaustive

testing.

Can I use software metrics to demonstrate a reliability figure?

There has been considerable research into the use of software measures (metrics) to help predict software reliability. This has focused upon measuring some characteristic of the system (process or product) which is believed to be related to the behaviour of concern (safety or reliability). There are two types of metrics:

- control metrics which relate to the development process and include measures such as the effort expended and elapsed time. These metrics are used to provide management control of the process;
- predictive metrics which relate to developed products and include measures such as the complexity of the software (ie: number of lines of code etc). These predictive metrics are used to provide a measure of an aspect of product quality.

In order for these metrics to be of value within the risk assessment three conditions must be met:

- some property of the software can be accurately measured
- a relationship must exist between what we can measure and what we would like to know about the product's behavioural attributes
- this relationship is understood, has been validated, and can be expressed in terms of a formula or model.

Experimental evidence suggests that there is little support for the last two of these conditions [INF ST]. It is therefore currently difficult to relate characteristics of the system to reliability and safety measures. In answering the above question it would seem that software metrics cannot be readily used to measure the reliability of a software system.

Can I use software reliability models to demonstrate a reliability figure?

Whereas testing aims to demonstrate unreliability of a system through executing input combinations, reliability growth models aim to predict reliability by providing a model of the system failure rates. Although there are a wide range of models to choose from there is little confidence in the practical application of the models. This view is supported by the following:

> *"During the preparation of this document, methods for estimating the post-verification probabilities of software errors were examined. The goal was to develop numerical requirements for such probabilities for software in computer-based airborne systems or equipment. The conclusion reached, however, was that currently available methods do not provide results in which confidence can be placed to the level required for this purpose. Hence, this document does not provide guidance for software error rates. If the applicant proposes to use software reliability models for certification credit, rationale for the model should be included in the Plan for Software Aspects of Certification, and*

agreed with by the certification authority". [EUR]

"There is little evidence available to show how effective these techniques are in practice, and experience of their practical application is needed before publishing them as a British Standard". [BSI 198]

The specific limitation of these models with respect to safety-critical systems is that they generally require a number of system failures to calibrate the system. It would therefore seem that as the models come of value (ie: by being calibrated with a number of identified errors) the system has already demonstrated that it is not fit-for-purpose (since a small number of system errors would raise doubt on the integrity of the system with respect to safety considerations).

ISSUES ARISING FROM RISK CONTROL ASSESSMENT

A number of important issues can be identified when considering the approaches available for risk control, eg:

- What development approach should I use for fault avoidance?
- How can I use diversity for fault tolerance?
- How practical are existing assessment guidelines for actual use?

What development approach should I use for fault avoidance?

There is an increasing choice of paradigms for the development of complex systems. Over the past decade these choices can be characterised as:

- From functions to objects: a move from functional and data-driven decomposition (eg: data-flow diagrams and jackson structured programming respectively) to object-oriented decomposition.
- From informal to formal: a move from informal notations (eg: natural language) to more formal (eg: Z, VDM and OBJ) specification, design and coding notations.

Practical experience of both functional and object-oriented notations [DARTS] has illustrated the need for both perspectives throughout the development process. At the more abstract levels the system can be viewed as static objects. The use of objects enables implementation detail to be hidden and the objects viewed as "black boxes". A further refinement of the system can emphasise the interactions of objects and hence focus upon the functional nature of the system. At the most detailed level the system can again be considered as basic objects (possibly data-types) with certain characteristics.

Our experience applying formal development techniques has highlighted the need to complement these with high-level structuring approaches (eg: Yourdon). This is particularly important when managing large formal specifications. There is considerable work aimed at providing a coherent methodology incorporating the advantages of formal techniques and the structuring capability of

graphical representations [SafeFM].

The mathematical basis gives a means to precisely define quality attributes such as consistency, completeness and correctness. A formal method typically includes a specification language with mathematically based syntax and semantics [IAEA 88]. Credit can be claimed for the use of a formal mathematical specification language since this will increase confidence in the correctness of the design and code. The specification should be validated by logical reasoning and peer review of this reasoning [NII].

The main difficulty in formal development is the translation of vague, incomplete, ambiguous or unavailable user requirements into a formal specification. It is difficult to ensure that the formal specification contains all of the user's requirements and that they have been correctly specified.

Experience with a range of different formal notations (Z, Occam, LARCH) has highlighted that there is often little to choose between techniques. Practical considerations such as the availability of tool support are still dominant issues in the choice and application of such techniques.

There is increasing guidance on the "minimum requirements of development approach" for software based systems [IEC 65A/10], [MOD 0056]. Within IEC 65A software is classified in terms of integrity levels and defined minimum development techniques are described, eg specification requirements are as follows:

Specification	L1	L2	L3	L4
Formal specification	-	-	R	R
Structured specification	R	R	HR	HR
Specification support tools	R	R	HR	HR
Prototyping/Animation	R	R	R	R
Natural language support struct/formal spec	R	R	R	R
Cause/effect diagram	-	-	R	R
Checklists	HR	HR	HR	HR
Inspections	R	HR	HR	HR
Formal design review	HR	HR	HR	HR

where L4 is of the highest criticality (eg: safety critical) and L1 is the lowest criticality (eg: no safety implications), R = recommended and HR = highly recommended.

How can I use diversity for fault tolerance?

Several systems assessed by CS have to some degree incorporated diversity within their design. From the assessor's point of view the major area of interest when assessing a diverse system is "how is the diversity maintained throughout the development so as not to compromise the system?".

Diversity has to have a "common starting point" in the software development lifecycle; this is typically at the requirements or specification stage, and from this the diverse designs and software are developed. Two major areas need to be addressed:

- how are the requirements/specification checked to ensure they are complete and correct?
- how are modifications to the original requirements/specifications controlled later in the development phases?

The first problem area isn't unique to diverse systems; all software systems need to resolve this issue and several techniques are available, eg Formal Methods, discussed above. The second area is more applicable to diverse systems, and therefore different approaches need to be taken, ie:

- firstly to apply controls to the information path;
- and secondly to assess the application of those controls.

From the assessor's point of view, the aim is to identify when diversity was compromised, and the consequences of that compromise. It has been the experience of CS that in all diverse systems there is usually a key individual (or team) who is the link between the diverse development groups. The responsibility of the link person is:

- to investigate faults found in each diverse development, and to trace these faults to determine if any originated at the "common starting point" for diversity
- to pass relevant information to other groups without compromising the diversity.

While the link person may be positioned to maintain diversity there is always the chance that this individual could influence all the diverse teams, and be a source of "common mode error", hence compromising the diversity.

Therefore, when assessing a diverse development it is important to probe into the management structure, because the structure shown on organisational charts can often be deceptive. For example, when assessing one small company, the company produced a structure chart which provided job titles only; when this was investigated further it was found the link person was also the lead designer and programmer for one the diverse channels; and as such had too much influence over the entire system.

Another area of potential compromise is in the final integration of the system, when the two (or

more) diverse software systems are brought together. It is not uncommon for a single software system to be used to provide the voting mechanisms for the diverse systems, potentially compromising the intended diversity benefits. In one system the "control" software had been rigorously developed and tested, but during the final on-site integration and commissioning a number of modifications were required. Due to the time pressures to complete the on-site integration, the consequences of some of the modifications were not fully explored. Whilst the aim was to save time (and money), the result was the on-site testing took longer than scheduled and cost significantly more.

How practical are existing assessment guidelines for actual use?

Guidelines which have been used extensively by CS are the HSE PES Guidelines [HSE PES]. These are designed as the basis for the development and assessment of safety-related PES, including hardware and software aspects, and were intended to be taken as the starting point for users to develop the Guidelines to suit the needs of their industries. CS has been asked by its clients to independently apply these checklists to their applications.

A main feature of the guidelines is a series of qualitative checklists, with associated questions which are intended to be used to assess aspects of risk control, both for hardware and software aspects; the software checklists focus on the software development process.

The Guidelines have been applied to several real-world system assessments, where a focus on the software risk control aspects was required. One of the advantages of the guidelines is that they provide the assessor with a standard approach from which an assessment can be built, since they guide the assessor through a software development lifecycle.

In practice, whilst the standard approach has been beneficial in organising the structure of an assessment, a number of problems do exist in the overall checklist headings and the internal questions. Strictly following the Guidelines, each question within a checklists should be answered either Yes, No or Not Applicable; but in reality, some questions are ambiguous and the responses do not easily fall into the above categories.

When questions are open to a number of different interpretations it is important to justify any response with a detailed commentary. Therefore when applying the Guidelines within CS more emphasis is placed on the commentary section for each question. This expanded commentary allows both the interpretation of the question to be defined and more importantly the assessor's findings. This approach within CS has led our assessors to use the adage "Has the spirit of the question been addressed", when reviewing any system.

The assessor's interpretation of a question and possible answers from this interpretation leads into another important aspect of applying the guidelines, that is, "what is the experience of the assessor?". As has been previously stated, several of the checklist questions are open to interpretation, therefore it is important that the assessor has the relevant experience and training in order to apply the guidelines in a meaningful manner. This fact is true for all assessment

approaches, but some organisations often believe that they can carry out a checklist assessment without any prior experience, simply because a checklist appears "easy" to complete.

When using the HSE PES Guidelines one problem which is commonly encountered is with the software development lifecycle model; the model presented in the HSE PES Guidelines is fairly rigid, and is particularly weak in the areas of testing and configuration control.

Perhaps the most significant problem with using checklists is "the robotic syndrome", ie where the assessor can fall into the trap of just addressing the questions within the checklists, rather than using the questions as a basis for further probing and uncovering strengths and weaknesses in the system being assessed. However, for a complete assessment some topics should be expanded and supplementary questions to those presented in the checklists should be used.

CS has resolved the above problem by including additional questions, where appropriate, and a final question, which is simply "Other?". The aim of including the "Other" question is it prompts the assessor to think of further questions; these questions may be due to inherent weaknesses or ambiguities of the existing questions, or due to supplementary questions derived from responses to earlier questions.

THE ASSESSMENT OF PROPRIETARY SOFTWARE

There is one category of software which is fraught with particular difficulty - proprietary software. There is an increasing trend for plant operators to employ systems with proprietary software embedded in them, the development of which is usually zealously guarded by the manufacture of such systems. The success of the assessment of proprietary/commercial grade software depends heavily on the software manufacturer to provide information on:

- the software development process, eg the standards and procedures used, the software QA applied, verification activities, configuration management, etc
- and the software product, eg: the amount of self-tests, fault tolerance, and the dynamic testing, static analysis, extent of validation undertaken, etc

This conflicts with the desire of the manufacturer to protect commercial secrets. Hence, the manufacturer is very careful as to who information is released to. Our experience shows that a manufacturer is much more amenable to releasing information to a 3rd party independent consultant, than to the end user, and even then signed agreements of non-disclosure are required.

But what if the manufacturer does not wish to release such information? There are ways of establishing (limited) confidence in the software based upon high level information, eg pedigree of the company and its products, stability of the software product, and use of the software in similar applications. This may or may not be adequate for a safety related system; the level of justification required will be determined by the dependence placed on the software by the system risk assessment. If the risk assessment requires a higher level of justification, and the manufacturer refuses to supply it to the assessor, then the system will not be justified against the

risk, and hence should not be used.

The SCOPE (Software Certification Programme in Europe) Project [SCOPE], an ESPRIT II project, was triggered by an EEC resolution to aim for a global approach for conformity and assessment, and it has addressed the above and other issues for a range of software categories. The evaluation methodology developed in this project has been accepted by an international standard [ISO IEC 9126], and it will soon be voted upon, to become a "DIS" - Draft International Standard.

Evaluation "bricks" have been applied to a number of case studies, and the results from these case studies have been fed back into the methodology. It is now possible to carry out an objective product assessment of commercial grade software in accordance with emerging European standards. This could be carried out at the lowest level if solely the documentation was available, or if the code were available, it could also be carried out as a much more detailed study via analysis tools, eg metrics.

PLC SYSTEMS

One particular example of proprietary software is in Programmable Logic Controllers (PLCs). The use of PLC systems is slowly increasing in the safety-related domain, and so assessment techniques for addressing these systems need to be derived. When assessing a PLC system, three main areas need to be addressed, the hardware system, the application software, and the embedded software, (amongst others, such as man-machine interface).

For the hardware system, several well-established techniques exist for the assessment task, but for the two software areas only limited techniques are available. When assessing the application software the task can be split into two areas: the assessment of the development process, and the assessment of the actual software product.

For the assessment of the development process several techniques are available, eg the HSE PES Guidelines checklists, but when assessing the software product several of the traditional techniques, eg Static Analysis, Metrics, are not useable. The reason for this is that analytical tools and techniques have not been developed for the types of language used to develop the application software, which is typically a form of "ladder logic".

Additionally, due to the intense competition within the PLC market there are few standards for ladder logic between manufacturers, who tend to develop their own particular language. When attempting to assess the PLC application, therefore, new manufacturer-specific techniques are required. But the problems in the assessment of the application language are minor when compared to the problems encountered in trying to attempt to assess that of embedded software. The embedded software, or commercial grade software, is the sole property of the PLC manufacturer and as such is a closely guarded commercial entity. The details of the development and maintenance procedures for the embedded software are therefore closely guarded, and the

manufacturer is highly reluctant to release these to an end user; however, CS has been allowed access to this type of software from a number of companies who wish to have the "pedigree" of their products established without releasing costly commercial "know-how".

The experiences of CS in the field of PLC assessment have been mixed. For application software there have been many improvements in recent years, particularly with the demand for companies to comply with UK and international quality standards [BS5750]. Compliance with BS5750 has resulted in improved quality assurance being applied throughout projects, including the software development phases. In addition, the manufacturers of PLC systems are now supplying improved software editors and compilation tools which allow some static and dynamic analysis to be performed.

The remaining problem with PLC assessment still lies in the assessment of the embedded software. To address this problem CS are participating in a project to develop guidelines for the assessment of embedded software [SAMPS].

As companies become increasingly aware of QA and safety issues, more pressure is being placed on the PLC manufacturers to supply evidence of the QA and development and testing process which applied to the product.

THE WAY FORWARD

A Procurement Framework

Numerous problems encountered in the assessment and licensing of software process arise from interaction problems between the assessor, regulator, and developer. These can be minimised by providing a generic, structured Procurement Framework to ensure that the relationships and responsibilities of the assessor, regulator, customer and developer are well-defined. The framework also requires that the development, justification and licensing activities are planned and scheduled together so that problem areas are rapidly detected and licensing delays are minimised. From the above, it is obvious that the assessment and licensing task should be considered as an exercise in communication, but more specifically, it should be considered as an exercise in formal written communication. This latter aspect cannot be over-emphasized.

The DARTS project has developed such a Procurement Framework, and is addressing the benefits of the above framework.

BUILDING ON CURRENT RESEARCH

In 1987 the UK Advisory Council for Applied Research & Development (ACARD) visualised the need for certification of not only the software, but of development organisations, their staff, and their development methods; ACARD also recommended the use of formal mathematical methods and suggested categorisation of systems based upon failure consequence, hence allowing

the amount of analysis to be geared to the failure consequence. This vision is now materialising with the advent of interim standards [MOD 0055] and [MOD 0056], and draft standards [IEC 65A/9] and [IEC 65A/10].

Some of the above trends, as perceived by CS, in assessing high integrity software based systems, are being addressed by CS via our participation in UK and EEC software research initiatives, building on previous and continuing collaborative research with the Halden Reactor Project, Norway. The focus of this research is to provide valuable guidance on the cost effectiveness of current technology in developing and assessing high integrity systems.

We believe that the DARTS guidelines, coupled with the maturing of formal system development approaches such as Z, VDM and OBJ will form the basis of the development of a cost effective development and assessment route for high integrity systems. This goal is being pursued through past and present research projects: Safety Assessment of Programs (SAP II), and Safe Formal Methods (SafeFM), [SafeFM].

The SafeFM project is a collaborative research initiative part funded under the Department of Trade and Industries" (DTI) SafeIT initiative. The project aims to provide guidelines for a cost effective approach using formal methods in the development and assessment of high integrity software systems. The project also aims to devise a methodology and calculus for constructing provably coherent system specifications.

REFERENCES

ATOM "Business Managers turn to Risk Assessment", Dr F R Allen, AEA Technology; Article in ATOM 428, (technical journal of AEA Technology, UK) May/June 1993.

BS5750 BS 57570 Part 1: 1987 (ISO 9001: 1987), "Quality Systems: Specification for Design/Development, Production, Installation & servicing"; British Standards Institution.

BSI 198 DD-198: Assessment of reliability of systems containing software, Draft for Development, British Standards Institute, 1991

DARTS "Software Licensing and Assessment - Problems and Solutions", M Barnes, P A Bradley, based on the DARTS project. Presented at the IEAE Specialists' Meeting on "Software Engineering in Nuclear Power Plants: Experience, Issues, and Directions", at AECL, Chalk River Laboratories, Pembroke, Ontario, Canada, 10 September 1992.

EUR EUROCAE ED-12B/DO-178B: Software Considerations in Airborne Systems and Equipment Certification, EUROCAE WG-12/RTCA SC-167, December 1992

EUR 1147 "Licensing Issues Associated with the Use of Computers in the Nuclear Industry", BLOOMFIELD R.E.; a CEC Report, EUR 1147 EN, 1987.

HSE PES HSE PES Guidelines: for Programmable Electronic Systems in Safety Related Applications. Part 2 "General Technical Guidelines". Produced by the UK Health and Safety Executive, and available from Her Majesty's Stationery Office, PO Box 26, London SW8 5DT

IAEA International Nuclear Safety Advisory Group Vienna 1988: IAEA Basic Safety Principles for Nuclear Power Plants, Safety Series No 75-INSAG-3), 1988, ISBN 9201231881

IEE/BCS Institute of Electrical Engineers, Software In Safety Related Systems, IEE/BCS Report, IEE, Oct 92

IEC 65A/9 "Software for Computers in the Application of Industrial Safety-Related Systems"; IEC 65A Secretariat (Working Group 9), BSI Draft Standard, Document 91/71012. (Draft Standard).

IEC 65A/10 "The Functional Safety of Programmable Electronic Systems: Generic Aspects; Part 1: General Requirements"; IEC 65A Secretariat (Working Group 10). (Draft Standard).

IEEE "PODS - A Project on Diverse Software", P G Bishop et al, article in IEEE Transactions on Software Engineering, Vol SE-12, No. 9, September 1986.

INF ST "Software Diversity: a way to enhance Safety?"; G Dahll, M Barnes, P G Bishop. Information & Software Technology, page 677, Vol 32, No.10, December 1990.

ISO IEC 9126 Draft ISO/IEC DIS 9126 "Information Technology - Software Product Evaluation - Quality Characteristics and Guidelines for their Use"; International Organisation for Standardisation, International Electrotechnical Commission, January 1991.

MOD 0055 "Requirements for the procurement of safety critical software in defence systems", UK Ministry of Defence, Interim Standard 0055 (parts 1&2).

MOD 0056 "Hazard analysis and safety classification of the computer and programmable electronic system elements of defence equipment", UK Ministry of Defence, Interim Defence Standard 0056.

NEUMANN "Illustrative Risks To The Public In The Use Of Computer Systems And

Related Technology", Neumann, PG, , Computer Science Lab, SRI International, Menlo Park CA 94025-3493.

NII Safety Assessment Principles for Nuclear Plants, Nuclear Installations Inspectorate, UK, ISBN 011 882043 5

NUCENG "Seeking a standard framework for dependable computing". Article published in Nuclear Engineering International, May 1989 page 30.

SafeFM "The Practical Application of Formal Methods to High Integrity Systems - The SafeFM Project", P Bradley, L Shackleton, V Stavridou, 1993, Directions in Safety Critical Systems, Proceedings of the Safety Critical Systems Symposium, Bristol 1993; ISBN 3-540-19817-2

SAMPS "An Investigation into Safety Assessment Methodologies for Proprietary Software", Brewer, MA, et al, Halden Reactor Project, Halden, Norway. Ref: SAMPS/03/MAB/191292, Issue 1.1, 1992.

SCOPE "SCOPE - a European Software Certification Initiative", M A Brewer, SRD Association Symposium, AEA Technology, August 1992, ISBN 0-85356-832-9

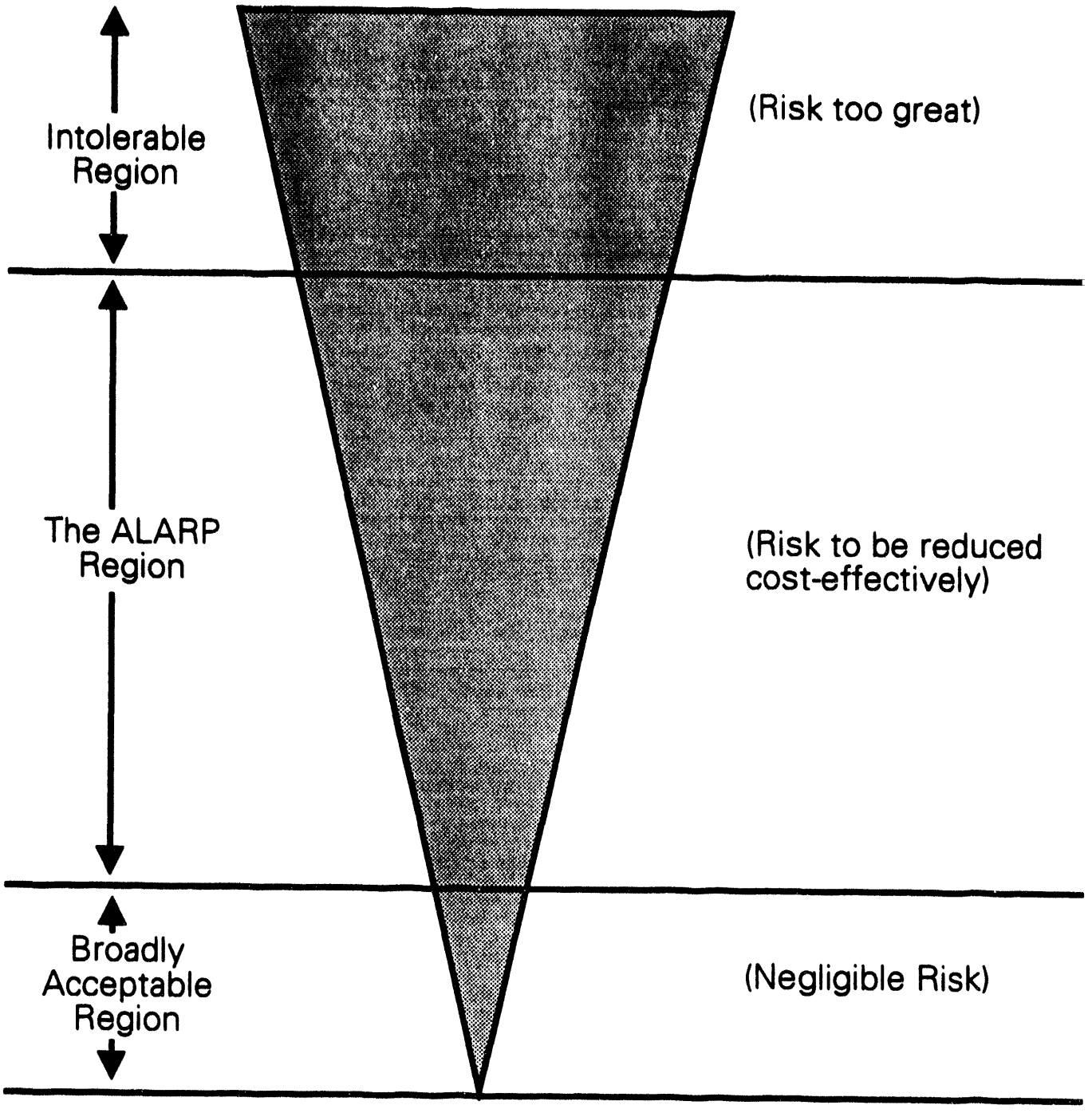


Figure 1 Tolerable Risk and ALARP

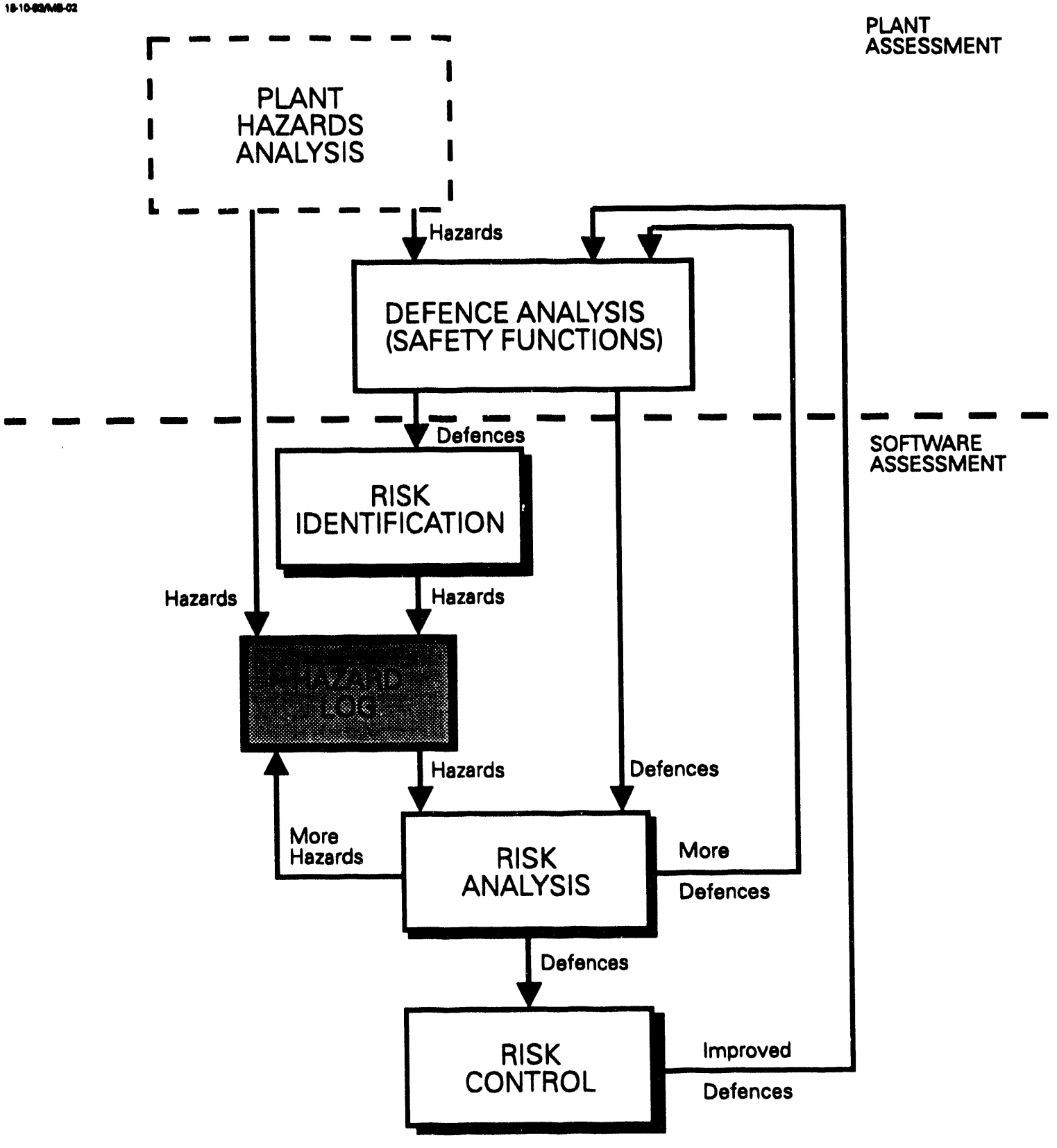


Figure 2 Software Risk Assessment Framework

Class 1E Software Verification and Validation: Past, Present, and Future[1]

Warren L. Persons and J. Dennis Lawrence
Lawrence Livermore National Laboratory
Fission Energy and Systems Safety Program
Computer Safety & Reliability Group

This paper[2] discusses work in progress that addresses software verification and validation (V&V) as it takes place during the full software life cycle of safety-critical software. The paper begins with a brief overview of the task description and discussion of the historical evolution of software V&V. A new perspective is presented which shows the entire verification and validation process from the viewpoints of a software developer, product assurance engineer, independent V&V auditor, and government regulator. An account of the experience of the field test of the Verification Audit Plan and Report generated from the V&V Guidelines is presented along with sample checklists and lessons learned from the verification audit experience. Then, an approach to automating the V&V Guidelines is introduced. The paper concludes with a glossary and bibliography.

1. INTRODUCTION

1.1. Task Description

The work in progress described in this paper builds upon previous work performed by the United States Nuclear Regulatory Commission (NRC), Office of Nuclear Regulatory Research (RES) and the Office of Nuclear Reactor Regulation (NRR) in the areas of verification and validation (V&V) guidelines for the evaluation of safety-critical software. The purpose of this effort is to field test the audit process and principles put forth in these guidelines. The major thrusts of this effort involve reviewing the V&V Guidelines, applying the guidelines to a verification and validation audit of Class 1E software, performing a cost/benefit analysis of computerizing the audit guidelines on a laptop computer to serve as an aid for reviewers, meeting with the NRC and guideline developers to discuss proposed modifications, and reporting on the work performed.

---

[1] This work was supported by the United States Nuclear Regulatory Commission under a Memorandum of Understanding with the U.S. Department of Energy, and performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

[2] The authors appreciate the guidance provided by the many discussions with Mr. Leo Beltracchi; Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, that led to concepts presented in this paper.

1.2. What is Class 1E Software?

IEEE Standard 379, *Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems* (1977), defines Class 1E as, "The safety classification of the electric equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment." In this paper, software used in Class 1E systems is referred to as Class 1E software. Class 1E software is currently being used in nuclear power plants and applications including (but not limited to) reactor trip systems and emergency generator load sequencers.

1.3. What is Software Verification and Validation?

The terms "verification," "validation," and "verification and validation" abound in the software literature and are used with various explicit or implicit meanings. Some of the diversification may be rooted in a particular author's need to customize the terminology so that it is appropriate for a specialized application area. Another reason may be the type or criticality of the software application; e.g., software applications range from a simple spreadsheet used to track hours an individual works on a project, to highly reliable flight control software used for the space shuttle. Intuitively, there is a difference in what V&V should mean in each case and in the amount of effort that should be applied to V&V activities for these extreme application types.

There is some consensus among software engineers that the activities of verification and validation are focused on the determination of whether the software performs its intended function and has the required quality attributes. This body believes that V&V as a formal discipline is near the midpoint of its development. As such, specific formal boundaries have yet to be established to define what the extent of the V&V functional activities should be. However, a large body of opinion agrees that V&V is one of the techniques used to help identify, assess, and manage risks in software development projects and can be carried out at varying levels of rigor, depending on the nature of the application and the risks involved in the development activity. The utmost rigor is required when one of the risks is safety.

The terms verification, validation, or verification and validation are used in this paper in accordance with the following IEEE Standard 610.12-1990 definitions:

Verification. The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of the phase.

Validation. The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.

Verification and validation. The process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and the final system or component complies with specified requirements.

1.4. What is the Problem?

Nuclear reactors, like any complex industrial plants, routinely experience equipment or operational failures, some of which could lead to serious consequences. Unlike many industrial plants, one potential consequence of reactor accidents is the release of radiation or radioactive material into the environment. Until the mid 1970s, software was not used in Class 1E systems, but a rapid transition into an era of computer and software control of these Class 1E systems is now occurring.

Many risks exist in the complex process of producing high-quality Class 1E software. Most software projects should be concerned with the risks of failing to meet cost and schedule goals. In some cases, there are additional technological risks due to the use of new hardware, new programming languages, new design techniques, or new software tools. When safety is at issue, special attention must be paid to all of the above risks as well as to the special risks to human life and health, property, and the environment. Software developers must build safe and reliable software products that satisfy the requirements allocated to the software portion of the Class 1E system. In particular, unless the set of software development activities is carefully managed, the complexities and uncertainties inherent in these procedures can cause unnecessary risk, delays, and expenses.

An aspect of the problem is that building any system or any software system is effectively a problem-solving exercise. As such, all of the difficulties associated with problem solving are encountered during the software development activity. In particular, there are limitations in the software engineer's communication skill, ability, experience, problem understanding, flexibility to view the problem from multiple perspectives — that is, the ability to shift paradigms — as well as normal technical difficulties associated with any problem-solving endeavor. Other components of the problem are specific to software development. First, software development is a labor-intensive, intellectual activity. A noted software expert, Edgar Dijkstra, stated in 1969 that software development is one of the most intellectually challenging activities in which humans can engage. Second, software does not wear out and hence, does not fail in the same manner that hardware does. Software can contain manufacturing or design defects which can produce hazards and failures in operational use. It is quite common for software errors to be very subtle and to be completely overlooked during implementation, but their presence can cause catastrophic failure after years of apparently successful operation.

1.5. What Makes Class 1E Software Different?

Considering the extensive use of computers and software during the last 20 years in various applications, why is there concern over the application of this technology to Class 1E systems? Simply stated, the following Class 1E software attributes raise the level of concern and make it different:

- Potential risk to life, property and environment,
- Safety requirements, and
- High reliability requirements.

There are two central concepts that are key to the development of Class 1E software. First, software safety and reliability considerations cannot be fully understood in isolation from

computer hardware and application considerations. Second, the process of engineering reliability and safety into a computer system requires activities to be carried out throughout the software life cycle. Thus, the development, use, and regulation of computer systems in nuclear reactors is a complex issue.

1.6. General Approaches to Increase Confidence in Class 1E Software

There are two general approaches for increasing the confidence of Class 1E software systems, as shown in Figure 1: (1) reducing, if not eliminating, the number of errors introduced during the software development process, and (2) increasing the percentage of overall errors found prior to system installation. Note that Figure 1 shows only one sample translation that occurs during the software development process. In this case, a translation is shown from the requirements, allocated by the Class 1E system to the Class 1E software, to the software design. Similarly, there are translations from design to code, from code to integrated components, and so forth, throughout the software development process. Each translation provides opportunities to insert or inject errors and to detect inserted errors. The goal is to insert fewer errors and simultaneously detect more errors as each translation occurs during the software development process. The goal is "error free software;" the focus is on continual process improvement and eliminating errors before they are propagated. For Class 1E software, both methods are appropriate.

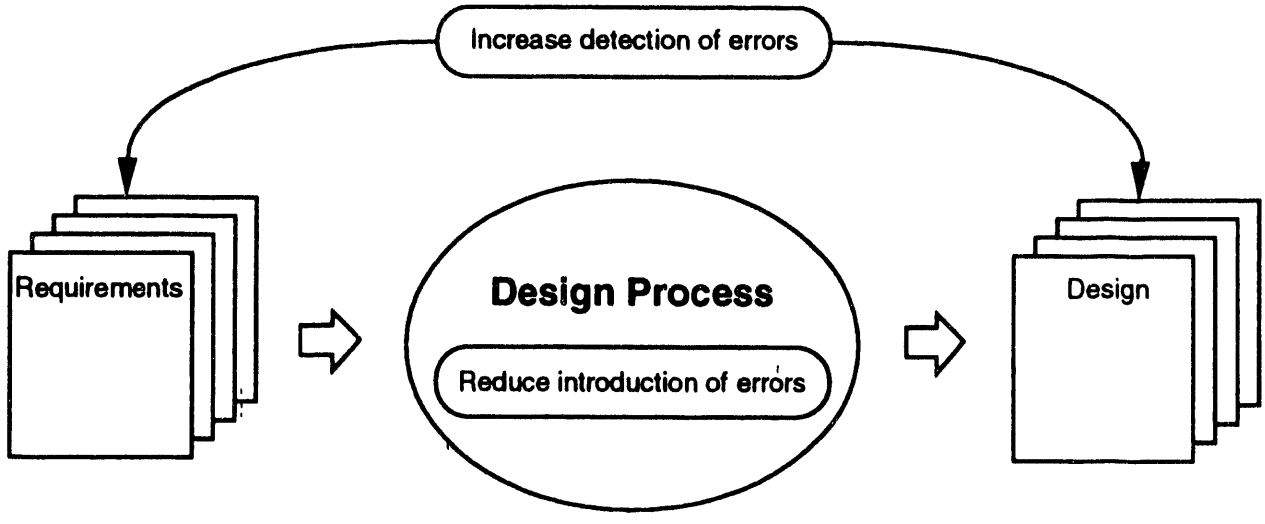


Figure 1. Reduction of Errors Versus Detection of Errors

1.7. Issues Associated with Class 1E Software

If a comparison is made between current electro-mechanical Class 1E systems and software-based Class 1E systems, several issues related to the use of software in these systems can be identified:

- Lack of experience in developing Class 1E software.
- Inability to measure required, ultra-high software reliability.
- Lack of a mathematical basis for safety-critical software construction.
- Difficulty in formally proving software correctness.
- New potential for common-mode failures.
- Lack of operational data.
- Small errors may have significant consequences.

In spite of this, software-based systems may be the only reasonable alternative for replacing aging nuclear reactor protection system components. Traditional analog/relay equipment is becoming much more expensive and, in some cases, is totally unavailable. If substitute equipment is available, it often contains embedded digital hardware and software which share the issues just listed. A large body of opinion, however, believes that with proper use of modern software engineering practices, the number of residual defects in delivered Class 1E software can be reduced to an acceptable minimum, and these remaining defects will not have severe consequences.

Many risks are involved in the development of Class 1E software for use in nuclear power generating stations. For example:

- Delaying an audit or evaluation until the end of the development effort can be very expensive. Extensive industry experience shows that errors are more easily fixed and less expensive to fix if they are found in early development phases.
- Delaying evaluations until after the development effort is complete may require more extensive proof that the safety requirements have been met, and it may actually be impossible at this point to assess the safety of the system.
- Inconsistencies among auditors, or by a single auditor over a period of time, can lead to unsettling differences in evaluation results and required corrective actions.
- Evaluations are inherently labor-intensive procedures. Lack of computer assistance increases the time and effort involved in performing these evaluations, which results in increased costs to both the developer and the regulatory agency.
- A possible result of these uncertainties and increased costs can be less-reliable software, which in turn can increase the difficulty of assessing the safety of the reactor.

2. THE EVOLUTION OF V&V

In the early history of computing, software was produced without a clear written document describing, beforehand, what the software was supposed to do. In some cases the results of a

particular software task surprised even those who were responsible for the detailed implementation. Many "features" were discovered as testing and use proceeded. A lack of discipline in the software development process wasted resources and caused considerable customer dissatisfaction. It was discovered by some software vendors that the production of a requirements specification prior to the writing of code led to a better product and reduced costs. But surprises still occurred. Testing was made more formal and it became more meaningful because there was a requirements specification against which to test. The requirements' specification also improved as ambiguous and untestable elements were removed from the specifications. Still, the results tended to contain "features" which were undesirable and defects which were discovered only during use.

Discipline in software development became more formalized and the notion of "design" was introduced as a formal step in the software development life cycle. It was recognized by some that software development is an "engineering" discipline and the term "software engineering" was introduced. Quality control and quality assurance issues were addressed as reviews and inspections slowly made their way into the software development life cycle. Configuration management was introduced as software engineering matured.

The notion of a software life cycle became commonplace with activities such as: planning, requirements, design, implementation, test, installation, operation and maintenance, and retirement. The terms "verification" and "validation" (termed collectively V&V) were introduced as part of the engineering discipline. Originally, V&V applied only to the technical products of the software development process. The managerial and product assurance aspects of software development were not originally subjected to V&V.

Both product assurance and configuration management can trace their historical roots to the hardware side of the engineering discipline. On the other hand, V&V came into existence to cope with software and its development. Gradually it was recognized that preventive testing was a part of management's tool kit for risk management and that testing should have a life cycle of its own. Testing should be planned, analyzed, designed, implemented, executed, and the results recorded. Moreover, each of these activities should be subject to inspections and reviews, with the results of each activity placed under configuration control.

Software projects and products have evolved from small systems that were typically developed by a few people to much larger, more complex systems involving up to several hundred people on the software development team. This change in the characteristics of software projects and products has caused a radical change in the notion of verification and validation. Originally, V&V was very informal and individualized and was focused on testing. Early V&V merely involved the programmer exercising the code that was produced. As the software systems were required to perform more and more functions, and the resulting systems became larger and more complex, the neglect of planning, design and execution of test procedures and test cases led to poor quality and to defective, unreliable software products.

Some companies have discovered that, when risks are high, V&V should apply to all aspects of software development. Companies which produce software for safety-critical applications are beginning to use a much more formal V&V process. This notion of V&V extends beyond the traditional restriction to technical aspects of software development in order to include

management and product assurance. This can only be done by an organization which is independent of the developer. Independent V&V (IV&V) is performed on all software products which are part of the software engineering and product assurance activities. In particular, this independent analysis must give considerable attention to identifying, assessing, and managing risks and hazards.

The overall goal of IV&V is to ensure that software quality is achieved. Part of this goal is achieved by providing specific visibility into the entire development process so that management decisions can be made to assure appropriate software quality. IV&V continues to evolve as software development projects change and has become a very powerful management tool.

3. A PERSPECTIVE ON V&V

3.1. Software Evaluation Perspectives

Any software evaluation process can be discussed from several different viewpoints. The viewpoint that is presumed has a considerable effect on the topics discussed, and particularly the emphasis placed on different aspects of the evaluation process. In this discussion, three viewpoints are considered: the regulatory view, the independent verification and validation view, and the software development view. Each viewpoint, as shown in Figure 2, has its own goals, evaluation perspective and activities, which are described below.

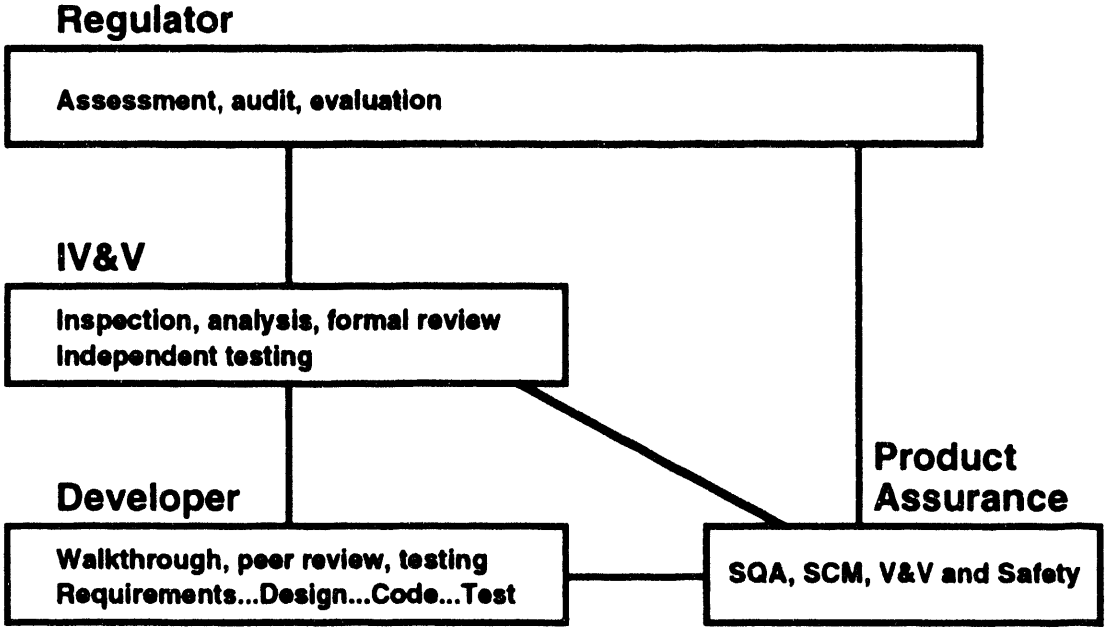


Figure 2. Model for Software Evaluation

3.2. Developer's Viewpoint

In this paper it is assumed that the developer of Class 1E software defines the methods to be used to deliver that software in a project plan, which is subject to regulatory approval. Once approved, the software developer is held accountable for development in accordance with the project plan. This two-step sequence of project plan approval followed by project plan accountability offers both flexibility on the part of the developer and insight on the part of the regulatory agency. The separation of the development function into the equivalent of requirements, design, implementation, integration, validation, installation, and operations and maintenance activities is a fairly standard practice.

The software developer will carry out certain product assurance activities, as suggested in Figure 2. In this paper, the term "product assurance" is used to cover the developer's activities which relate to V&V, testing, software quality assurance (SQA), software configuration management (SCM), and safety analysis. The developer's product assurance provides the first objective evidence of the quality of the development effort.

3.3. IV&V Viewpoint

The ultimate result of the software development process, as considered here, is a suite of computer programs and its related documentation. The documentation guides the user, developer, installer, and maintainer of the software throughout the life cycle. These programs must have characteristics such as safety, reliability, performance, usability and function. The purpose of IV&V is to provide independent assurance that the required characteristics have been met by the developer. The importance of IV&V is emphasized in various standards listed in the bibliography at the end of this paper.

3.4. Regulator's Viewpoint

Regulators are required by legislation to license nuclear power generation stations. One aspect of this is to analyze the evaluations performed by the software developer (in the form of product assurance activities) and the IV&V team activities. This may best be done using standards (such as those found in the bibliography) to help evaluators perform assessments or audits in an efficient cost-effective fashion. These audits or assessments should be consistent over time, across companies, and across projects within companies.

4. THE VERIFICATION AUDIT FIELD TEST

4.1. Verification Audit Context

The first major activity on the field test was to review and apply the V&V Guidelines to the development of an audit plan to be used to audit existing Class 1E software components. The V&V Guidelines were provided as NRC-furnished material. This audit was performed at a vendor's facility in January 1993 and was conducted by an interdisciplinary audit team consisting of personnel from NRC/NRR, SoHaR Incorporated, and Lawrence Livermore National Laboratory. The audit evaluated both the software development process used to develop Class

1E software products that are components of Class 1E systems, and the products of that process.

Figure 3 identifies checkpoints at which software audits of the software development activities, processes, or products can be performed. The number of audits depends, among other things, on the specific software life cycle used by the vendor or software developer. Each audit analyzes the work done relative to that checkpoint. Many reliability, performance, and safety problems can be resolved only by careful design of the software product, so they should be addressed early in the software development process, no matter which life cycle is used. Any errors or oversights can require difficult and expensive retrofits, so they too are best found as early as possible. Consequently, an incremental V&V audit process is believed to be more effective than a single audit or evaluation at the end of the development process. Using multiple audits, problems can be detected early in the software life cycle and corrected before large amounts of resources have been consumed.

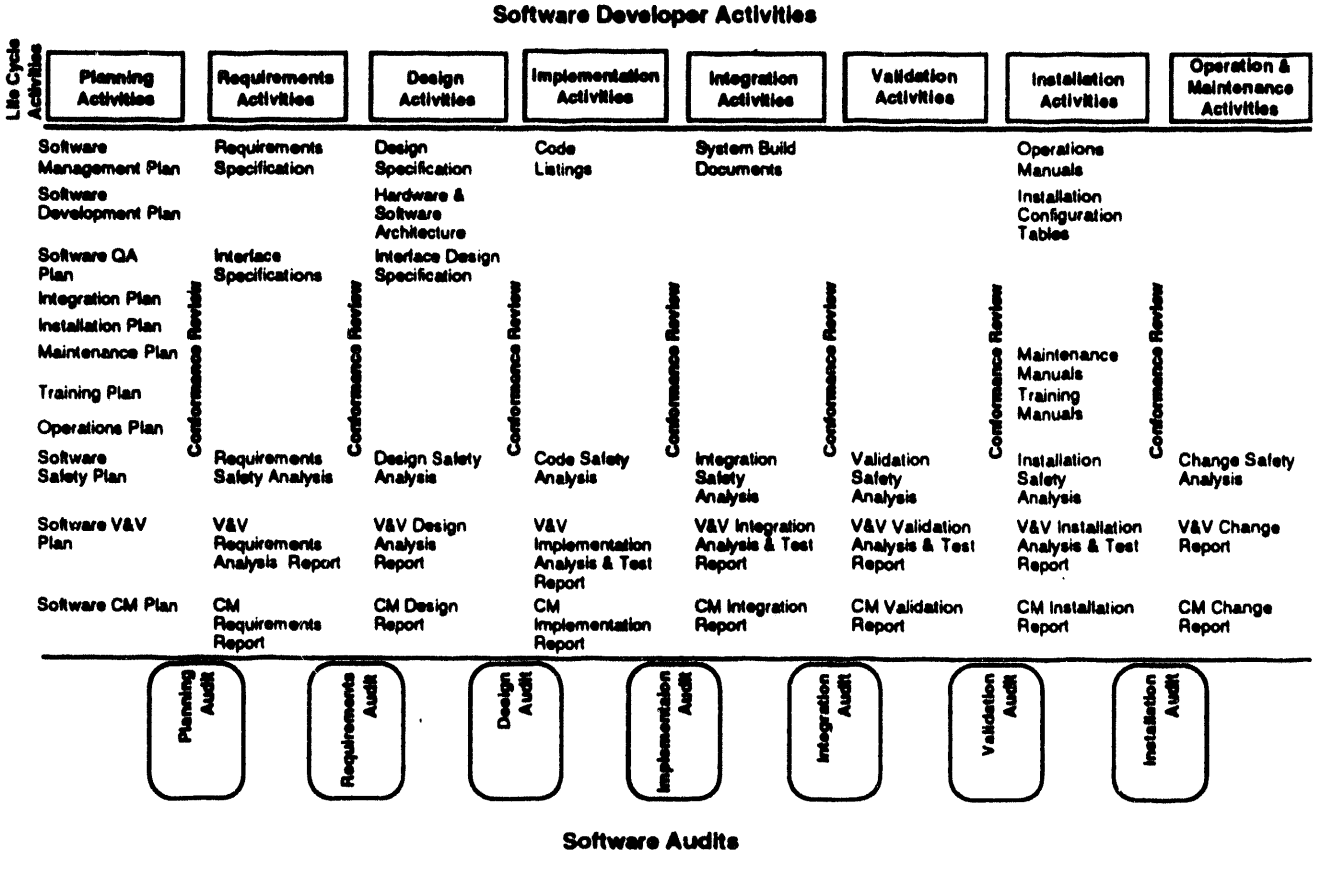


Figure 3. Class 1E Software Life Cycle Activities

4.2. Verification Audit Process Description

The audit process proposed in the guidelines consists of four phases:

- Audit Preparation Phase,
- Audit Performance Phase,
- Audit Reporting Phase, and
- Audit Close-out Phase.

The majority of the effort is expended during the Audit Preparation Phase, which is performed before the on-site visit. This phase consists of the definition of the audit purpose, identification of the audit scope, and identification of the audit performance standards. During this phase, interactions with the vendor occur to obtain required audit material and to tailor the audit plan to the vendor's software development process. This phase is complete with the selection and orientation of the audit team. The next phase, the Audit Performance Phase, begins with the entry briefing or opening meeting, and includes performing the audit using the audit procedures and checklists prepared in the audit plan, the daily audit team meetings, and the daily briefings to vendor management. The Audit Reporting Phase begins with the audit exit briefing or closing meeting and concludes with the production of the Audit Report. It should be noted that the Audit Report is the only product produced by the audit team as part of the audit process. As such, this document is extremely important since it is the only evidence that the audit actually occurred. The Audit Close-out Phase consists of interaction between the NRC and the vendor as findings are reviewed and corrective actions are planned and analyzed.

4.3. Verification Audit Processes and Products Audited

As shown in Figure 3, the set of software development activities performed during the software development process, in accordance with a particular vendor software life cycle, uses several processes to produce software products. It should be noted that some of the processes are totally contained within a specific set of software development activities, such as the process that is used to produce the software V&V Plan. On the other hand, some processes span several sets of software development activities. A case in point is the software configuration management process, which spans all sets of software development activities. In all cases, the processes used for software development produce interim software products that can each be evaluated. The verification audit field test described in this paper looked at the following software processes and products: software planning, software requirements, software safety requirements, software safety analysis, software verification and validation, software configuration management, software design, software implementation, software test, and hardware and software integration activities.

4.4. Verification Audit Sample Checklists

Each of the processes and products shown in Figure 3 can and should be evaluated using a checklist or set of questions developed for the audit plan using the guidance provided by the V&V Guidelines. Portions of sample checklists used to evaluate software products are shown below. These include partial samples of the following software products; namely, a software development plan, a software requirements specification, and a software code safety analysis.

More detailed information can be found in the field test verification audit plan. (See Persons 1993a.)

4.4.1. Sample Software Development Plan Checklist

The following is a sample of a verification audit checklist that can be used to audit a software development plan for a Class 1E software project.

Software Development Plan Checklist

The Software Development Plan is the plan that guides the technical aspects of the development project. It will specify the life cycle that will be used, and the various technical activities that take place during that life cycle. All methods, tools and techniques which are required in order to perform the technical activities will be identified.

1. **Life Cycle Process Questions.**
   a. Is a software life cycle defined?
   b. Are the defined life cycle processes sufficient to provide confidence that a safe and adequate product will be produced?
   c. Are the inputs and outputs defined for each life cycle process?
   d. Is the source of each life cycle process input specified?
   e. Is the destination of each life cycle process output specified?
   f. Does each life cycle phase require a safety analysis?
   g. Does each life cycle phase include a requirement for an audit at the end of the phase?

4.4.2. Sample Software Requirements Checklist

The following is a sample of a verification audit checklist that can be used to audit a software requirements specification (SRS) for a Class 1E software project.

Software Requirements Specification (SRS) Checklist

The Software Requirements Specification (SRS) documents all the software requirements. These come from the specific system or product design and the specific system or product hazard analysis.

1. **User Characteristics Questions.**
   a. Is each category of user identified in the SRS?
   b. Is the expected experience level of each category of user defined?
   c. Are the training requirements for each category of user defined?

6. **Performance Requirements Questions.**

   a. Are all static performance requirements fully described?

   b. Are all system timing requirements included in the SRS?

   c. Are the timing requirements specified numerically?

   d. Are timing requirements expressed for each mode of operation?

4.4.3. Sample Code Safety Analysis Checklist

The following is a sample of a verification audit checklist that can be used to perform a code safety analysis audit for a Class 1E software project.

Code Safety Analysis Checklist

The purpose of the safety analysis is to identify any errors or deficiencies in the code which could contribute to a hazard.

1. **Logic Questions.**

   a. Does the code logic correctly implement the safety-critical design criteria?

   b. Are design equations and algorithms correctly implemented in the code?

   c. Does the code correctly implement the error handling design?

   d. Does the code correctly implement the off-normal and emergency operations design?

   e. Is there convincing evidence that no code considered to be non-critical can adversely impact the function, timing, and reliability of the safety-critical code?

   f. Is there convincing evidence that any interrupts that may be included in the code will not take precedence over or prevent the execution of safety-critical code modules?

2. **Data Questions.**

   a. Are the definition and use of data items in the code consistent with the software design?

   b. Is each data item in the code explicitly typed?

   c. Is there a convincing argument that no safety-critical data item can have its value changed in an unanticipated manner, or by an unanticipated module?

   d. Is there a convincing argument that no interrupt can destroy safety-critical data items?

4.5. Verification Audit Report

The verification audit report is the only product of the audit team and serves as evidence that the audit was performed. It encapsulates the audit scope, purpose, audit process used, and associated information. Based on the V&V Guidelines, a sample audit report was generated and used for the field test verification audit. More specific information can be found in the verification audit report. (See Persons 1993b). A sample table of contents for a typical verification audit plan is shown below:

- Executive Summary
- Introduction
- Software Verification Audit Description
  - Scope
  - Purpose
- Definitions and Acronyms
- Identification of the Auditors
- People Contacted
- Software Verification Audit Summary
- Software Verification Audit Results
  - Findings
  - Observations
  - Concerns
- Recommendations
- Positive Indications
- Software Verification Audit Procedure
- References
- Attachments
  - Audit Plan
  - Audit Schedule
  - Entrance Briefing Viewgraphs
  - Vendor Approach to Software Development
  - Completed Checklists.

Most of the table of contents entries are self-explanatory; however, it should be noted that the Software Verification Summary includes all the processes and products that were analyzed during the audit. In addition, the Verification Audit Procedure section should describe the audit procedures and checklists that were used to perform the verification audit.

4.6. Verification Audit Lessons Learned

Audits are of necessity conducted during a very limited time frame. The V&V Guidelines provide guidance as to how to increase the effectiveness of audits for safety-critical software performed within the limited time available. The purpose of V&V Guidelines, audit plans, audit procedures, and audit checklists is to aid the audit team in the final evaluation of the risk associated with the safety-critical software in question.

Focus on the software development process and its related products provides visibility into the software planning, management, analysis, design, implementation, and testing phases and greatly increases the understanding of the various software development and product assurance processes. It provides a valuable framework for the auditors as they make their determination as to whether the licensee/vendor complies with applicable standards for Class 1E software for nuclear power plants. The following are lessons learned which, when incorporated into the V&V Guidelines, should yield a more powerful assessment tool for verification audits that will serve both Class 1E software developers and NRC regulators alike.

- A pre-audit visit should be performed to establish the scope and purpose of the audit.
- Review of the vendor's software development process should be completed prior to developing the verification audit plan.
- Review of available system and software development documentation should be completed in advance of the on-site visit.
- Tailoring of the audit process to the vendor's software development process should be completed as part of the audit plan development.
- The auditee should be given advance notification of the materials to be reviewed by the audit team.
- Several verification audits should occur to assess the software processes and products as they are created. Start the audit process early in software development life cycle with a review of the planning documentation.
- The audit team should include specialists in the specific processes and/or products under evaluation. The composition of the audit team can and should change from one verification audit to another.
- The audit process is labor-intensive and attention to detail is required.
- A two-level evaluation process is desirable. The first level screens the processes or products to determine if further evaluation is appropriate.
- The audits need to be consistent across time and companies. Knowledge of past audits of the same process or product is desirable and helpful in performing the current verification audit.
- Easy access to standards is helpful.
- Automated assistance for the audit team in the creation of daily activity summary and interim documentation would make the audit process more efficient.

5. FUTURE VISION OF CLASS 1E EVALUATION

The evaluation of Class 1E software by the regulator should be consistent with the developer's life cycle. Many different life cycle models exist and are used by software development companies, but they include the same basic activities. These models differ primarily in the ordering of activities through time. As a result, the regulator can concentrate on evaluating the activities as they occur during the developer's life cycle. Because of this variation between life cycle models, evaluation means must exist for each different activity in the life cycle. This argument is the basis for the vision presented in this paper.

This vision of future Class 1E software evaluation suggests a change in perspective that involves computer assistance for the evaluation process. Human Factors studies and task analysis experiences suggest that there is a general pattern for automating any process. As applied to the regulatory evaluation process, the following steps are useful:

- Control the complexity of the audit process.
- Define and separate the audit activities by software life cycle activity.
- Define activity-specific audit procedures.
- Develop support tools to encourage the use of consistent evaluation practices.
- Develop an integrated environment to assist in the audit process.

5.1. Automation Issues

To be successful in introducing automated support into auditing Class 1E software, an integrated approach is suggested that includes the auditor, methods, tools, and data. Goals for the support environment include increased accuracy; consistency and productivity; ability to customize to specific evaluation needs; and acceptance by the auditors.

Automated support for audits or evaluations raises several issues that needed to be addressed.

- Increasing consistency among auditors.
- Reducing the time and effort required to perform an audit.
- Training team members in the use of the evaluation process and supporting tools.
- Determining the processes and products to be audited.
- Defining the audit process.
- Tailoring the evaluations to life cycles used by different companies.
- Maintaining consistency among tools.
- Providing a common user interface.
- Maintaining a data base of past audits.
- Maintaining a data base of important guidance and standards.
- Providing security and access control.

5.2. Automation Architecture

A conceptual architecture for an automated approach is shown in Figure 4. Suppose that an audit is imminent. Through the graphical user interface the auditor selects the developer's activities to be evaluated. The automated support provides appropriate tools, standards, and guidance for use in the specific audit and then guides the auditor through that process.

This conceptual architecture has two objectives. The first objective is to provide step-by-step guidance to the evaluator in the use of the evaluation process. The second objective is to provide automated support for preparing the auditor's documentation, including the audit plan, supporting data, the audit report, and information that is to become part of the historical data base. A cost/benefit analysis of such an automated approach is in progress.

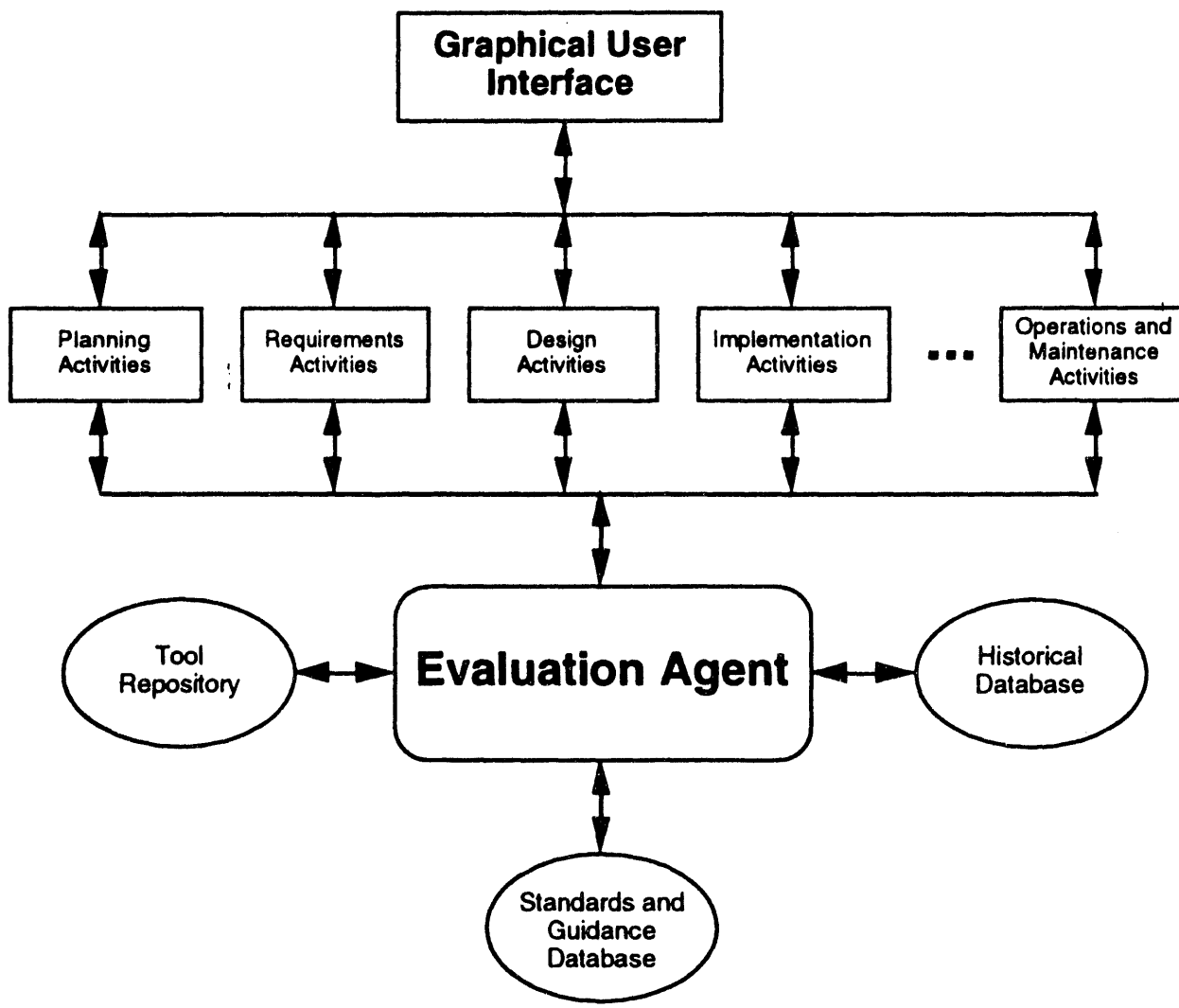


Figure 4. Conceptual Architecture of the Evaluation Assistant

GLOSSARY

audit. An independent evaluation of software products or processes to ascertain compliance to standards, guidelines, specifications, and procedures based on objective criteria that include documents that specify:
(1) the form or content of the products to be produced
(2) the process by which the products shall be produced
(3) how compliance to standards or guidelines shall be measured. (IEEE Std. 610.12).

Class 1E software. The safety classification of the electric equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment. Software used in Class 1E systems is referred to as Class 1E software. (IEEE Standard 379).

Class 1E system. The safety classification of the electrical equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling and containment and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment. (IEEE Std. 379).

evaluation. Determination of fitness for use. (IEEE Std. 1074).

procedure. (1) A course of action to be taken to perform a given task. (2) A written description of a course of action as in (1); for example, a documented test procedure. (IEEE Std. 610.12-1990).

process. (1) A sequence of steps performed for a given purpose; for example, the software development process (IEEE Std. 610.12). (2) A function that must be performed in the software life cycle. A process is composed of activities. (IEEE Std. 1074).

product assurance. The software developer's activities which relate to verification and validation, testing, software quality assurance (SQA), software configuration management (SCM), and safety analysis.

review. An evaluation of software element(s) or project status to ascertain discrepancies from planned results and to recommend improvement. This evaluation follows a formal process (for example, management review process, technical review process, software inspection process, or walkthrough process). (IEEE Std. 1028).

safety. (1) Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment (MIL-STD 882C). (2) The expectation that a system does not, under defined conditions, lead to a state in which human life, limb and health, economics or environment are endangered. Note: For system safety, all causes of failures which lead to an unsafe state shall be included; hardware failures, software failures, failures due to electrical interference, due to human interaction and failures in the controlled object. Some of these types of failure, in particular random hardware failures, may be quantified using such measures as the failure rate in the dangerous mode of failure or the probability of the protection system failing to operate on demand. The system safety also depends on many factors which cannot be quantified but can only be considered qualitatively. (IEC 65A (Secretariat) 122).

safety-critical software. (1) Software whose inadvertent response to stimuli, failure to respond when required, response out-of-sequence, or response in unplanned combination with others can result in an accident. Also, software that is intended to mitigate, or recover from the result of an accident (IEEE P1228 Draft E). (2) Software which ensures that a system does not endanger human life, limb and health, or the economics of environment of the capital equipment and control. (IEC 65A (Secretariat) 122).

software development process. (1) The process by which user needs are translated into a software product. The process involves translating user needs into software requirements, transforming the software requirements into design, implementing the design in code, testing the code, and sometimes, installing and checking out he software for operational use. Note: These activities may overlap or be performed iteratively (IEEE Std 610.12). (2) A set of activities, methods, practices, and transformations that people use to develop and maintain software and the associated products (e.g., project plans, design documents, code, test cases, user manuals, etc.). (CMU/SEI-91-TR-24).

software life cycle (SLC). A project-specific, sequenced mapping of activities. (IEEE Std. 1074).

software reliability. The probability that software will not cause the failure of a system for a specified time under specified conditions. The probability is a function of the inputs to and use of the system as well as a function of the existence of faults in the software. The inputs to the system determine whether existing faults, if any, are encountered. (IEEE Std. 982.1).

software product. (1) The complete set of computer programs, procedures, and possibly associated documentation and data designated for delivery to a user. (2) Any of the individual items in (1). (IEEE Std. 610.12).

task. The smallest unit of work subject to management accountability. A task is a well-defined work assignment for one or more project members. Related tasks are usually grouped to form activities. (IEEE Std. 1074).

validation. The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements. (IEEE Std. 610.12).

verification. The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase. (IEEE Std. 610.12).

verification and validation. The process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and the final system or component complies with specified requirements. (IEEE Std. 610.12).

BIBLIOGRAPHY

Andriole, S. J., Editor, *Software Validation, Verification, Testing and Documentation*, Petrocelli Books, 1986.

AFSC/AFSLC Pamphlet 800-5, Acquisition Management: Software Independent Verification and Validation (IV&V), 1988.

ANS-10.4-1987, *American National Standard for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry.*

American Society of Mechanical Engineers.

ASME NQA-1-1989, *Quality Assurance Program Requirements for Nuclear Facilities.*

ASME NQA-2-1989, Proposed Addition to ANSI/ASME-NQA-2, Part 2.7, *Quality Assurance Program Requirements for Nuclear Facility Applications*, Draft 3.3.

CMU/SEI-91-TR-24, *Capability Maturity Model for Software*, Version 1.1, February 1993.

DO-178B, *Requirements and Technical Concepts for Aviation*, Draft Revision to *Software Consideration in Airborne Systems and Equipment Certification.*

DOD-STD-2168, Military Standard, *Defense System Software Quality Program*, 29 April 1988.

Institute of Electrical and Electronic Engineers.

IEEE-ANS-7-4.3.2-1982, *Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations.*

IEEE 379-1977, *Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems.*

IEEE 603-1991, *Criteria for Safety Systems for Nuclear Power Generating Stations.*

IEEE 610.12-1990, *IEEE Standard Glossary of Software Engineering Terminology.*

IEEE 730-1989, *IEEE Standard for Software Quality Assurance Plans.*

IEEE 828-1990, *IEEE Standard for Software Configuration Management Plans.*

IEEE 830-1984, *IEEE Guide to Software Requirements Specifications.*

IEEE 982.1-1988, *IEEE Standard Dictionary of Measures to Produce Reliable Software.*

IEEE 983-1986, *IEEE Guide for Software Quality Assurance Planning.*

IEEE 1012-1986, *IEEE Standard for Software Verification and Validation Plans.*

IEEE 1016-1987, *IEEE Recommended Practice for Software Design Descriptions.*

IEEE 1028-1988, *IEEE Standard for Software Reviews and Audits.*

IEEE 1042-1987, *IEEE Guide to Software Configuration Management.*

IEEE 1058-1987, *IEEE Standard for Software Project Management Plans.*

IEEE 1074-1991, *IEEE Standard for Developing Life Cycle Processes.*

IEEE 1228 Draft (1993), *IEEE Standard for Software Safety Plans*, Draft J.

IEEE 1298-1992, *IEEE Standard Software Quality Management System.*

International Electrotechnical Commission.

IEC Standard Publication 880-1986, *Software for Computers in the Safety Systems of Nuclear Power Stations.*

IEC 65A (Secretariat) 122 (1989), *Software for Computers in the Application of Industrial Safety-Related Systems*, August 1, 1991.

International Organization for Standardization.

ISO 9000-1987, *Quality Management and Quality Assurance Standards — Guidelines for Selection and Use.* This is also ANSI/ASQC Q90-1987, *Quality Management and Quality Assurance Standards — Guidelines for Selection and Use.*

ISO 9000-3, *Quality Management and Quality Assurance Standards — Part 3: Guideline for the Application of ISO 9001 to the Development, Supply and Maintenance of Software.*

ISO 9001, *Quality Systems — Models for Quality Assurance in Design/Development, Production, Installation, and Servicing.*

ISO 9002, *Quality Systems — Models for Quality Assurance in Production and Installation.*

ISO 9003, *Quality Systems Models for Quality Assurance in Final Inspection and Test.*

ISO 9004, *Quality Management and Quality Elements — Guidelines.*

MIL-HDBK-286, Military Handbook, *A Guide for DOD-STD-2168 Defense System Software Quality Program*, 14 December 1990.

MIL-STD 882C, *Military Standard System Safety Program Requirements.*

Nuclear Regulatory Commission.

NUREG-0493, *A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System.*

NUREG-4640, *Handbook of Software Quality Assurance Techniques Applicable to the Nuclear Industry*, 1987.

Persons, Warren L., "Software Verification Audit Plan," Lawrence Livermore National Laboratory, Livermore, CA, 1993a.

Persons, Warren L., "Software Verification Audit Report," Lawrence Livermore National Laboratory, Livermore, CA, 1993b.

COMPARISON OF THE EFFECT OF PAPER AND COMPUTERIZED PROCEDURES ON OPERATOR ERROR RATE AND SPEED OF PERFORMANCE

Sharolyn A. Converse, Pedro B. Perez,
Steve Meyer, and Walden Crabtree

North Carolina State University
Raleigh, North Carolina, USA

Abstract

The Computerized Procedures Manual (COPMA-II) is an advanced procedure manual that can be used to select and execute procedures, to monitor the state of plant parameters, and to help operators track their progress through plant procedures. COPMA-II was evaluated in a study that compared the speed and accuracy of operators' performance when they performed with COPMA-II and traditional paper procedures. Sixteen licensed reactor operators worked in teams of two to operate the Scaled Pressurized Water Reactor Facility at North Carolina State University. Each team performed one change of power with each type of procedure to simulate performance under normal operating conditions. Teams then performed one accident scenario with COPMA-II and one with paper procedures. Error rates, performance times, and subjective estimates of workload were collected, and were evaluated for each combination of procedure type and scenario type. For the change of power task, accuracy and response time were not different for COPMA-II and paper procedures. Operators did initiate responses to both accident scenarios fastest with paper procedures. However, procedure type did not moderate response completion time for either accident scenario. For accuracy, performance with paper procedures resulted in twice as many errors as did performance with COPMA-II. Subjective measures of mental workload for the accident scenarios were not affected by procedure type.

Comparison of the Effect of Paper and Computerized Procedures on Operator Error and Speed of Performance

Sharolyn A. Converse, Pedro B. Perez,
Steve Meyer, and Walden Crabtree

North Carolina State University
Raleigh, North Carolina, USA.

INTRODUCTION

The majority of event reports for nuclear power plants (NPPs) in the United States list problems caused by operating procedures as important determinants of errors [1] [6]. In the United States, NPP operating procedures are typically symptom-based guidelines that list a set of sequential steps that must be taken in response to a particular normal or abnormal plant parameter. Each step consists of one or more instructions to monitor a plant parameter or to adjust plant settings [2]. Because components of NPPs are often interrelated, the abnormality of one plant parameter is often reflected by the abnormality of other related component. When faced with symptoms of abnormality, reactor operators are often required to institute several emergency procedures concurrently. If multiple emergency procedures as activated, the reactor operator must coordinate the execution of steps from each procedure. Often the operator interrupt the performance of a unified sequence of steps to perform a related but subordinate set of actions [2] [5]. It is not surprising that, under these conditions, operators sometimes become confused, or lose track of their place in the procedures. This confusion, in turn, may lead to operator errors [3].

COPMA-II.

Computerized procedures have been suggested as a means of assisting reactor operators in complex or confusing plant conditions. For example, computerized procedure systems can be programmed to monitor plant parameters, signal operators when specified plant conditions are met, track and illustrate operators' progress through multiple procedures, and to mark the particular point in a latent procedure to which operators should return when a branching procedural step has been completed [2] [3].

Since 1985, researchers at the OECD Halden Reactor Project in Halden, Norway have been working to construct a computerized procedures manual. The first prototype of this tool, the Computerized Procedure Manual (COPMA), was evaluated in the Halden Reactor Project's advanced experimental control room facility, HAMMLAB. The results of this evaluation were used to create an improved version of the COPMA system, COPMA-II. COPMA-II represents a substantial improvement in the acceptability and usability of the original COPMA system. A mouse device can be used to enter most command to COPMA-II [4], COPMA-II can be run

on the majority of Unix workstations are equipped with an X Windows operating system, 128 MB RAM, and a 19" color monitor [3]. COPMA-II incorporates two main systems, a procedure editor and an online system. The procedure editor (PED-II) divides each procedure into a list of procedure steps, and converts the procedures to the PROLA computer language. The procedures are then entered into the data base of the on-line COPMA-II system. The on-line system is the component of COPMA-II that is used by reactor operators to select and execute procedures in the control room.

As can be seen in Figure 1, the interface of the COPMA-II on-line system contains five window panes [3] [4]. The Bookshelf Pane provides a list of all procedures that are included in the COPMA-II data base. The Desk Pane provides a list of the procedures and related activities that are currently activated. The Main Menu Pane is positioned above the Bookshelf at the top left of the interface, and includes several selection buttons. To activate a procedure, the operator clicks the mouse on the "OPEN" Button. The "MONITOR" Button is used to identify system parameters that are to be automatically monitored by COPMA-II. Selecting the "VALUES" Button allows operators to monitor a readout of all parameters that are currently being monitored automatically.

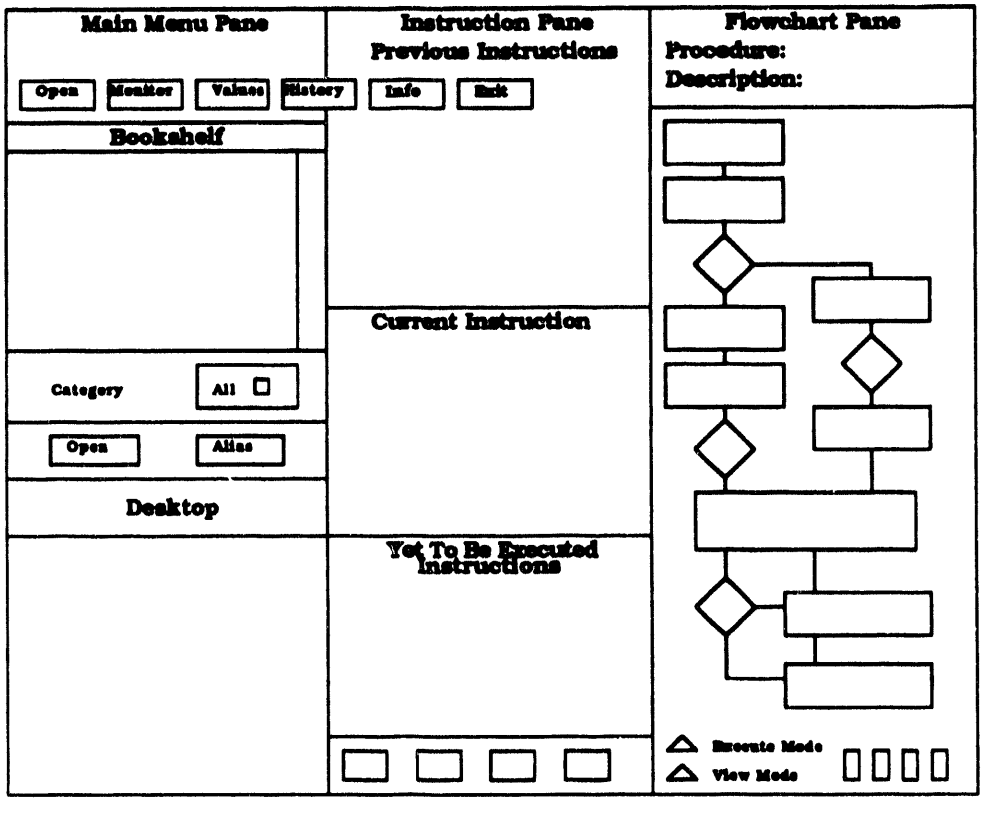


Figure 1. COPMA-II On-Line System Interface

The Instruction Pane is located in the middle of the COPMA-II interface. It contains three horizontal windows that display the name, description, and category of each active procedure in a scrollable text window. Procedures are coded in terms of their state of execution by screen position and by color. Previously executed, current, and yet to be executed instructions are displayed from top to bottom of the Instruction Pane, respectively. Current instructions are colored yellow, previously executed instructions are red, and yet to be executed instructions are blue. Four selection Buttons are located at the bottom of the Instruction Pane. The "Execute" Button activates the procedure in the current instruction window. The " Skip" Button allows COPMA-II to omit the current procedure. The "Previous" Button restores the current status of a previously executed procedure. Finally, the "Comments" Button retrieves a pop-up window that contains a small text editor with which the operator can store comments about the current procedure.

The Flowchart Pane is located at the far right of the COPMA-II interface. It provides a graphical overview of selected procedures in flow-charts that are structured in a tree-like manner. Each procedure step is listed in a small box that is color coded in terms of whether the step represents a previous, current, or yet to be executed instruction. The boxes are connected with vertical lines that illustrate the sequential relationships between procedure steps [4].

EVALUATION OF COPMA-II

A study was conducted to compare the effect of paper procedures and COPMA-II on the accuracy and speed of power plant operation. Sixteen licensed reactor operators controlled the Scaled Pressurized Water Reactor Facility (SPWRF) at North Carolina State University under normal operating conditions and during two accident scenarios. The SPWRF provided an excellent environment in which to evaluate COPMA-II because the facility preserves much of the complexity of operational control rooms, but provides a safe environment for testing systems under abnormal conditions. The SPWRF is a 1/9-scale working model of the Prairie Island Nuclear Generating Plant, which is a two-loop Westinghouse pressurized water reactor (PWR). Both primary and secondary sides are represented. The secondary side of the SPWRF contains almost every major system and component of a commercial PWR, including condensers, condensate and feed pumps, feed water heaters, auxiliary feed water pump, and turbine throttle valves [1]. The SPWRF continuously displays settings for all major operating parameters on the control console, and the control computer displays a representation of system conditions in a variety of easily understood graphic formats.

The 16 reactor operators who served as volunteers in the study were grouped into eight teams of two operators each. Each team included one Senior Reactor Operator (SRO) who located and read procedures, and one reactor operator (RO) who performed procedure steps and monitored plant variables as instructed by the SRO.

Team members were first trained to operate the SPWRF with traditional paper operating procedures. Once they demonstrated proficiency at this task, they were trained to operate the SPWRF with the COPMA-II system. Each team then performed a routine change of power task with both paper and COPMA-II procedures. Next, the teams performed one of two accident scenarios (small break loss of cooling accident or steam generator tube rupture) with traditional procedures, and the remaining scenario with the COPMA-II system. The order in which teams performed with each procedure type, and in which teams performed the two accident scenarios, was completely counterbalanced.

Error rates, time to initiate a procedure, and time to complete the procedure were recorded for each performance trial. Each operator completed the NASA-TLX Subjective Workload Estimation Scale following the performance of each task scenario. The NASA-TLX Scale requires operators to respond to questions about six components of workload: (1) Mental Demand; (2) Physical Demand; (3) Temporal Demand; (4) Performance; (5) Effort; and (6) Frustration. Operators were also encouraged to record free-form comments or suggestions on the back of the NASA-TLX questionnaire.

RESULTS AND DISCUSSION

Performance data and subjective workload estimates were grouped according to each combination of team number (1-8), procedure type (paper vs. COPMA-II) and scenario type (normal vs. loss of cooling accident vs. steam tube rupture). The time to initiate response, time to complete response, and the subjective workload estimates were subjected to separate analyses of variance (ANOVAs). For the error and response time data, team number, procedure type, and scenario type served as the independent measures. For analysis of the subjective workload estimates, operator type (SRO vs. RO), team number, procedure type, and scenario type served as the independent measures.

Change of Power Task Data

Because the change of power task simulated performance under normal operating conditions, we did not expect to find a difference, in terms of performance time or errors, or in terms of subjective estimates of workload, between performance with COPMA-II and with paper procedures. This hypotheses was confirmed by the performance data. There were no significant main or interactive effects on response initiation time, response completion time, or accuracy for the change of power task.

The subjective ratings of mental workload were less supportive of our hypotheses. The procedure type variable moderated operators' subjective ratings of their own performance, with higher ratings obtained under COPMA-II (m = 7.48 sec.) than under paper procedure conditions (m = 5.64 sec.). This finding suggests that the operators were more confident of their performance with COPMA-II than with paper procedures. Several operators commented that the COPMA-II system structured their responses more rigidly than did the paper procedures, and that,

due to this fact, they believed they were least likely to miss a required action, or to perform procedural steps in the incorrect order, with the COPMA-II procedures.

While operators were most confident of their performance of the change of power task when they performed with COPMA-II, they did not rate the mental workload of COPMA-II lower than they rated the mental workload of paper procedures. Taken in combination, these findings suggest that, while the operators believed that frustration and mental demand were highest for COPMA-II, they did not believe that this workload discrepancy would degrade their performance of the change of power task when they used the COPMA-II procedures.

Accident Scenario Data

We expected procedure type to moderate response time, accuracy, and subjective ratings of mental workload in the accident scenario data because of the relative difficulty of the performing these tasks. While there was no effect of procedure type on response completion time, our hypothesis was supported by a significant effect of procedure type on response initiation time. Response initiation time was faster for paper (m = 208.50 sec.) than for COPMA-II procedures (m = 297.37 sec.). Procedure type did not moderate response completion time. Thus, the accident scenario data suggest that operators were able to implement paper procedures faster than they could implement COPMA-II procedures. However, once the response pattern had been initiated, there was no difference in performance time for the two types of procedures.

For accuracy of response, there was an interaction between procedure type and task type. However, the direction of the effect of procedure time on accident scenario accuracy was the opposite of that found for response initiation time. The number of errors was greater for paper (m = 18.75) than for COPMA-II procedures (m = 4.00) for the loss of cooling accident only. For the steam generator tube rupture, the number of errors was not substantially different for paper (m = 13.00) and for COPMA-II procedures (m = 12.75).

The accuracy advantage for the COPMA-II procedures in the loss of cooling accident may have been due to the fact that the COPMA-II system constrained the operators' response patterns more effectively than the paper procedures did. Several operators commented that the COPMA-II system made it impossible for them to "skip ahead" and preview future procedure steps, as they could do with paper procedures. The COPMA-II system does include features that allow operators to skim future procedures. However, we did not teach the operators to perform this maneuver with the COPMA-II system. On the other hand, the paper procedures were very similar to the procedures the operators used in their home plant, and they became comfortable with the paper procedures almost immediately. Thus, they were able to manipulate the paper procedures with ease soon after the SPWRF training had begun. While operators were restrained from previewing future procedures when they employed the COPMA-II system, they seemed to move about in the paper procedures quite easily. If a more methodical

method of progressing through procedures reduced the likelihood that operators would skip a procedure or commit some other type of error, performance would be more accurate for the COPMA-II than for the paper procedures, as was the case in this study.

There were no significant main or interactive effects of procedure type, scenario type, or operator type for the subjective ratings recorded after performance of each accident scenario.

References

[1] P.C. Goodman, & C.A. DiPalo, "Human factors information system: A tool to assess error related to human performance in U.S. nuclear power plants." Proceedings of the Human Factors Society 35th Annual Meeting. October, 1991, 662-665.

[2] M. Krogsaeter, J.S. Larsen, S.R. Nilsen, & F. Owre, The Computerized Procedure System COPMA - System description and user interface (OECD Halden Reactor Project HPR-337), 1989.

[3] W.R. Nelson, N.T. Fordestrommen, C.B.O. Holmstrom, M. Krogsaeter, T. Karstad, & O. Tunold, "Experimental evaluation of the computerized procedure system COPMA (OECD Halden Reactor Project HWR-277), 1990.

[4] K.W. Olsen & J. Teigen, The COPMA Procedure Editor, PED-II (OECD Halden Reactor Project HWR-284), 1991.

[5] C.A. Tolbert, C.J. Moore, & D.R. Wieringa, "Emerging issues for procedures in the nuclear industry." Proceedings of the Human Factors Society 35th Annual Meeting. October, 1991, 1238-1242.

[6] J.A. Wachtel, & R.P. Correia, "Designing for the future of nuclear power plants: International perspectives on advanced control room design and philosophy." Proceedings of the Human Factors Society 35th Annual Meeting. October, 1991, 627-628.

Validation of the Use of Network Modeling of Nuclear Operator Performance

Michael Lawless and Ron Laughery
Micro Analysis and Design, Inc.
Boulder, Colorado

Dr. J. Persensky
U.S. Nuclear Regulatory Commission

ABSTRACT

Research and evaluation on human factors issues can be very expensive owing to 1) the high cost of running experiments and 2) high inter-team variability which makes it necessary to run large numbers of subjects to get stable estimates of performance. Increasingly, the engineering disciplines are looking towards computer modeling as a means of predicting performance as a function of engineering design. Human factors engineering has that goal as well. This paper presents the results of a validation study that evaluated a human performance modeling technology termed *task network modeling*. Task network models were built of a crew executing two emergency procedures and one normal procedure. For each of these three procedures, one model was built reflecting the use of paper procedures and one reflecting the use of computerized procedures. Model predictions were then compared to data on actual crews performing under identical conditions. In general, the model predictions were representative of actual performance, although a number of issues arose that should be addressed prior to using these models as a technical basis for regulatory action.

1. INTRODUCTION

The Nuclear Regulatory Commission (NRC) is responsible for evaluating the safety impact of proposed plant and procedure design modifications. Whenever the control room changes (e.g., panel or system modifications) or the plant procedures change significantly, it is the NRC's responsibility to ensure that these changes do not compromise safety. Therefore, there is a need to predict how proposed changes will impact operator performance and, ultimately, plant safety. When the need for such evaluation arises, the first approach is typically to review the literature and other available sources to determine whether there is an existing knowledge base that can be tapped, such as the knowledge of fundamental aspects of human performance or experience from other plants or similar industries. However, more often than not, the existing knowledge base is deficient with respect to it's applicability to a nuclear power plant environment. This leads to the need to study the phenomena of interest in a way that directly relates to the nuclear environment.

The obvious choice is human subjects experimentation in a realistic environment. However, experimentation with nuclear power plant operators requires extensive resources and can be difficult to conduct. There is a limited number of operators whose time is in great demand and a limited number of simulators or plants in which experimentation can be conducted. Furthermore, even with unlimited resources, the time required to perform experimentation in simulators may exceed the time available to make the decision. Yet, The question is, if we can't study real operators, what are the alternatives?

One alternative is computer modeling of the human-plant system. In the past decade, a variety of tools and techniques for modeling human-based systems have emerged and have been found to be increasingly useful for studying human operator behavior in closed-loop systems. One technology that has proven particularly useful for predicting human-system performance is *task network modeling.* In a task network model, human performance of an individual performing a function (e.g., implementing an EOP) is decomposed into a series of subfunctions which are then subsequently decomposed into tasks. This is, in human engineering terms, the task analysis. The sequence of tasks is defined by constructing a *task network.* This concept is illustrated in Figure 1 which presents a series of tasks for dialing a telephone.

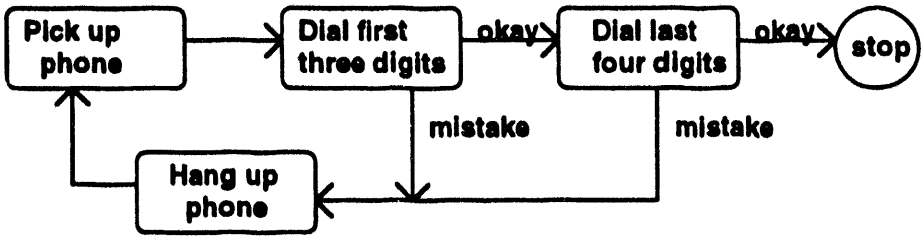


Figure 1. Example of a Task Network for Dialing a Phone

Task network modeling is an appealing approach to modeling human performance in complex systems for several reasons. First, it is ideally suited for extending task analysis. Task analyses organized by task sequence are the basis for the task network model. Second, through the use of existing modeling tools, it can be extremely powerful. In addition to extremely complex operator models, task network models can include sophisticated submodels of the plant hardware and software to create a closed-loop representation of the nuclear power plant control room environment. Third, task network modeling is relatively easy to use and understand. Recent advancements in task network modeling technology, including the development of the modeling system, *Micro Saint,* have made this technology more accessible to human factors engineers. Finally, task network modeling can be used to answer the following question:

> *"What are the expected changes in operator and plant performance based upon plant procedure and/or control room changes?"*

For the purposes of the Nuclear Regulatory Commission, this is the value of this technology.

An Example of a Task Network Model of the Nuclear Operator. This example illustrates many of the basic concepts of how task network modeling can be applied to studying human performance in a nuclear environment.

The example is of an operator responding to an annunciator using a procedure requiring comparison between two meter readings. Based on these readings, the operator must either open or

close a valve until the two meter values are nearly the same. The operator activities for this model are represented by the task network in Figure 2. Also, to allow the study of the effects of different plant dynamics (e.g., control lags), a simple one node model of the line in which the valve is being opened is included in Figure 3.

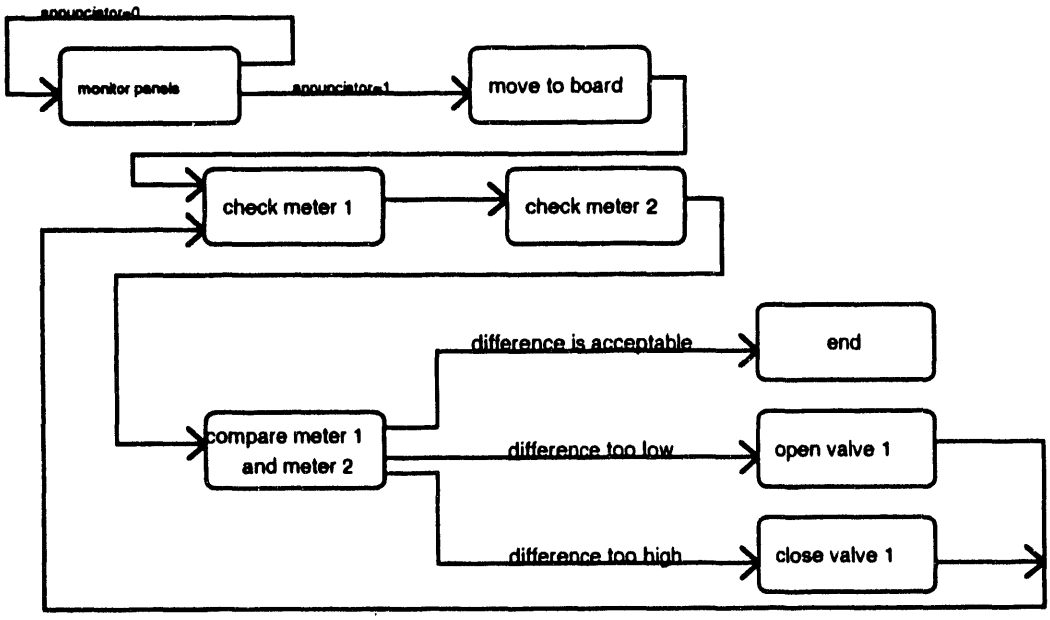


Figure 2. Sample Task Network Model of a Nuclear Power Plant Operator Responding to an Annunciator

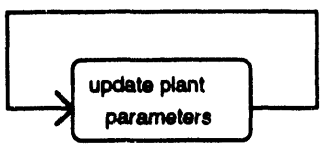


Figure 3. One node Model of the Plant

The operator portion of the model will run the "monitor meters" task until the values of the variables "meter1" and "meter2" are different. The simulation could start out with these values being equal and then precipitate a change in values with what is known in Micro Saint as a scenario event. This event (representing some change in the plant such as a line break or stuck valve) could be as simple as:

meter1 = meter1 + 2.0;

or as complex as an expression defining the change in the meter as a function of line break size, flow rates, etc. An issue which consistently arises in model construction is how complex the model should be. If the problem under study is purely operator performance, simple models usually suffice. However, if overall plant behavior is of interest, then the models of plant dynamics, such as meter values, are more important.

When the transient occurs and the values of "meter1" and "meter2" start to diverge, the annunciator signal will go on. This annunciator would be triggered in the plant portion of the model by a task ending effect such as:

if meter1 <> meter2 then annunciator = 1;

In this simple model, the values of "meter1" and "meter2" are treated as being identical to the plant processes they are reflecting. However, a more sophisticated model may distinguish between the plant parameter values and those reflected on the operator displays. This would allow the study of display error and lag times.

Once the plant model sets the value of the variable "annunciator" to 1, the operator will begin his activities by moving to the appropriate board. Then, he will continue through a loop where he checks the values for "meter1" and "meter2" and either opens "valve1," closes "valve1," or makes no change. The determination of whether to make a control input is determined by the difference in values between the two meters. If the value is less than the acceptable threshold, then the operator would open the valve further. If the value is greater than the threshold, then the operator would close the valve. This opening and closing of the valve would be represented by changes in the value of the variable "valve1" as a task ending effect of the tasks "open valve1" and "close valve1." In this simple model, operators do not consider rates of change in values for "meter1" and, therefore, would get into an operator induced oscillation if there was any response lag. A more sophisticated operator model could use rates of change in the value for "meter1" in deciding whether to open or close valves.

Again, this is a very small model reflecting simple operator activity on one control via a review of two displays. However, it illustrates how large models of operator teams looking at numerous controls and manipulating many displays could be built via the same building blocks used in this model. The central concepts of a task network and shared variable reflecting system dynamics remains the same.

Given a task network model of a nuclear operator in a "current" control room, how might the model be modified to address relevant research or regulatory issues? Some examples are:

1. Modifying task times based on changes in the time required to access a new display

2. Modifying task times and accuracies based upon changes in the content and format of displays

3. Changing task sequence, eliminating tasks, and/or adding tasks based upon changes in plant procedures

4. Changing allocation of tasks and ensuing task sequence based upon reallocation of tasks among operators

Changing task time and accuracies based upon stressors such as sleep loss or drug effects

The above list is not a definitive list of all the ways that these models may be used to study design or

operations concepts, but it should serve to illustrate the points. The question is, do these models provide valid predictions. The research discussed below focuses on that specific issue.

2. EXPERIMENTAL METHOD

To determine the utility of task network modeling in addressing this question, a study was performed to evaluate the following three issues:

1. Can valid task network models of existing systems be created from a task analysis data base?

2. Once created, can a task network model be modified to reflect control room redesign or procedure changes?

3. Do these modified task network models provide valid predictions of human performance times and error rates?

Our method of evaluating these issues was to "shadow" an empirical study that was itself investigating human performance issues in a nuclear power plant control room environment. Work ongoing at the North Carolina State University (NCSU) was selected as the study to shadow. That study was intended to evaluate a procedural aid called COPMA-II (Computerized Procedures Manual). The study was performed in the Scaled Pressurized Water Reactor Facility (SPWRF) at NCSU. The SPWRF performs and reacts to controls in a way that is very similar to a true pressurized water reactor. The procedures, from "Start-Up" to "Shut Down", are very similar to procedures that are used by operators every day in pressurized water reactors (see Scaled PWR Facility: Operations manual, 1993).

The NCSU experiment was a direct comparison between paper procedures and COPMA-II procedures in the Scaled Pressurized Water Reactor Facility (SPWRF) at NCSU. The primary goal of the NCSU experimentation was to test the hypothesis that COPMA-II would allow operators to perform accident scenario procedures more rapidly, more accurately and with fewer control responses than with paper procedures. Sixteen licensed nuclear power plant operators were paid to participate in this study. Dependent measures included accuracy (as measured by response deviations), number of responses required, and time to initiate and complete response. The scenarios performed by subjects in the NCSU study were 1) Loss of Coolant Accident (LOCA), 2) Steam Generator Tube Rupture (SGTR) and 3) a Load Maneuvers procedure. These procedures were divided into two parts for the purpose of assessing the chosen dependent measures referred to as *the preliminary procedure set* or *the final procedure set* for each condition. The preliminary procedure set starts with the initialization of the procedure (i.e. start load maneuvers, initiate the LOCA, initiate SGTR) and ends at a point where procedures change abruptly. The final procedure set starts with the new change in procedural instructions and ends when status is brought back to normal operating conditions. Table 1 summarizes the experimental conditions.

Table 1. SPWRF Procedures and Associated Conditions

SPWRF Procedures	Condition
Load Maneuvers	Paper Procedures COPMA-II Procedures
Small Break Loss of Coolant Accident(LOCA)	Paper Procedures COPMA-II Procedures
Steam Generator Tube Rupture(SGTR)	Paper Procedures COPMA-II Procedures

Model Development and Data Collection. The procedures that already existed for the SPWRF were ideal for modeling purposes. These procedures clearly show the flow of tasks for every SPWRF procedure and were used to construct task networks. Performance data (e.g., task times) were derived from the NCSU Paper procedures data. The use of the paper procedures reflected the same approach that would be used to model a "baseline" state (e.g., before the modifications that the model was being built to evaluate).

COPMA-II performance data estimates were generated from observations of COPMA-II operations (e.g., no formal time data collection, just a demonstration of the procedures) as well as information from previous uses of COPMA-II. The modeler in this study made *subjective estimates of expected changes* in performance caused by COPMA-II as opposed to the Paper procedures for which hard data were used. In essence, the procedure that were followed to make COPMA-II time estimates was expert opinion supported by any available data - the same procedure followed in almost every model-based study.

Model Execution. Once completed, models of each experimental condition (i.e. 6 models) were executed with 5000 runs each. Performance time and variance of performance time data were collected from the model runs. There were other data collected with actual human crews in the NCSU study.

3. RESULTS

Table 2 presents the data used in the analysis. The focus was on comparing the model predictions of time to perform the procedures vs. the actual data obtained in the NCSU study. These data are presented graphically in Figures 4 through 7 to illustrate the differences between model predictions and empirical data. These graphs illustrate the plus and minus one standard deviation range from the mean data.

Table 2. Comparison of Model Runs and NCSU Study

Condition	COPMA-II	Paper	COPMA-II	Paper
	Preliminary Set	Preliminary Set	Final Set	Final Set
	Mean/Sd	Mean/Sd	Mean/Sd	Mean/Sd
Load-NCSU	58.62/29.79	33/12.95	361.25/174.3	314.25/195.9
Load-Model	44.52/17.35	36.61/13.91	320.2/207.8	317.29/204.8
LOCA-NCSU	575.5/80.6	377.75/55.2	1463/893	431.25/242.3
LOCA-Model	445.4/79.7	385/61.1	490.4/264.1	457.4/261.6
SGTR-NCSU	476.75/88.62	390.25/175.5	618.5/286.7	1050.8/656.6
SGTR-Model	427/246.8	401.6/249.8	1159.5/759	1091.1/754.6

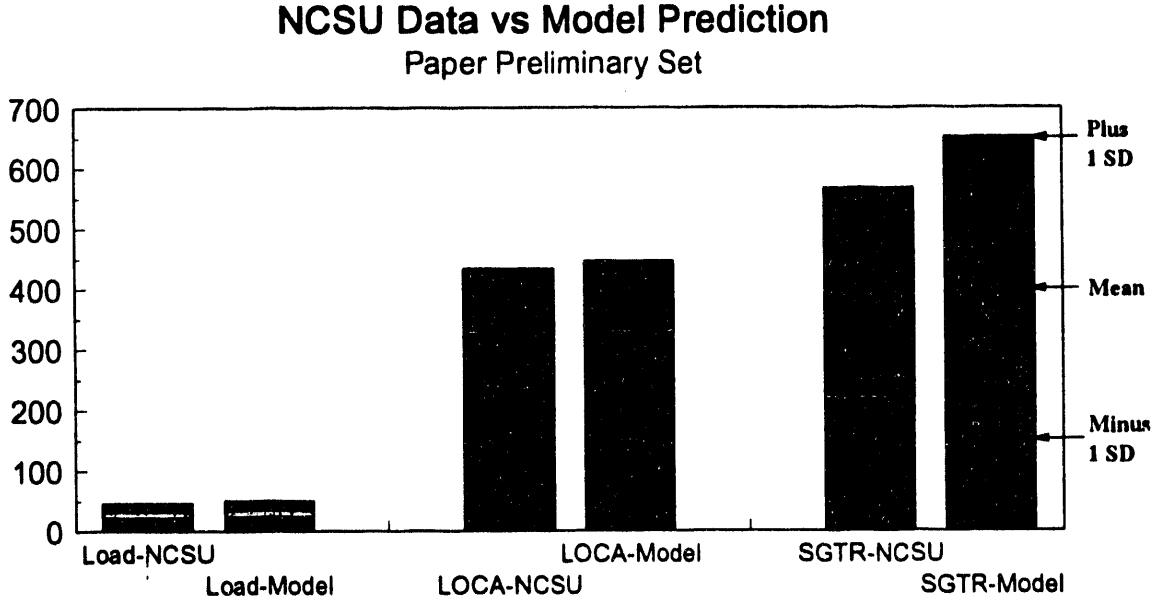


Figure 4. NCSU Data versus Model Prediction - Paper, Preliminary Set

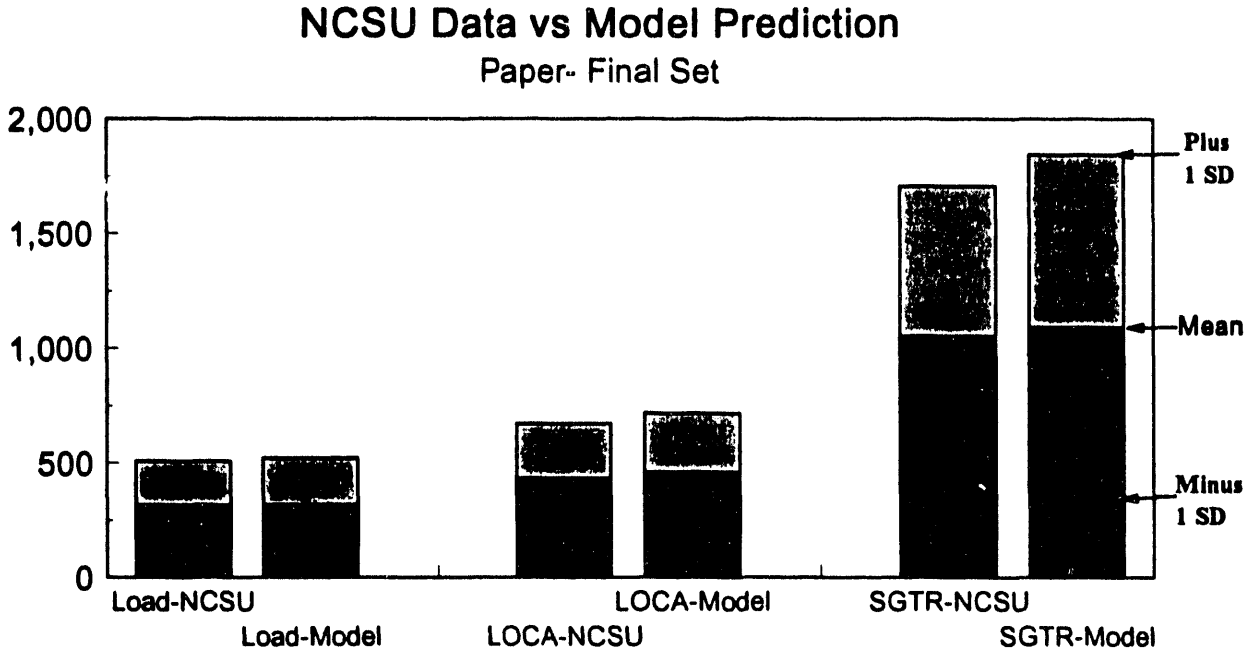


Figure 5. NCSU Data versus Model Prediction - Paper, Final Set

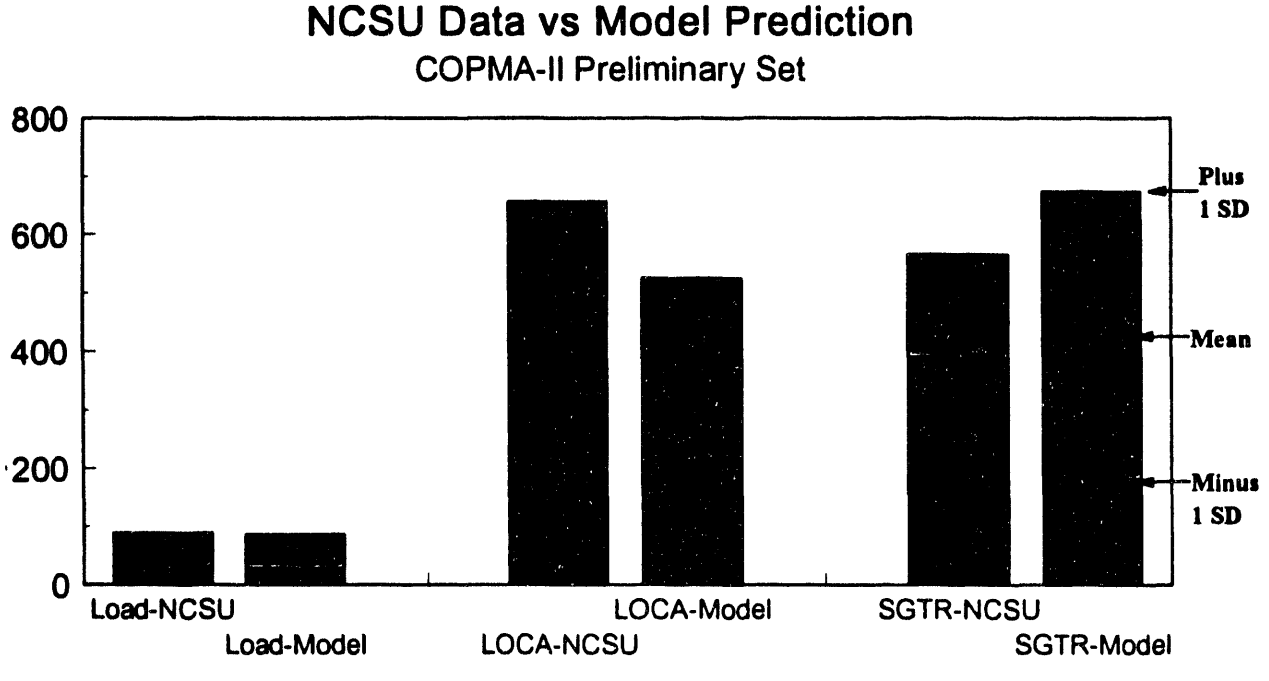


Figure 6. NCSU Data versus Model Prediction - COPMA-II, Preliminary Set

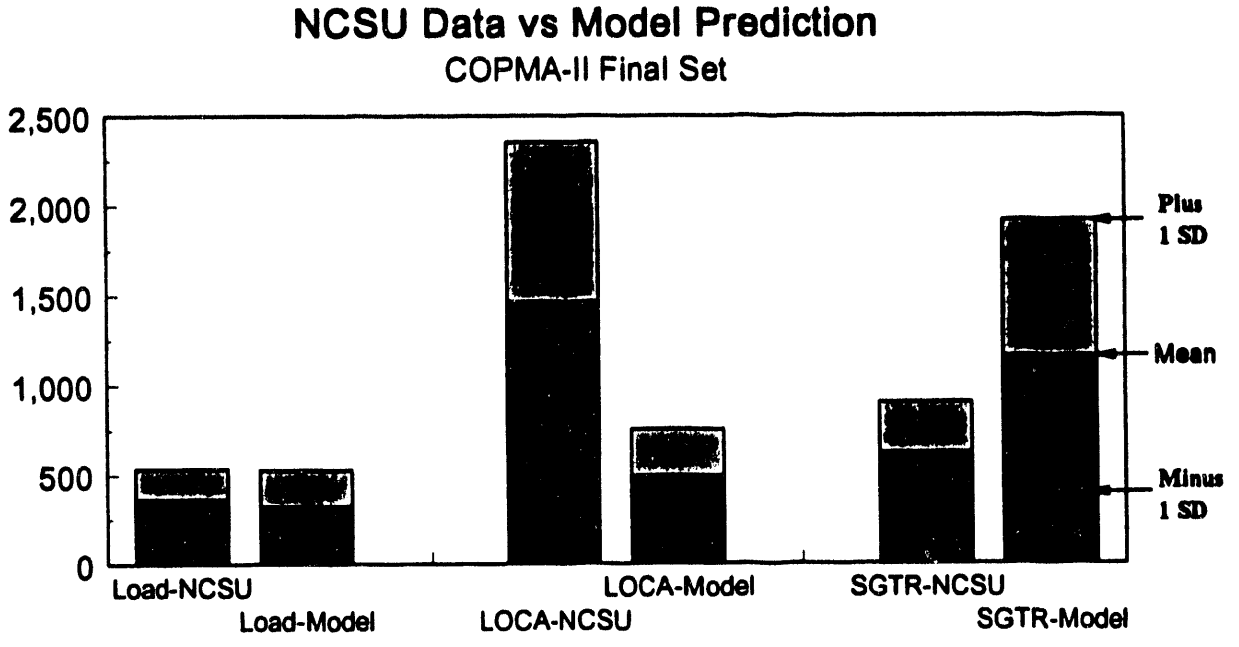


Figure 7. NCSU Data versus Model Prediction - COPMA-II, Final Set

A statistical comparison of the model predictions vs. the empirical data is presented in Table 3. We did not analyze the paper procedures data since the NCSU data from these were used in calibrating the models and, therefore, the match was, not surprisingly, nearly perfect. Two significant differences from predications of the models were found, both relating to the LOCA condition.

Table 3. COPMA-II from the NCSU Study versus COPMA-II from Model Runs
** indicates significant differences*

	COPMA-II N Preliminary Mean/Sd	COPMA-II M Preliminary Mean/Sd	COPMA-II N Final Set Mean/Sd	COPMA-II M Final Set Mean/Sd
Load	58.62/29.	44.52/17.	361.25/17	320.2/207
LOCA	** 575.5/80*	** 445.4/79*	** 1463/89*	** 490.4/26*
SGTR	476.75/88.	427/246.	618.5/286.	1159.5/75

4. DISCUSSION AND CONCLUSIONS

There were three questions of interest in this study feasibility, modifiability, and validity. These questions are stated below in more detail and findings summarized with respect to each.

***Feasibility* - Can valid task network models of existing systems be created from the existing task analysis data bases?**

Strengths of Task Network Modeling Approach

Models can easily be built from existing procedures - The process of defining the task networks for the procedures studied was very straightforward.

Time to build and modify the models for procedures is relatively short because of the detailed documentation of procedures - Modeling and simulation is only viable to the extent that the models can be developed in a reasonable period of time. The time required to collect all of these data and build it into a model was roughly one man-month.

Developing the model forced a level of analysis and rigor that experimentation did not require, but that was worthwhile - Whereas high level data could be collected and analyzed in the experiment at a relatively abstract and high-level (e.g., performance of large task groupings provided single points for data analysis), model development required a more detailed analysis of what was occurring during the procedures (e.g., at the task level) and, therefore, what might be affected by COPMA-II.

Weaknesses of the Task Network Modeling Approach

No significant weaknesses were identified in the ability to model crew procedural performance.

Outstanding Issues

Ability to model non-procedural tasks such as diagnosis, strategy development, and problem solving? While Micro Saint and task network modeling has the capacity for embedding models of higher level cognitive behavior into crew performance models, they are not inherently part of the technology. A complete model of nuclear crew performance may need to be able to simulate these higher-order aspects of human performance.

Question 2. *Modifiability* - Once created, can a task network model be modified to reflect control room redesign or procedure changes?

Strengths of Task Network Modeling Approach

Identification of changes required of the model were straightforward - Given a baseline model, it was easy to identify where and how the model needed to be changed to reflect the differences between paper procedures and COPMA-II.

Reasonable estimates of time differences for affected tasks were possible without empirical data - The approach used to generate new time estimates for tasks affected by COPMA-II was, in essence, expert opinion, which, in general, provided sound predictions of overall task improvements/decrements as a function of COPMA-II.

Weaknesses of the Task Network Modeling Approach

Making time estimates for the new models lacked the rigor and structure that would provide a more defensible model for decision making - While the use of expert opinion provided reasonably sound results, they would undoubtedly be more difficult to defend as part of any regulatory action than if a more scientific or technical basis were used for estimation or way of eliciting expert judgment.

Difficult to predict effects on performance may not be picked up with network modeling - In this study, the operator behaviors were fairly structured and, therefore, the reductionist task network modeling approach was sufficient. As the crew tasks become more emergent (i.e., crew strategies change in unpredictable ways as the event emerges), it will be more difficult to capture these emergent strategies in a task network model.

Outstanding Issues

What about non-procedural tasks? - The same issues that apply to the development of models for higher-order cognitive behavior apply to how would the models be modified to predict the system design or other changes to be studied with the model.

How can the process of revising performance parameter estimates be improved? -While new technologies are emerging and being incorporated into task network modeling tools, the question that still must be addressed is "What is a sufficient basis for estimation of task parameter changes?"

What will be the acceptance by NRC regulators and industry? - Practically, to use task network models to develop and evaluate technical bases for regulatory action by the NRC and industry, the approach must be accepted as valid by these communities. What will that require?

Question 3. ***Predictive Validity*** **- Do these modified task network models provide valid predictions of human performance times and error rates?**

Strengths of Task Network Modeling Approach

The task network models predicted the human performance data results reasonably well - The following points summarize the data with respect to predictive validity:

1. While there were some conditions where the model did not predict statistically significant differences, in five of the six cases the model predicted effects in the correct direction. In the sixth case, the model predicted a very small increase when there was, in fact, a decrease in performance time.

2. The model predicted significant effects of the experimental conditions in the same manner that the data showed significant differences in four out of six experimental conditions.

3. When directly compared, the COPMA-II model and experimental data were not statistically significantly different in five of the six conditions (including control conditions).

4. The correlations between the model data predictions and the actual data were statistically significant.

These results are encouraging, but not conclusive evidence of the strength of task network modeling in accurately predicting nuclear operator performance in all situations.

Weaknesses of the Task Network Modeling Approach

The predictive validity was too low to definitively prove the predictive validity of task network modeling - As stated above, the results were good, but not good enough to declare a clear success of the modeling approach.

Outstanding Issues

A more detailed analysis of the individual time data would be illuminating with respect to how individual task estimates compared to actual data - As discussed above, future validation studies should include data analysis at a higher resolution than permitted in this study. Only then can the real strengths and weaknesses of modeling vs. experimentation be properly assessed.

Summary

In summary, the following could be said about this study of task network modeling:

1. Models were straightforward to develop for nuclear power plant procedures.

2. Defining how the models had to be changed to reflect computerized procedures was also straightforward.

3. The method for estimating model parameter changes used in this study, educated guessing, could be improved on with new human performance modeling technologies.

4. The predictive validity of task network modeling as shown in this study is encouraging, but probably not sufficient for establishing it as a standard for forming technical bases for regulatory action.

All in all, the above results are encouraging. Given that this was intended to be an exploratory study to evaluate feasibility with an eye towards evaluating validity, the results indicate that further research on this technology is warranted.

A REVIEW OF POTENTIAL USES FOR FIBER OPTIC SENSORS IN NUCLEAR POWER PLANTS, WITH ATTENDANT BENEFITS IN PLANT SAFETY AND OPERATIONAL EFFICIENCY*

David E. Holcomb
Oak Ridge National Laboratory, P.O. Box 2008, Oak Ridge, Tennessee 37831-6010

Christina Antonescu
NRC Office of Nuclear Regulatory Research

ABSTRACT

Fiber optic-based sensing has a wide range of potential applications in nuclear power plants, and a fiber optic analog presently exists for virtually every conventional nuclear power plant sensing system. Fiber optic-based sensors are likely to eventually supplant many conventional sensors because of their inherent advantages—reduced mass, reduced size, ruggedness to vibration and shock, physical flexibility, high sensitivity, electrical isolation, extreme resistance to electromagnetic interference, high temperature resistance, reduced calibration requirements, passive operation, and high radiation resistance. In addition, fiber optic-based sensors exist which are capable of measuring parameters important to safety and performance which cannot be conventionally measured (high electromagnetic field, in-core, and distributed measurements). However, fiber optic sensors remain at too low a level of development for immediate application in safety-critical systems. Moreover, fiber optic sensors have different failure modes and mechanisms than conventional sensors; hence, considerable regulatory research will be necessary to establish the technical basis for the use of fiber optic sensors in safety-critical systems.

1. INTRODUCTION

Fiber optics is an emerging technology with many inherent advantages in sensing and communication applications as compared to conventional technology. Some of the potential advantages of optical fiber technology are greatly increased communications bandwidth, reduced mass, reduced size, tolerance of vibration and shock, physical flexibility, high sensitivity, electrical

*Research sponsored by the Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, under Interagency Agreement 1886-W179-8L and performed at Oak Ridge National Laboratory, managed by Martin Marietta Energy Systems, Inc., for the U.S. Department of Energy under contract DE-AC05-84OR21400.

isolation, extreme resistance to electromagnetic interference (EMI), resistance to high temperatures, reduced calibration requirements, passive operation, and resistance to radiation.

Fiber optic communication is a mature technology with optical fibers rapidly replacing copper wire for the vast majority of communication lines. Prices for optical fibers and laser diodes have dropped roughly three orders of magnitude over the past decade, with an equally great increase in product reliability and performance.

Since fiber optic sensors rely upon developed fiber optic communication components, they have been introduced only as the fiber optic communication industry has matured. A fiber optic analog currently exists for virtually every conventional sensing system in a nuclear power plant. Moreover, a variety of optically based sensors now exists for performing measurements that cannot currently be made (e.g., in-core temperature measurements, distributed measurements, and high EM field measurements). These advanced fiber optic sensors range in state of development from conceptualization to small-scale commercialization, with none yet having been ruggedized sufficiently for use in safety-critical systems.

With some notable differences, the optical fibers used in nuclear power plant containments are similar to standard communication-type fibers. Since the critical components of nuclear power plants tend to be submerged in high-pressure, hot water and since significant portions of nuclear power plants are exposed to radiation, the fiber optics used within the containment of nuclear plants must be radiation hardened, hermetically coated, and resistant to high temperatures. Pure silica core optical fibers (particularly within the 1300- and 1550-nm communications bands) are highly radiation resistant, often not showing measurable damage for doses of several thousand Gray.[1] Hermetic carbon coatings (which prevent the ingress of water) are available for optical fibers from several fiber manufacturers. Conventional (for communication-type fibers) polyimide coatings survive temperatures of more than 300°C, and for higher temperatures metallic coatings are available, some of which can survive up to 900°C. Because of the small size and durability of optical fibers, fiber optic penetrations into containment and across pressure boundaries should be no more difficult than conventional penetrations. In fact, conventional gland seals with only minor modifications are likely to be suitable for permitting optical fiber access into piping. Fiber optic bundles require an additional barrier (as compared to single fibers) for passing through a penetration. To prevent leakage within the bundle (along the fibers), the fibers must be appropriately cemented together.

This paper was prepared at the request of the NRC Office of Nuclear Regulatory Research. It presents the current status of fiber optic sensing and communication as it relates to nuclear power plants, including the potential safety and operational efficiency improvements. The review is presented from a standpoint of parameter measurement. The available optical techniques for measuring each process parameter are presented, and the most promising techniques are analyzed to give the potential benefits, limitations, and the current state of sensor development.

2. FIBER OPTIC THERMOMETRY

Temperature is a key process parameter throughout nuclear power plants. Hence conventional temperature sensors have been extensively studied and, in general, perform quite well. However, conventional temperature sensors suffer from a variety of limitations such as a need for periodic recalibration, EMI and radiation sensitivity, single-point measurement, slow response time, and need for isolation from the process fluid. Fiber optic temperature sensors have the potential for overcoming all of these limitations.

A fiber optic temperature sensor exists in some state of development based upon virtually every known thermo-optical property. Temperature-dependent optical properties that have been seriously considered to date include change in fluorescent properties, change in optical absorption, change in

optical reflection, change in optical scattering, change in optical path length (resulting in change in optical interference), change in birefringence, change in thermally generated radiation (blackbody radiation), and change in fiber light loss due to thermally induced microbending.

2.1 Photoluminescence Decay

For nuclear power plant temperature ranges, the dominant optical temperature measurement technique is photoluminescent decay time measurement. The basic measurement technique involves optically exciting a phosphor located at the tip of an optical fiber and monitoring the emitted fluorescence transmitted back down the same optical fiber. Since the lifetime of an excited atomic state is a function of temperature, the rate of decay of the fluorescence provides an indication of the phosphor temperature. The major advantage of this technique is the simplicity of the components and processes involved. It is of note that since excited state lifetime is a fundamental atomic property, sensors based on fluorescence decay time may not require periodic recalibration (degradation will manifest itself as a reduction in overall signal strength rather than as a change in time signature). Note that this is true only if the fluorescence results from atomic transitions involving nonbonding electrons—for which chemical stability is not a concern; thus careful phosphor selection is required.

A limitation of this technique is the low amount of light being produced by the phosphor, resulting in a low signal-to-noise ratio. Fluorescence decay time sensors are commercially available from several manufacturers, although none has yet been demonstrated in a high radiation environment. Among these are Luxtron Corporation and Rosemount, Inc. With proper component specification, it should be possible to perform temperature measurements throughout (including in-core) nuclear power plants with this technique.

2.2 Radiation Pyrometry

For higher temperatures, fiber optic radiation pyrometers have been developed. In these sensors, a blackbody cavity is attached to the tip of a sapphire fiber that transmits the light back to a conventional communications-grade fiber and then to a photodetector. Major limitations of this technique for nuclear plants include its limitation to extremely high temperatures (500+°C) and its requirement for nonvarying surface emmissivity of the measured object.

Noncontact versions of radiation pyrometry are also possible. In this system an object's infrared emissions are coupled into an optical fiber and transmitted back to a detector. For temperatures above a few hundred degrees Centigrade, the optical fiber is located remotely from the process and the infrared emissions are focused on the fiber bundle. This necessitates a direct optical path into the high-temperature environment. Systems have been developed based on this technique for measurements ranging from 40 to 2800°C.[2] Multiple wavelength ratiometric techniques have been applied to reduce the effects of a nonvarying surface emmissivity.

2.3 Fabry-Perot Interferometry

A wide variety of Fabry-Perot etalon-based temperature sensors has been developed.[3] Fabry-Perot etalons are composed of two reflectors on either side of an optically transparent medium. The theory of Fabry-Perot devices has been extensively reviewed by Born and Wolf.[4] The transmittance and reflectance of these devices is strongly dependent on the spacing of the reflectors and the wavelength of the incident light. Thus, thermal expansion (the "expansion" is typically dominated by an optical expansion due to change in refractive index as opposed to a change in physical size) of the material between the reflectors yields an optical signal that is a function of temperature. MetriCor, Inc., has produced a commercial temperature sensor based on a thin film of

single-crystal silicon hermetically sealed between two transparent substrates. To avoid signal variation due to nonthermal effects (optical fiber darkening, connection variation, etc.), multiple wavelength ratiometric techniques are incorporated into the signal detection and processing. The major limitation of this technique for nuclear plants is that current implementations are based on the optical properties of thin films, which may prove to be quite radiation sensitive.

2.4 Distributed Temperature Sensing

Each of the previously described temperature sensing techniques yields the process temperature at a single spatial location. It is also possible to measure the temperature continuously along the length of an optical fiber.

The most common form of distributed fiber optic temperature measurement relies on the temperature-dependent change in the relative amounts of Stokes and anti-Stokes scattering from an incident light pulse. Stokes (and anti-Stokes) scattering is a form of Raman scattering in which the incident photon interacts with a phonon of the material lattice in which the photon is propagating. (Phonons are the localized wave packets representing lattice vibration much as photons are the localized wave packets representing electromagnetic propagation.) Raman scattering has been reviewed by Kittel.[5] In Stokes scattering the propagating photon interacts with the material lattice, emitting a phonon and downshifting in energy. In anti-Stokes scattering the photon absorbs a phonon and is upshifted in energy. The number of phonons in the material and hence the ratio of Stokes to anti-Stokes scattering are a function of temperature. This form of sensing is implemented by injecting a narrow wavelength band optical pulse into a fiber at a known time and measuring the subsequent Stokes and anti-Stokes light scattered back down the fiber. Since both the time of injection of the optical pulse and the index of refraction of the optical fiber are known, the time at which the backscattered light arrives at the fiber end is a measure of the location of the scattering. Correspondingly, the intensity ratio of the Stokes to anti-Stokes components of the backscattering is a measure of the temperature.

The technique of obtaining spatial information about reflections from the time interval between pulse injection and reflection return is referred to as optical time domain reflectometry (OTDR). The major limitations of this technique for nuclear plants are that complicated, expensive electronics and optics are required (to pick out the relatively low-intensity Raman lines from all of the other scattering processes occurring in the fiber) and that the technology has yet to be demonstrated outside the laboratory.

Another form of OTDR-based distributed fiber optic temperature sensing has recently been demonstrated outside the laboratory. In this system a conventional fiber optic core is coated with a polymer cladding containing scattering centers. The polymer cladding has a temperature-dependent refractive index. Therefore, the optical power present in the cladding and hence the amount of backscattered light both vary with temperature. This sensor has been reported to be able to pick out hot spots of less than 10 cm length and to have an accuracy of ±2°C from 0 to 60°C and ±5°C from 60 to 150°C.[6] Limitations of this sensor for nuclear power applications are the complicated, expensive electronics that are required and the possible radiation sensitivity of the scattering cladding.

3. FIBER OPTIC PRESSURE MEASUREMENTS

Pressure is a fundamental process parameter that requires accurate and reliable measurement throughout nuclear power plants. Improved pressure measurement will result in enhanced plant safety and increased operational efficiency. Conventional pressure sensors have been studied extensively, yet significant areas remain for performance enhancement. Many conventional

pressure sensors use oil to buffer the gauge mechanism from the process fluids and are subject to insidious failures when the oil leaks. Also, conventional pressure sensor performance verification and calibration require significant periodic effort. In addition, conventional pressure sensor accuracy under accident conditions is as low as ±10%.[7] Moreover, conventional pressure sensors provide only single-point pressure measurement.

Fiber optic-based pressure sensors have the potential for overcoming all of these limitations. However, the potential benefits of fiber optic sensing do not accrue unconditionally merely by switching to fiber optic sensors. Poorly designed or inappropriately applied fiber optic sensors often are undesirably cross sensitive to other variables (notably temperature and vibration), require complex and expensive signal processing, and degrade rapidly under harsh plant conditions. The basic types of fiber optic pressure sensors being seriously considered for industrial applications are diaphragm deflection measurement (both intrinsic and extrinsic), Fabry-Perot interferometric measurement, Mach-Zehnder interferometric measurement, and piezoluminescence measurement.

3.1 Diaphragm Deflection

Diaphragm deflection measurement can take many forms. The fiber itself may be fabricated from a pressure deformable material (typically, silicone rubber). The sensor signal is then obtained as either the total optical attenuation due to the total pressure along the fiber or as a distributed pressure measurement using OTDR techniques. Deformable fibers, however, are not precision engineering components. They thus have several limitations, including static fatigue, cycling-induced response variation, and cross sensitivity to temperature. This type of sensing system is thus best suited for applications not requiring precise measurements (machinery interlocks, personnel and vehicle location, etc.).

The second type of diaphragm deflection sensor is the furthest developed for nuclear applications. Babcock & Wilcox has developed a high-temperature, fiber optic pressure transducer [8] based on using the pressure-induced deflection of a high-strength steel diaphragm to cause increased microbending loss in an optical fiber. A series of these diaphragms can be deployed along a single fiber and interrogated using OTDR techniques to obtain quasi-distributed pressure measurements. Major limitations of this sensor type are that (1) it is an intensity-based measurement and thus susceptible to connector variations, source power fluctuations, radiation darkening of the fiber, etc., and (2) the sensor will eventually fail because of the mechanical cycling of the fiber used to transduce the pressure.

The final diaphragm deflection measurement system is also the most basic. In this system a bifurcated fiber optic bundle is located such that its single end points at a high-strength, temperature-invariant diaphragm. Light is coupled into one of the forks of the bifurcated end of the fiber. The diaphragm deflection alters the amount of reflected light coupled back into the fiber bundle. The major limitations of this design are the hysteresis and cross temperature sensitivity of the diaphragm. Also, without multiple wavelength ratiometric techniques and temperature compensation, the sensor's accuracy will be limited.

3.2 Fabry-Perot Interferometry

Fabry-Perot pressure sensors consist of a Fabry-Perot etalon (of roughly the same cross section as its optical fiber lead) located at the distal end of a fiber optic cable.[9] The thin distal reflector of the etalon serves as a pressure-sensitive diaphragm, the deflection of which alters the interferometer tuning. The sensor is interrogated by an LED with a relatively narrow wavelength band. The pressure-induced interferometer tuning change alters the spectral distribution of the reflected light. The reflected light is filtered into two wavelength bands, with the intensity ratio of the two bands being proportional to the applied pressure. This approach is the basis of the MetriCor ColorOptic™

pressure sensor. One possible limitation of this sensor is that the sensitivity of its thin silicon diaphragm to radiation has not yet been determined. An advantage of this sensor type is that the diaphragm can be fabricated of a material (silica or sapphire, for example) that does not have a phase change within the operational temperature region, and thus the sensor may be made nearly insensitive to temperature.

3.3 Mach-Zehnder Interferometry

A fiber optic Mach-Zehnder interferometric pressure sensor consists of a long-coherence-length optical source invariantly coupled into the two interferometer legs (single-mode, polarization-maintaining optical fibers). Light emerging from the legs is recombined and coupled into a photodetector. Pressure transduction takes place by altering the optical path—via pressure—along one of the two legs (typically by coiling the fiber around a material having a large piezoelastic response). The output from the two legs then interferes, and the combined intensity is a measure of the pressure along the measurement leg. The main limitation of this system is its cross sensitivity, since minor temperature or vibrational differences between the two legs also alter the interference. Also, interference maxima counting logic is required to obtain an absolute pressure measurement, since several (often hundreds) of interferometric cycles occur between zero differential pressure and full scale. Unless the cross sensitivity issues can be solved, this pressure measurement technique is likely best suited for dynamic measurements such as hydrophonic sensors rather than for typical industrial quasi-static measurements.

3.4 Piezoluminescence

The final fiber optic pressure sensor type is the pressure analog of the photoluminescent decay time measurement system described previously for temperature measurement. The major limitation of this type of sensor is that currently available piezoluminescent materials exhibit pressure responses only in the gigaPascal pressure range. Piezoluminescent materials are the subject of active research that, if successful, would open up new markets for this type of sensor.

4. RADIATION MEASUREMENTS

Optical fibers are well suited to transmit scintillator light back from the harsh process environment to a control room environment, where sensitive detection electronics can survive. For example, a neutron-sensitive phosphor can be painted on the tip of an optical fiber. Because of the small scintillator size, such a sensor would have virtually no cross sensitivity to gammas. Since the scintillator is a solid, the neutron interaction cross section would be much higher than with a gas-filled ion chamber of equal size. The eventual limitations of this type of radiation detector would be in the radiation damage to the scintillator and in the radiation darkening of the optical fiber. If sufficiently radiation-hardened, long-wavelength (1.3–2-m) scintillators can be developed (to utilize the wavelength band in optical fibers where radiation darkening is very small), this type of detector could be deployed throughout a nuclear power plant (including in-core) for neutron monitoring. An interesting combined neutron flux and temperature sensor has been developed at Oak Ridge National Laboratory based on a combination of a neutron-sensitive phosphor and an activated thermophosphor.[10] In this sensor, incident neutrons are absorbed, thereby creating charged particles that produce scintillations in the thermophosphor. Neutron flux information is obtained from the number of pulses, and temperature is determined from the pulse decay time.

Gamma monitoring is also possible using small scintillators coupled to the tip of fiber optic bundles. The majority of the nonneutron radiation detector work with optical fibers is currently

being performed in the field of medical instrumentation. Optical fiber gamma and electron beam dosimeters suitable for use in radiation therapy environments have been demonstrated.[11]

Radiation measurements can also be made in a spatially distributed manner. One possible arrangement would be to segment an optical fiber by interleaving small scintillator pieces within an otherwise continuous fiber. The optical pulse intensity would indicate the radiation flux/energy, while the differential pulse time of arrival at either end of the fiber would yield the location of the radiation source. This type of quasi-distributed sensor shows promise for area radiation monitoring, replacing a series of point radiation detectors.

Since well-designed optical-fiber-based radiation sensors possess all the inherent advantages of passive optical sensing, they are likely to eventually supplant virtually all conventional harsh environment radiation detectors, as well as many multipoint radiation sensor systems.

5. FLUID LEVEL MEASUREMENTS

Fluid level measurement is required throughout a reactor's primary and secondary coolant systems, with several of the measurements being safety critical. The pressurizer, steam generator secondary side, reactor vessel, safety injection tanks, and containment sump all require safety-grade fluid level measurement. One method to determine fluid presence is to couple the output light from a fiber segment into a prism. Using the proper prism angle and material, the light is totally internally reflected when the prism is in air and lost into the liquid when the prism is submerged in water. This sensor thereby serves as a fluid switch with a very high signal-to-noise ratio. A vertical sequence of these sensors can be used to infer fluid level. Sensors of this type are available commercially from several manufacturers (EcTec and Tedco, for example).

Another possible fluid level measurement technique involves running a durable, large-core, unclad multimode optical fiber (likely a sapphire rod) along the height of the tank. Since air and water have different indices of refraction, different numbers of optical modes will be guided in such a fiber on either side of an air–water interface. The added loss point (interface) should be detectable using OTDR. Pointwise optical fluid level detection is an accepted technique that has been deployed industrially for more than a decade. Its primary limitations are fouling of the optical components, giving only pointwise spatial information, and in some implementations a need for multiple vessel penetrations. Continuous optical liquid level sensing has yet to appear in the technical literature. However, if the materials difficulties can be solved, it will be the technology of choice for precise measurement of fluid level.

6. POSITION MEASUREMENT

Optical fiber position measurement has made significant inroads into the aviation industry because of its simplicity, reliability, reduced mass, reduced size, physical flexibility, and potential for multiplexing. These same advantages pertain to nuclear power plants, and it is likely that most position measurements in them will eventually be made optically.

Nuclear power plants have a variety of mechanical components whose position must be known (e.g., control rods, valves, and circuit breakers) for safe operation of the plant. Several optical methods are possible for measuring each of these displacements. It may be possible to use the plate encoder technique developed for the aviation industry to track control rod motion. In this scheme, two fixed arrays of optical fibers are placed facing each other, and a plate with a coded pattern of holes is placed between them. The plate is attached to the linear travel component (in this case a control rod). As the plate moves, the coded pattern of holes uniquely yields the component's linear position. The major limitations of this type of system are the need for sufficient optical access and

clean fiber optic face plates. Another linear motion measurement technique requiring much less optical access is a variation of the diaphragm pressure sensor with the bifurcated fiber optic bundle. In this case the top of the control rod would be reflectively coated (polished), and a variable amount of light would enter the return fibers based on its distance from the top of the guide tube. The major limitations of this technique are its requirements for optical access, the difficulty of obtaining sufficient signal change throughout the range of travel of the rods, and the necessity of providing an invariant reflecting surface. The difficulties of these systems may, however, be outweighed by the obvious advantage of having a direct measurement of control rod position.

Much simpler optical position transducers are possible for determining valve position. The most fundamental technique would be a simple light and photocell arrangement located within the piping on opposite sides of the valve or a light/reflector arrangement across the valve. The main limitation of this technique is the requirement for optical access. Encoder plate techniques are also applicable to valve position indication.

7. FLOW MEASUREMENT

Fiber optic-based flow meters offer significant potential advantages over conventional instruments. If sufficiently rugged and reliable fiber optic flow meters become commercially available, they are likely to be the technology of choice for industrial flow measurement. Flow rate is a critical thermodynamic parameter for determining the plant thermal power level, and as such its measurement is key to efficient plant operation. Currently, flow measurements are typically made using the differential pressure across an orifice plate or venturi. Several of the optical pressure sensors discussed previously are applicable to the measurement of differential pressure. However, a potentially significant limitation of this type of sensor is orifice fouling.

Vortex shedding flow meters are another possible technique for measuring flow. In this scheme, two fibers (or one fiber and a reflector) are positioned facing each other with one fixed in position and the other subjected to the mechanical oscillations of the vortices shed by an obstacle upstream from it (either directly or by mechanical linkage to a lever in the flow path). A flow meter based on this technique is available commercially from Bailey Controls. The main limitations of this type of system are that (1) it only measures a section of the flow and is thus unsuitable for stratified flows, (2) it requires optical access to piping, and (3) the long-term reliability of mechanically moving optical fibers in hot liquid environments has not been demonstrated.

Laser Doppler velocimetry is another optical technique suitable for flow metering in fluids with scattering particles (e.g., steam droplets and possibly the entrained chemicals in the primary coolant loop). An interesting monobeam, fiber optic, distributed, laser Doppler velocimeter was recently described by Martinelli and Gusmeroli.[12] Their system is based on a Michelson interferometer that uses a low-coherence light source as its input and has one of its legs in the process fluid. Scattering from particles located within the coherence length of the optical source of the path differential between the two optical legs produces interference fringes. This technique yields a flow velocity profile across a pipe as the length of the external optical leg is changed.

8. STRAIN AND TEMPERATURE MEASUREMENT

Improved strain measurements on high-pressure components and welds in nuclear power plants would be of significant benefit, since strain increase provides an indication of incipient cracking and failure (thus giving an estimate of remaining component life). Conventional strain measurements are performed with electrical strain gauges that are difficult to install and have difficulties with linearity, longevity, and resistance to high temperatures. All of the fiber optic strain measurement techniques

developed thus far suffer from unwanted cross sensitivity to temperature. The approach taken to solve this problem has been to measure temperature simultaneously with strain and then compensate for its change.

Three different optical interferometric approaches to strain measurement appear to be particularly promising. The first of these is the Sagnac ring resonator in which coherent light is coupled via a 2 x 2 coupler into the two ends of a fiber optic ring. The frequency of the light traveling in one direction of the ring is shifted so that upon recombination at the coupler, a heterodyne beat pattern is produced. As the fiber loop is strained, different amounts of phase change are produced in the counter-propagating beams because of the frequency shift in one propagation direction. This produces a change in the beat pattern, which is monitored on the final arm of the 2 x 2 coupler.

A second interferometric technique involves laying a fiber containing short breaks along the piping. The fiber is pinned to the piping at each break point, and the short breaks serve as Fabry-Perot interferometers. The distance between the end planes of the resonant cavities varies as the pipe deforms, thus giving a measure of the strain occurring at each break. This arrangement gives a pointwise-distributed measure of strain when probed using OTDR techniques. Temperature compensation may be achieved in several ways, such as embedding thermophosphors along the sensor or simultaneously monitoring the Stokes/antiStokes scattering ratio within the sensor.

A final interferometric strain sensor is the Mach-Zehnder configuration. In this system, one of the two interferometer legs (which are composed of birefringent fiber) is embedded within the monitored structure. The interference between the light output from the two legs is monitored along both the fiber's slow and fast optical axes. The cross sensitivity between strain and the fiber thermal expansion (determined from finite-element modeling of the mechanical temperature response of the fiber and confirmed by experimental measurement) is expressed as a coupled set of equations relating the interference along the fiber's slow and fast optical axes to the change in temperature and strain.[13]

Optical fiber strain gauges show a great deal of promise for the future. However, all still require considerable development effort before being ready to install in safety-critical applications.

9. LEAK DETECTION

Leak detection in a nuclear power plant has as its goal the detection of small leaks before they become larger ones. The primary coolant piping, valve packing, and pump seals are notorious problem areas. Small leaks of borated water can lead to more serious problems via boric acid corrosion. Currently, leaks are detected by a combination of area radiation monitors, sump level monitors, and monitors on the condensate flow from the building air coolers. Because of the number of valves, length of pipe, and number of pump seals to be monitored, pointwise acoustic monitoring of the plant is prohibitively expensive. However, distributed acoustic monitoring of the primary pressure boundary shows promise for leak detection.[14]

One possible distributed acoustic leak detector is based on the Sagnac resonator. The position of the noise source alters the null frequencies of the resonator, thereby allowing it to act as a distributed sensor. This technology shows promise for the future; however, significant development work remains to be done. Another possible distributed leak measurement scheme involves running bare fiber into leak accumulation areas. Water contacting the bare fiber will alter the fiber's light guiding properties (introducing a light loss point). These light loss points would then be detected using OTDR techniques. The main limitations of this technique are the fragility of bare optical fiber and the difficulty of repairing a failed fiber segment while the plant remains on-line.

10. VIBRATION MEASUREMENT

Vibration measurement yields important information on the status of moving equipment and can be implemented optically and noninvasively. Pointing an optical fiber bundle at a reflective surface on the monitored equipment, illuminating the surface with fibers from the bundle center, and measuring the time and spatial location of the light back-coupled into the receiver fibers yield a signal proportional to equipment vibration. All the noise analysis tools conventionally used with accelerometers can then be applied to the resultant signal. In addition, the output optical signal can be normalized relative to reflection from the illumination fiber end cleave, thus reducing the signal variation due to radiation darkening of the fiber, connection variation, and power variation of the optical source. The major limitations of this type of system are the need for optical access and a requirement for clean optical surfaces.

Intrinsic, interferometric vibration measurements in two-mode fibers have also been demonstrated. In these sensors the fiber is attached to the vibrating component, and the vibration produces a phase differential between the two propagating modes.[15] The main weaknesses of this technique are that it requires contact with the vibrating component and that it is still in a laboratory stage of development. Also, microbending-based vibration measurement has been demonstrated.[16] In these sensors, the fiber is attached to the measured component, and its vibration (via some form of attached mass) causes microbending losses in the fiber. Since this is an intensity-based measurement, a multiwavelength ratiometric scheme is necessary to compensate for environmentally induced measurement variation. Other limitations of this technique are cyclic fatigue of the fiber and the requirement of contact with the equipment.

11. ELECTRICAL MEASUREMENTS

Circuit breaker status, power to critical equipment, generator output conditions, switchyard status, and transformer status are all important parameters for safe and efficient operation of nuclear power plants. The status of high-voltage electrical components is difficult to determine electrically because of the high levels of electromagnetic interference present. Fiber optic current and voltage measurements have been under investigation for over a decade.

One technique for optically measuring current is to wrap a highly circularly birefringent fiber around the current-carrying wire and then measure the rotation of polarized light in the fiber (Faraday effect). The main difficulty with this technique is cross sensitivity to vibration, fiber bending, and other environmental variables. However, novel techniques for reducing the dependence of the measurement on environmental variables have recently been demonstrated.[17] Although as yet no optical fiber current sensor has reached the market, electric field sensors based upon the Pockels effect have been demonstrated. In materials exhibiting the Pockels effect, the induced birefringence varies linearly with the electric field. Pockels-effect sensors thus pass light through Pockels-active optical media and measure the change in birefringence (typically, interferometrically). Fabry-Perot-based electric and magnetic field sensors have also been proposed and are under investigation by the Electric Power Research Institute.[18] In these sensors, materials that change optical path length in response to applied electric and magnetic fields are placed in the gap of a Fabry-Perot etalon. Thus, both the transmission and reflection spectrum of the etalon change with applied field. The main limitations of fiber optic current and voltage measurements are that (1) the desired sensors are at a relatively low state of development and (2) rather than measuring current and voltage directly, the sensors actually measure magnetic and electric fields.

12. CHEMICAL MEASUREMENT

A wide spectrum of chemical measurements are made at nuclear power plants. Water chemistry is monitored chiefly to ensure proper pH (and thereby prevent corrosion), detect fuel leaks, and monitor boron concentration. Atmospheric chemical monitoring is also important to plant safety and efficiency. The level of hydrogen in containment is a key parameter in postaccident scenarios, and effluent monitoring directly relates to public health. Advantages of optically based chemical sensing are its speed (measurements are performed on-line[19]) and its ability to access harsh environments.

Fiber optic chemical sensors are commercially available from several manufacturers. In these sensors, fibers are used to enable remote fluorescence, absorption, index-of-refraction, and spectroscopy measurements. Multiple wavelength ratiometric methods are incorporated into these sensors to promote stable and precise measurements. Fiber optic chemical sensing is winning rapid acceptance in the medical, industrial process, and environmental fields. Lidar-based systems are currently being used to monitor atmospheric pollutant levels in cities. Lidar-based sensing systems can create three-dimensional maps of effluent (including accidental releases) over distances of several kilometers. The main limitation of optical chemical sensing in nuclear power plants is the industry's unfamiliarity with it. Overall, several optically- based chemical sensors are currently available that are suitable for nuclear plant measurements, and the field is developing rapidly because of its wide applicability.

13. CONCLUSIONS AND RECOMMENDATIONS

Several conclusions are apparent from this review of the potential uses for fiber optic sensors in nuclear power plants:

- Fiber optic-based sensing has a wide range of applications in nuclear power plants.
- Fiber optic-based sensors are likely to eventually supplant many conventional sensors because of their inherent advantages (reduced mass, reduced size, ruggedness, physical flexibility, high sensitivity, electrical isolation, extreme resistance to EMI, resistance to high temperatures, reduced calibration requirements, passive operation, and resistance to nuclear radiation).
- Fiber optic-based sensors are capable of measuring parameters important to plant safety and performance that cannot be measured conventionally (high EM field, in-core temperature, and distributed measurements).
- Fiber optic sensors remain at too low a level of development for immediate application in safety-critical systems.
- Fiber optic sensors have different failure modes and mechanisms than conventional sensors, and hence considerable regulatory research will be necessary to establish the technical basis for the use of fiber optic sensors in safety-critical systems.

REFERENCES

1. D. W. Miller et al., *Radiation Effects on Optical Fibers*, EPRI-TR-100367, Electric Power Research Institute, 1992.
2. Vanzetti Systems, Inc., personal communication with Ed Mahoney, product engineer.
3. Eric Udd, *Fiber Optic Sensors*, John Wiley & Sons, Inc., New York, 1991, pp. 146–153.
4. M. Born and E. Wolf, *Principles of Optics*, Pergamon Press, Oxford, 1964.

5. Charles Kittel, *Introduction to Solid State Physics*, 6th ed., John Wiley & Sons, Inc., New York, 1986, p. 307.
6. A. A. Boiarski and V. D. McGinniss, *Fiber Optic Distributed Temperature Sensor Demonstration*, EPRI TR-101950, Electric Power Research Institue, March 1993.
7. J. Weiss, W. Esselman, and R. Lee, "Assess Fiber Optic Sensors for Key Power Plant Measurements," *Power*, pp. 55–58 (October 1990).
8. J.W. Berthold, W. L. Ghering, and D. Varshneya, "Design and Characterization of a High Temperature, Fiber-Optic Pressure Transducer," *IEEE Transactions on Lightwave Technology*, **LT-5**(7) (July 1987).
9. K. L. Belsley, D. R. Huber, and J. Goodman, "All Passive Interferometric Fiber-Optic Pressure Sensor," pp. 1151–1158 in *Proceedings of the ISA*, 1986.
10. S. A. McElhaney, D. D. Falter, R. A. Todd, M. L. Simpson, and J. T. Mihalczo, "Passive (Self-Powered) Fiber Optic Sensors," *Conference Record of the IEEE Nuclear Science Symposium*, Orlando, FL, Oct. 25–31, 1992.
11. A. S. Beddar, T. R. Mackie, and F. H. Attix, "Water-Equivalent Plastic Scintillation Detectors for High-Energy Electron Beam Dosimetry," *Phys. Med. Biol.*, **37**(10), 1883–1913 (1992).
12. Mario Martinelli and Valeria Gusmeroli, "Distributed Laser Doppler Velocimeter," *SPIE*, **1797**, 31–37 (1992).
13. M. C. Hastings and B. Chiu, "Simultaneous Measurement of Strain or Acoustic Pressure and Temperature with an Optical Fiber Interferometer," accepted for presentation and publication in *SPIE*, **2070**, Fiber Optic and Lasers Sensors XI, Sept. 7–10, 1993.
14. J. P. Kurmer, S. A. Kingsley, J. S. Laudo, and S. J. Krak, "Applicability of a Novel Distributed Fiber Optic Sensor for Leak Detection," *SPIE*, **1797**, 63–71 (1992).
15. Kent A. Murphy, Brian R. Fogg, and Ashish M. Vengsarkar, "Spatially Weighted Vibration Sensors Using Tapered Two-Mode Optical Fibers," *Journal of Lightwave Technology*, **10**(11) (November 1992).
16. D. R. Miers, D. Raj, and J. W. Berthold, "Design and Characterization of Fiber-Optic Accelerometers," SPIE OE/FIBERS Conference, San Diego, CA, August 16–21, 1987.
17. Natale C. Pistoni and Mario Martinelli, "Vibration-Insensitive Fiber-Optic Current Sensor," *Optics Letters*, **18**(4), 314–316 (Feb. 15, 1993).
18. T. F. Morse, A. Mendez, L. Reinhart, and J. Stein, "A Novel Optical Fiber Electric Field Sensor," *Proceedings: 1992 Workshop Optical Sensing in Utility Applications*, EPRI-TR-102349, May 1993.
19. A. A. Garrison, C. F. Moore, M. J. Roberts, and P. D. Hall, "Distillation Process Control Using Fourier Transform Raman Spectroscopy," *Process Control and Quality*, 3, 57–63 (1992).

Engineering the Development of Optical Fiber Sensors for Adverse Environments

Mardi C. Hastings, P.E., Ph.D.
The Ohio State University
Department of Mechanical Engineering
Columbus, Ohio 43210

ABSTRACT

During the last decade, many optical fiber sensors have been developed for particular applications in harsh environments with limited success. Off–the–shelf optical fiber sensors and measurement systems are not available, partly because they have not been engineered to meet tough environmental requirements necessary for applications outside the laboratory. Moreover, no generalized computer–aided tools exist to help advance their development, design, and use. Computer–aided design tools currently being developed are described in this paper. Structural finite element analyses have been coupled with optoelastic analyses of both all–fiber interferometers and serial microbend sensors for distributed measurement of various physical quantities. The combined analyses have been parameterized and implemented on personal computers and work stations for use as design/development tools that can be used to determine the performance of different sensor configurations in various environments. Potentially, these computer–aided tools could be used for failure diagnosis and redesign of existing optical fiber sensors. Performances predicted by the computer simulations are verified with experimental data and numerical analyses from the literature. The long–term goal is to develop user–friendly software packages for both sensor manufacturers and end users.

INTRODUCTION

Optical fiber sensors offer immunity to electromagnetic interference and inherent electrical isolation which give them many advantages over their electromechanical counterparts where noise, high voltage, and ground loops are problems. In addition, these sensors may be installed in previously inaccessible areas because of their relatively small size and small, flexible connecting fiber. Thus they have significant potential for use in harsh environments, high–speed rotating machinery, biomedicine and other applications that require remote sensing. Over the last decade, many sensors have been developed for particular applications in these areas with limited success. In many cases, off–the–shelf optical fiber sensors and measurement systems are not available because they have not been engineered to meet the environmental requirements necessary for applications outside the laboratory.

The objective of the current work is to develop generalized computer–aided design tools to help advance development, design and use of optical fiber sensors. Use of these tools will reduce empirical iterations in the development and design stage, and thus reduce cost. The development

of these tools is inter–disciplinary in nature. Engineering mechanics must be integrated with electromagnetic wave theory and communications theory.

Types of Optical Fiber Sensors

Optical fiber sensors may be divided into three different categories: intensity modulated, phase modulated, and change in state of polarization. The first category, intensity modulated, includes extrinsic reflective type sensors, mode–mode interference sensors, and microbend sensors. In extrinsic reflective type sensors, the light leaves a large core multimode fiber or a fiber bundle, reflects from an external surface, and re–enters the fiber or adjacent fibers in the bundle. The intensity of the reflected light that re–enters the fiber(s) is a function of the distance between the end of the fiber and the surface. This type of sensor is relatively simple and already has wide industrial use, so it will not be considered here. Mode–mode interference sensors are based on launching two or three light modes in a single mode or relatively small core multimode fiber. Interference between the modes caused by an external disturbance (e.g., pressure or temperature) changes the intensity of the output. These sensors require either a special fiber, light source, or launching conditions to ensure that only a few modes will propagate in the fiber. Microbend sensors are by far the most common intensity modulated fiber sensors. In these sensors, a small length of multimode fiber is pressed between a series of bends where the disturbance to be measured acts on the sensor. The series of bends has a spatial wavelength that causes the light modes traveling in the fiber core to be coupled out of the fiber. This causes a loss in transmitted light that is proportional to the amplitude of the transverse deformation of the fiber core and thus the measurand. Although these linear sensors are easy to fabricate, mathematical modeling of the transduction mechanism is extremely difficult. Theory predicts the optimum spatial wavelength of the microbend, but it does not describe sensing conditions at that optimum or off–optimum.

Phase modulated sensors include all types of fiber interferometers. These interferometers use single mode or polarization–maintaining fibers because a single phase difference can be measured only between two single modes of light. Polarization–maintaining fibers forcefully maintain the two polarized states of a single mode; if regular single mode fiber is used, then a manual polarization controller must be used on one arm of the interferometer to match the polarization orientations at the output. In these sensors the phase difference between a sensing light mode and a reference light mode is a function of the disturbance to be measured which acts on the sensing portion of the fiber. Sagnac interferometers are the basis for commercially available fiber optic gyroscopes. Other types include the Michelson and Mach–Zehnder interferometers. These sensors are more difficult to construct than microbend sensors but are much easier to analyze.

In change–in–state–of–polarization sensors, the disturbance to be measured creates a mixing of the polarized states of one or more light modes traveling in the core of the fiber. These sensors are similar to mode–mode interference sensors except that the interference occurs between two polarized states rather than two modes. These types of sensors also require special fibers and light launching conditions and are not in wide use. Thus the focus of the current study is on the most common optical fiber sensors, microbend and fiber interferometers.

MICROBEND SENSORS

Figure 1 illustrates the basic principle of a microbend sensor. A short length of the fiber is sandwiched between two deformers. An external disturbance such as displacement, force, or temperature acts on the deformer and transversely bends the fiber core. This causes light traveling in the core to leave the fiber. Figure 2 shows an example application of many microbend sensors placed in series and monitored by an optical time domain reflectometer (OTDR) to measure the surface temperature of a high pressure steam line.

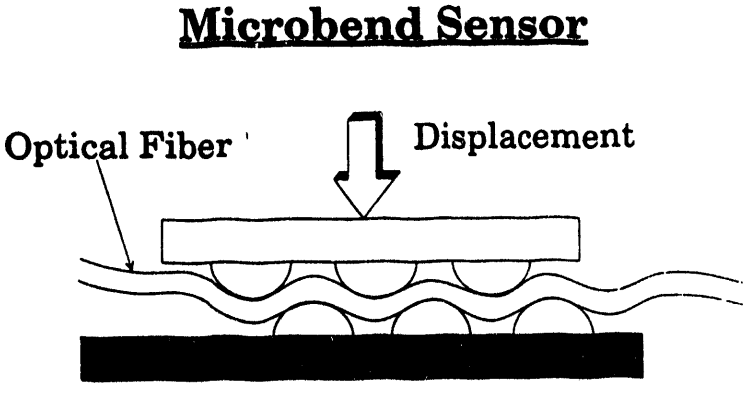


Figure 1. Simplified schematic of an optical fiber microbend sensor.

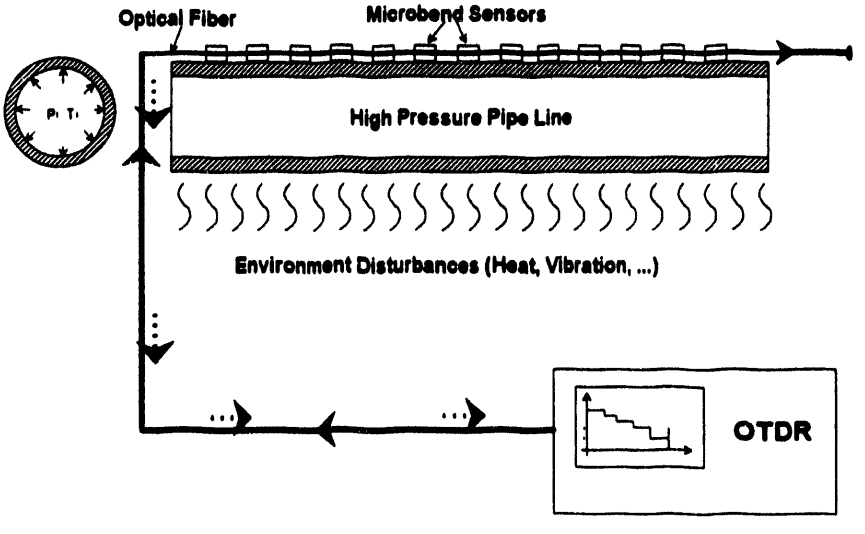


Figure 2. Illustration of an application of serial microbend sensors to measure surface temperature of a high pressure steam line using an optical time domain reflectometer (OTDR).

Electromagnetic wave theory predicts that power lost from the core in a microbend is optimum when the fiber's spatial bend frequency equals the difference in propagation constants between the propagating and radiated modes. Theory fails to predict, however, how the sensor performs at the corresponding optimum spatial wavelength or what happens if the optimum wavelength is not used. Generally, all performance questions are addressed experimentally during the sensor development and design stages. This is not only costly, but sensor performance outside the bounds of the experiment remains unknown.

Modeling of Light Propagation through a Microbend

Many parameters contribute to the performance of this sensor. These include fiber core radius, cladding radius, jacket radius, core and cladding refractive indices, core refractive index profile, fiber flexural rigidity, light source wavelength, light source power, spatial bend wavelength, number of bends and bend amplitude. Several approaches were considered to develop a mathematical or numerical model for the propagation of light through a microbend that would incorporate all the parameters involved. These included ray tracing, Fourier Transform beam propagation, and finite difference beam propagation.

Ray tracing was used by Mavaddat (1984) on a two-dimensional model of a step index fiber. Graded index fibers and fibers with microbend-induced stresses which alter the index profile due to the photoelastic effect, have more complex and irregular refractive index profiles; consequently they are not well suited for ray tracing analysis. Beam propagation methods are easier to apply when the refractive index profile is not uniform. The finite difference beam propagation method (BPM) summarized by Chung and Dagli (1990) was superior to the Fourier Transform BPM described by Feit and Fleck (1978) in computing time and application of boundary conditions. Thus the finite difference BPM was determined to be the best approach.

The BPM is based on the solution of the Helmholtz equation (i.e., wave equation for constant frequency) for a paraxial, transverse electric field traveling in a two-dimensional slab:

$$2jk_o n_o \frac{\partial E_y}{\partial z} = \frac{\partial^2 E_y}{\partial x^2} + k_o^2\left[n^2(x,z) - n_o^2\right]E_y \tag{1}$$

where k and n are the wave number and refractive index, respectively, and the subscript o denotes the centerline of the fiber. Equation (1) describes the y transverse component of an electric field traveling in a medium transverse in the x direction and longitudinal in the z direction. Using a center-based finite difference scheme to discretize the field and medium yields:

$$\begin{aligned} &-a_i E_{i-1}(z+\Delta z) + b_i E_i(z+\Delta z) - a_i E_{i+1}(z+\Delta z) \\ &= a_i E_{i-1}(z) + c_i E_i(z) + a_i E_{i+1}(z) \end{aligned} \tag{2}$$

where

$$a_i = \frac{\Delta z}{2\Delta x^2},$$

$$b_i = \frac{\Delta z}{\Delta x^2} - \frac{\Delta z k_o^2}{2}\left(n_i^2(z+\Delta z) - n_o^2\right) + 2jk_o n_o \text{, and}$$

$$c_i = \frac{\Delta z}{\Delta x^2} - \frac{\Delta z k_o^2}{2}\left(n_i^2(z) - n_o^2\right) + 2jk_o n_o .$$

When extended over the entire computational grid, Equation (2) forms a tridiagonal matrix which can be solved using a digital computer algorithm.

Formulation of the proper boundary conditions are extremely important in the numerical model. Recently Hadley (1992) reported the development of an algorithm for implementation of a "transparent boundary condition" for use with the BPM. The transparent boundary condition assumes that the electric field approaching the boundaries can be described as $E = E_o e^{jk_x x}$ where k_x is the x–direction propagation constant of the field. It indicates how rapidly energy is approaching a boundary. By monitoring this parameter after each computational step, the appropriate level of absorption is determined. This boundary condition requires that at the left boundary ($i = 1$):

$$\frac{E_1(z)}{E_2(z)} = \frac{E_1(z+\Delta z)}{E_2(z+\Delta z)} = e^{jk_{x1}\Delta x} \tag{3}$$

and at the right boundary ($i = N$):

$$\frac{E_N(z)}{E_{N-1}(z)} = \frac{E_N(z+\Delta z)}{E_{N-1}(z+\Delta z)} = e^{jk_{xN}\Delta x} \tag{4}$$

where Δx is the distance between adjacent grid points in the x direction.

The refractive index profile is easily placed on the computational grid by using a one–dimensional array of size N containing the indices of refraction $n_i(z)$. To begin the analysis, an electric field, initially of Gaussian profile, is propagated down the fiber until a steady state electric field develops as determined by a constant (with propagation distance) energy distribution in the core, cladding, jacket and air, and the magnitude of the on–axis field. Then the steady state beam is stored to be used as input to the microbend section of the sensor simulation.

Modeling of Fiber Deformation

A two-dimensional finite element model (FEM) was developed for an optical fiber deformed by a microbend using ANSYS (1993). The model is simply repeated for multiple bends. The FEM determines changes in the refractive index profile caused by (1) fiber deformation and (2) the photoelastic effect due to the induced stress-strain state. Using the strains predicted by the FEM, the change in refractive index is determined by the Lorentz-Lorenz relation:

$$\Delta n = -\frac{1}{2} n_i^2 p \varepsilon \tag{5}$$

where p is the photoelastic material property (Pockel's coefficient) and ε is the strain amplitude.

Microbend Simulation Program

A program was written which performs the microbend loss analysis by integrating the BPM and FEM. Figure 3 shows the fiber finite element grid integrated with the 2048 node finite difference beam propagation grid. The finite difference grid is larger than the finite element one because the BPM includes the surrounding medium (air). An algorithm was developed to determine the resulting refractive index distribution.

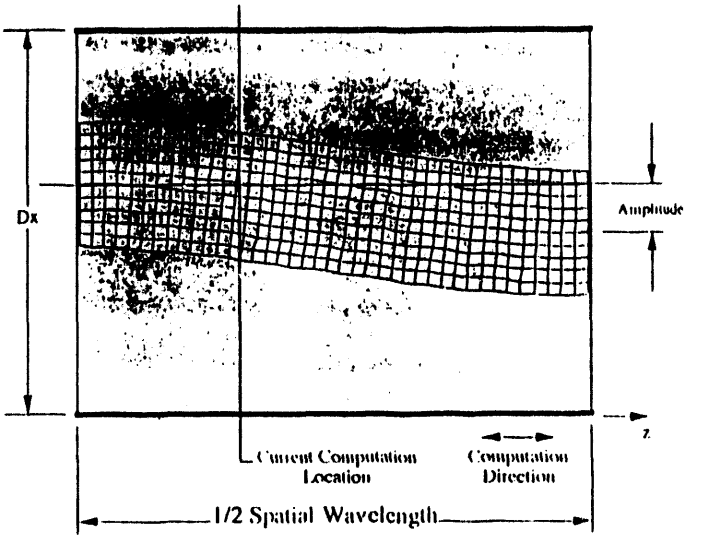
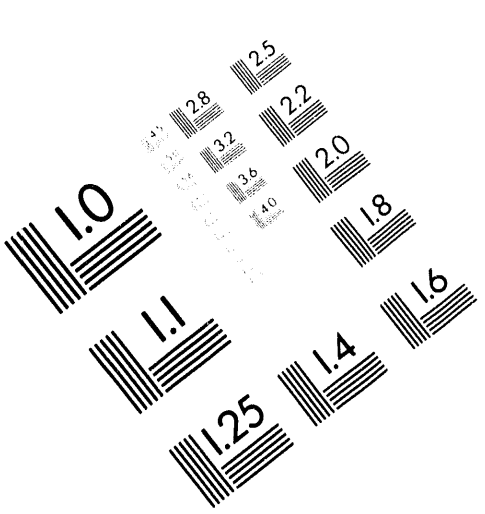
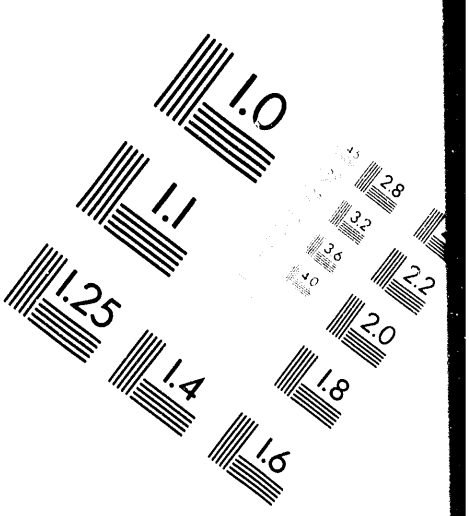


Figure 3. Integration of FEM and finite difference BPM grids.

Figure 4 shows the structure of the overall program which was written in the C programming language and runs on an SGI work station. A user defined script file is used at the start of the program to specify the physical parameters for a particular microbend configuration. After propagating the source beam to steady state and storing it for future use, the program propagates the beam through a specified number of microbends defined by the FEM. Then the beam is again

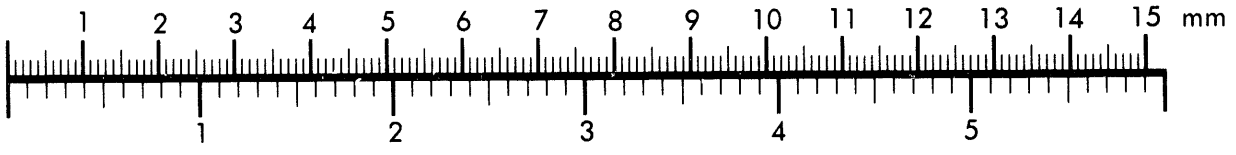



Association for Information and Image Management

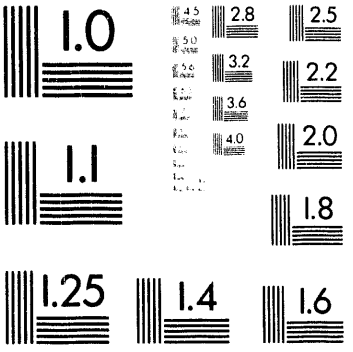
1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910

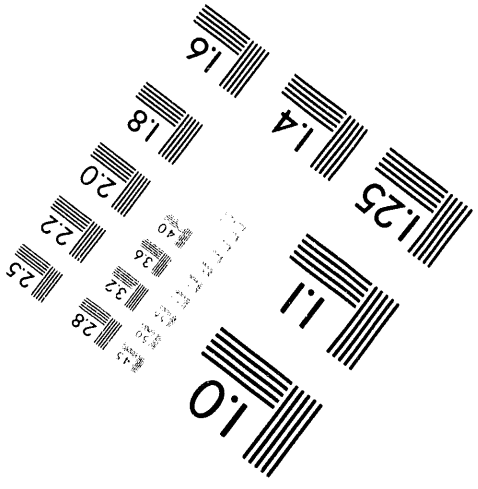
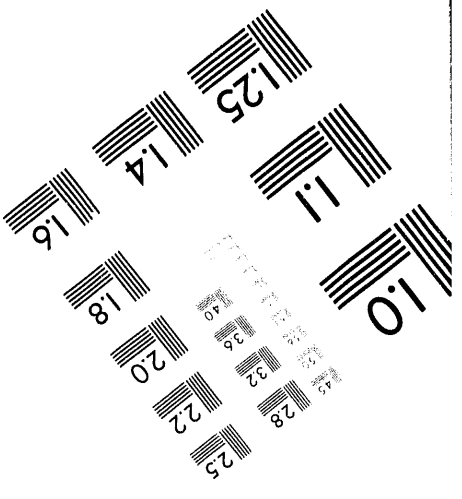
301/587-8202

Centimeter



Inches



MANUFACTURED TO AIIM STANDARDS
BY APPLIED IMAGE, INC.

3 of 7

propagated to steady state. The transmission loss is determined by the difference between the steady state power before the microbend and the steady state power after the microbend.

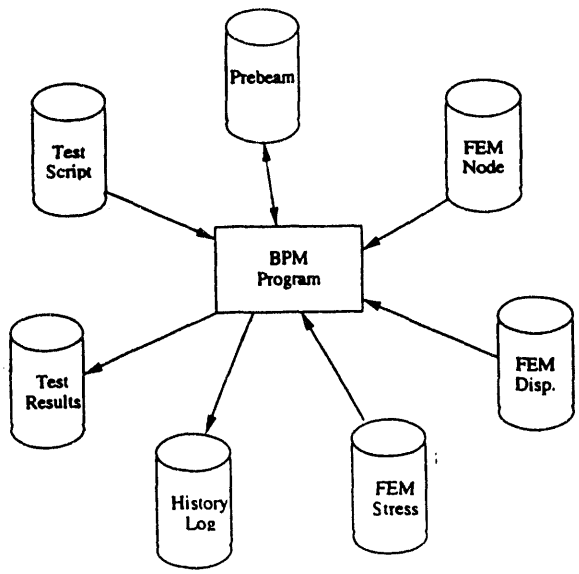


Figure 4. Structure of microbend sensor simulation program.

Simulation Results

The microbend sensor simulation program was correlated with experimental measurements using AT&T 100/140/250 multimode graded index optical fiber with source wavelengths of 633 nm and 1300 nm. Using the simulation, the spatial wavelength of a sinusoidal bend was varied from 0.5 mm to 2.5 mm for 2, 4, 6, 8, and 10 bends to determine if the model would predict the theoretical optimum spatial wavelength and correlate with experimental measurements. The domain width of the model was 500 μm, twice the diameter of the fiber, and the computational step size in the direction of propagation was 1 μm.

Figure 5 is a three–dimensional plot of a developing beam in the fiber from a 1300 nm source. This figure clearly shows that the light is contained within the fiber core and the group velocity of signals traveling in a parabolic graded index fiber. Figure 6 displays the index of refraction profile of the fiber as predicted by the FEM that includes the photoelastic effect. This figure indicates that much of the deformation occurs in the fiber coating. Thus the compliance of the coating significantly affects microbend sensor performance. Figure 7 is a three–dimensional plot of the beam propagating through a microbend after it has reached steady state. This figure explicitly shows loss of power from the core. The maximum field magnitude is about half that of the developing beam in Figure 5.

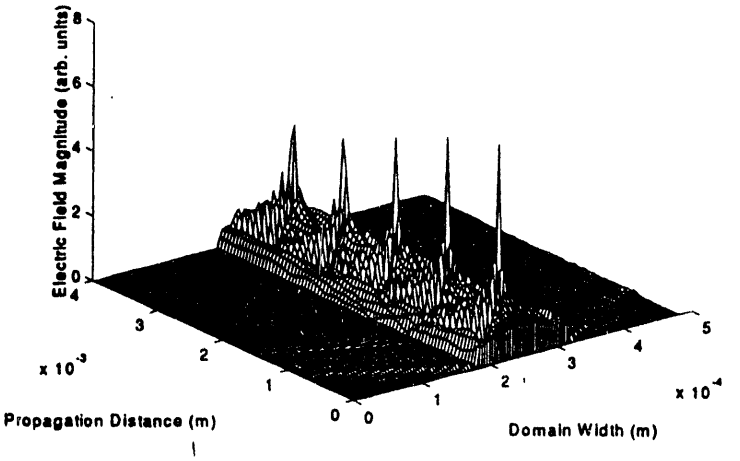


Figure 5. Finite difference BPM simulation of a beam developing in an AT&T 100/140/250 graded index multimode fiber.

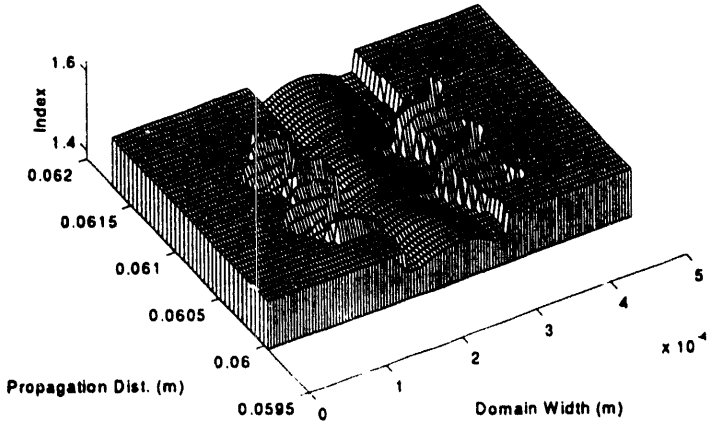


Figure 6. Refractive index profile predicted by the fiber FEM and integrated with the BPM grid.

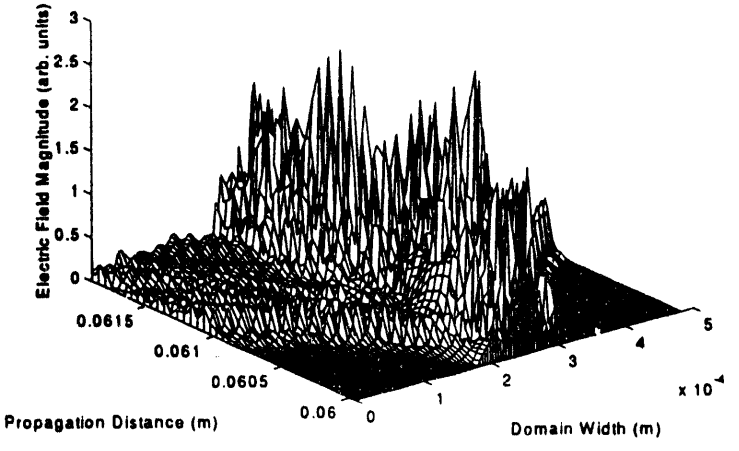


Figure 7. Beam propagation through the microbend as predicted by the simulation.

Figure 8 displays the transmission loss predicted by the microbend sensor simulation as a function of the number of bends and spatial wavelength. The overall spectral broadening and decrease in transmission loss with a decrease in the number of bends was experimentally measured by Horsthuis and Fluitman (1982). The theoretical optimum spatial wavelength for the AT&T fiber is 1.57 mm. The curves for 4, 6, 8, and 10 bends predict an optimum transmission loss between 1.5 and 1.6 mm. The cause of the decrease in the curve for 2 bends at the optimum spatial wavelength is being investigated. No experimental measurements are available to verify this result.

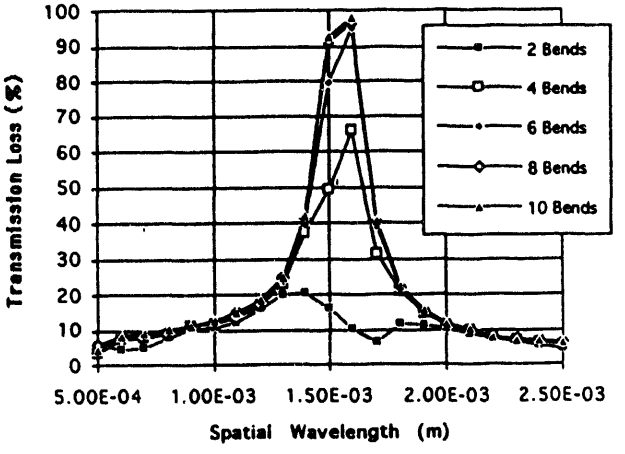


Figure 8. Transmission loss predicted by the simulation as a function of spatial wavelength and number of bends for AT&T 100/140/250 graded index multimode fiber.

Figure 9 shows the results of experimental measurements to determine the microbend sensitivity of the AT&T fiber at spatial wavelengths of 0.5, 1.0 , 1.5 and 2.0 mm. These measurements, which predict the optimum spatial wavelength to be at or near 1.5 mm, are in excellent agreement with both electromagnetic wave theory and the finite difference BPM microbend sensor simulation.

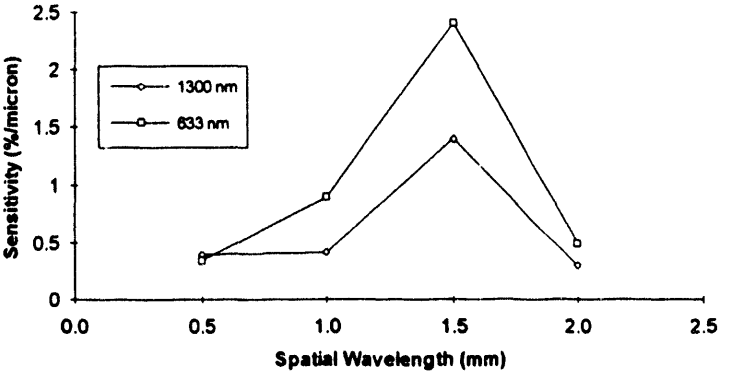


Figure 9. Experimental verification of the optimum spatial wavelength for the AT&T 100/140/250 graded index multimode fiber.

Summary

Work is continuing to further correlate microbend sensor simulation results with experimental measurements. A major problem is obtaining material properties for the different sections of the fiber, particularly the coating. In addition, experimental work has begun using a high resolution OTDR to examine the back scatter output of three microbend sensors in series. A preliminary model for the back scattered signal has been developed. Finally, the simulation is being applied to develop a model for a prototype microbend temperature sensor to further verify and enhance its capabilities as a design and development tool.

INTERFEROMETRIC SENSORS

Considerable interest exists in embedding optical fiber sensors in composite materials to provide spatially distributed sensing for health monitoring over the life of the structure, so this was chosen as an example to exercise the sensor simulation. Figure 10 illustrates this example for an all polarization–maintaining (PM) fiber Mach–Zehnder interferometer being developed for simultaneous measurement of strain and temperature. The two forcefully maintained polarization states act as two separate interferometric sensors. The 1×2 and 3×3 couplers form the interferometer structure. The former splits light from a laser source between the arms of the interferometer. The later combines light from the sensing and reference arms for passive homodyne demodulation. The sensing arm is embedded in a cantilevered E–glass/epoxy coupon. For true simultaneous measurement of temperature and strain, two polarizers and another 3×3 coupler (not shown in Figure 10) would be needed to separate the polarizations prior to interferometry and process signals from each state.

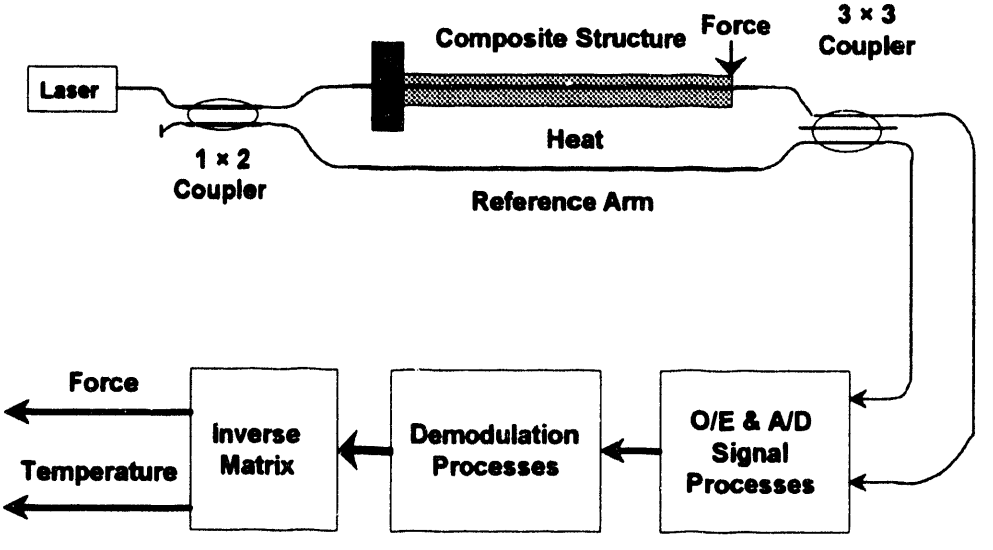


Figure 10. Composite beam with embedded optical fiber for simultaneous measurement of strain and temperature using Mach–Zehnder interferometry.

Optical Analysis

Figure 11 displays the cross-section of the PM fiber used in this study. The residual stress region (RSR) between the cladding and outer cladding maintains the orientation of the polarized states of the single mode propagating in the core. The diameter of the core is 10 μm and the outer diameter of the fiber is 250 μm.

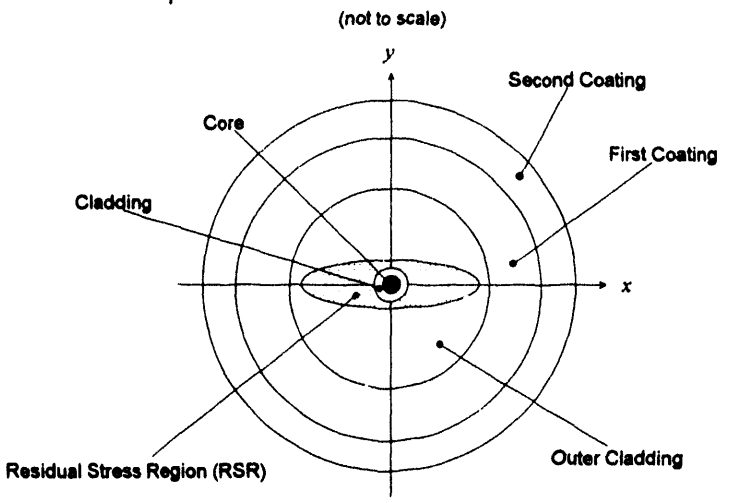


Figure 11. Cross-section of PM fiber.

For a PM fiber with length L and longitudinal propagation constants β_p and β_s, where p and s indicate the fast and slow polarized states of the single mode lightwave traveling inside the fiber core, respectively, the phase ϕ_j of each polarization is $\phi_j = \beta_j L$, where $j = p,s$, $\beta_j = 2\pi n_j / \lambda$, λ is the free space wavelength, and n_j the refractive index. The changes in phase of the two polarized states due to an external disturbance acting on the fiber are:

$$\Delta\phi_{jT} \approx \left[\beta_j \frac{\partial L}{\partial T} + L\frac{\partial \beta_j}{\partial T}\right]\Delta T \tag{6}$$

and

$$\Delta\phi_{j\xi} \approx \left[\beta_j \frac{\partial L}{\partial \xi} + L\frac{\partial \beta_j}{\partial \xi}\right]\Delta \xi \tag{7}$$

Equations (6) and (7) may be expanded, evaluated in terms of the Cartesian strain components in the fiber core, the strain optic coefficients (Pockel's coefficients), and the refractive index temperature coefficient, $\partial n_j / \partial T$ (a material property), and then summed to yield the total phase change, $\Delta\phi_j$ (= $\Delta\phi_{jT}$ + $\Delta\phi_{j\xi}$), of each polarized state of the lightwave [Hocker, 1979; Hughes and Jarzynski, 1980]:

$$\Delta\phi_j \approx \left[\beta_j L\varepsilon_z \frac{\beta_j L}{n_j}\frac{\partial n_j}{\partial T}\Delta T - \beta_j L\left\{\frac{n_j^2}{2}\left[P_{11}\varepsilon_{xj} + P_{12}\varepsilon_{yj} + P_{12}\varepsilon_z\right]\right\}\right]_T + \left[\beta_j L\varepsilon_z - \beta_j L\left\{\frac{n_j^2}{2}\left[P_{11}\varepsilon_{xj} + P_{12}\varepsilon_{yj} + P_{12}\varepsilon_z\right]\right\}\right]_\xi \quad (8)$$

where P_{11} and P_{12} are Pockel's coefficients, and ε_{xj}, ε_{yj}, ε_z are Cartesian strain components in the fiber core. Although the longitudinal strain ε_z, is the same for both polarized states, the transverse strains, ε_{xj} and ε_{yj}, are different due to the anisotropy in the PM fiber core and cladding. The subscripts T and ξ indicate that the bracketed quantities are evaluated for a particular change in temperature and longitudinal strain, respectively. Thus the strains in the fiber core must be determined for a particular sensing configuration and measurand.

Simulation Program Structure

Figure 12 illustrates the structure of the Mach–Zehnder interferometric sensor simulation program. For the example shown in Figure 10, the macro structure analysis is a FEM of the whole composite beam and its loading (end force and temperature). The stress–strain state of the macro structure is used to determine the boundary conditions for the micro structure FEM of the fiber and the region immediately surrounding it [Davidson and Roberts, 1992; Valis, et al., 1991]. In this case the macro structure, a 2.5×25×1.0 cm E–glass/epoxy coupon is modeled with 1050 anisotropic elements using ANSYS (1993). Figure 13 displays the geometry used for the micro structural analysis. Due to symmetry, the micro structure FEM grid is one–quarter of the physical region. For longitudinal strain and temperature measurands, the fiber is approximated as two 2–D slab waveguides, one for each polarized state. For the FEM, this is equivalent to having one slab waveguide for the x–z plane and another for the y–z plane (z is the longitudinal axis). Each slab waveguide is one fiber diameter wide and contains 2500 four–node, quadrilateral structural solid elements.

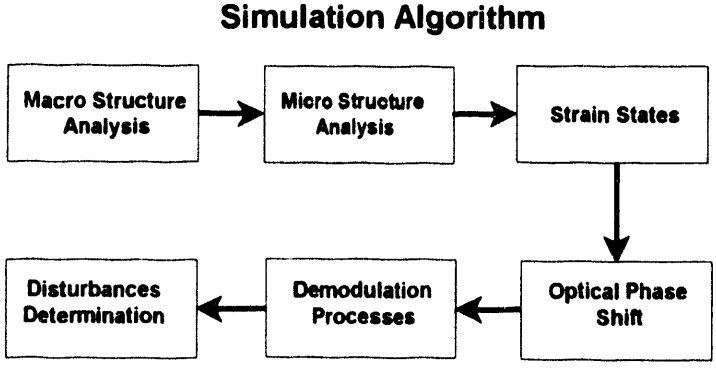


Figure 12. Simulation program structure for the all fiber Mach–Zehnder interferometric sensor.

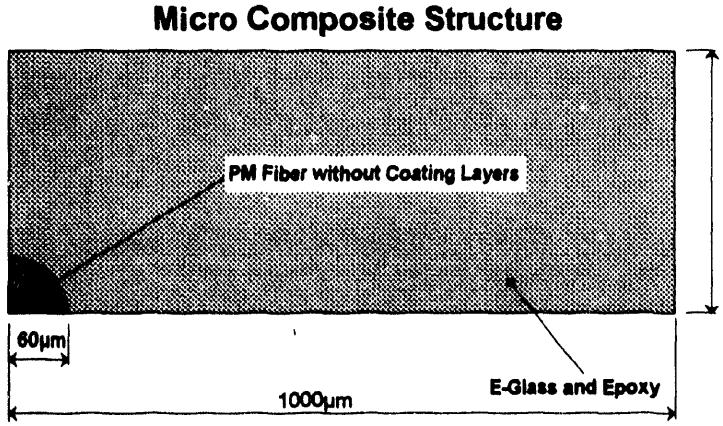


Figure 13. Geometry for FEM of fiber and adjacent region in E–glass/epoxy coupon.

The phase difference between the reference and sensing arms for each polarized state of the single mode lightwave is determined from the output a 3×3 fiber optic coupler where the reference and sensing arms are combined. The 3×3 coupler provides the following signals:

$$\begin{aligned} I_1 &= B_1 + B_2\cos\Delta\phi + B_3\sin\Delta\phi \\ I_2 &= B_1 + B_2\cos\Delta\phi - B_3\sin\Delta\phi \\ I_3 &= -2B_2(1+\cos\Delta\phi) \end{aligned} \tag{9}$$

where B_1, B_2, and B_3 are constants that are properties of the coupler and $\Delta\phi$ is the desired phase shift information. By adding and subtracting I_2 and I_3, the following outputs are obtained:

$$\begin{aligned} V_1 &= I_1 + I_2 = 2B_1 + 2B_2\cos\Delta\phi \\ V_2 &= I_1 - I_2 = 2B_3\sin\Delta\phi \end{aligned} \tag{10}$$

where the phase difference between V_1 and V_2 is always $\pi/2$. Photodetectors receive the two lightwaves exiting the 3×3 coupler and generate currents proportional to their intensity. Preamplifiers convert the currents into voltage signals. A software algorithm was developed for the simulation program to extract the phase shift information. Equation (8) is really a set of two equations, one for each polarized state. By substituting the strain state determined by the FEM and the phase shift for each polarized state determined from the output of each 3×3 coupler in Equation (8), ΔT and $\Delta\xi$ can be determined using matrix inversion.

Simulation Results

For the simulation, the composite beam of Figure 10 was loaded with an alternating force and slowly increasing temperature shown in Figure 14. Each simulation point represents a point in time. The stress–strain state in the fiber core was determined using the macro and micro FEM's. Figure 15 displays the corresponding output from the 3×3 coupler for the *p*–polarization. A similar output was obtained for the *s*–polarization.

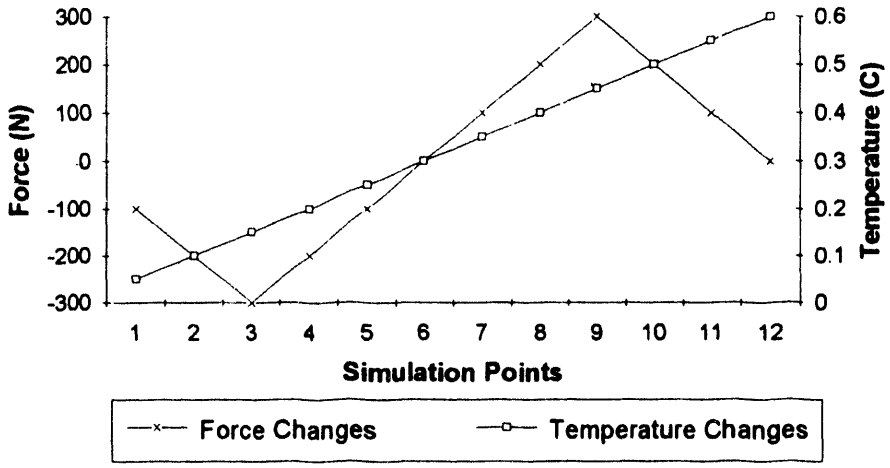


Figure 14. Force and temperature inputs for the interferometric sensor simulation.

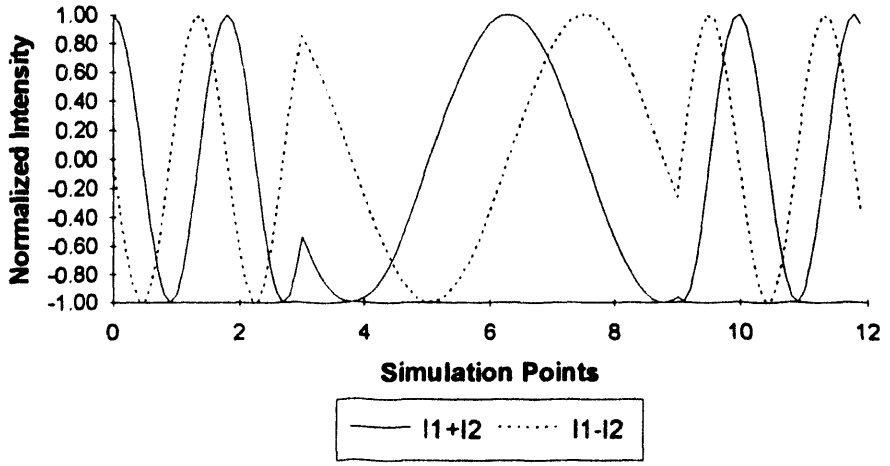


Figure 15. Intensity outputs from the 3×3 coupler for the *p*–polarization.

Figures 16 and 17 show the excellent agreement between the inputs to the simulation and the predicted values obtained from the demodulation algorithm using intensity outputs from the 3×3 coupler for each polarized state.

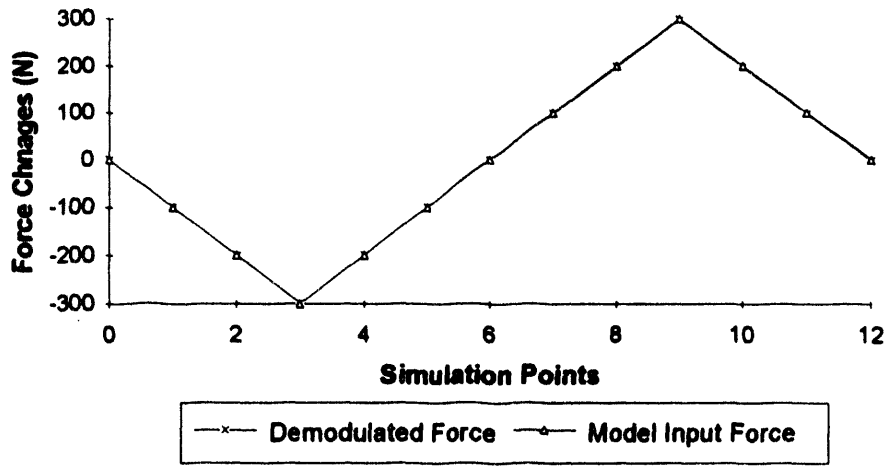


Figure 16. Comparison between simulation input and demodulated force changes.

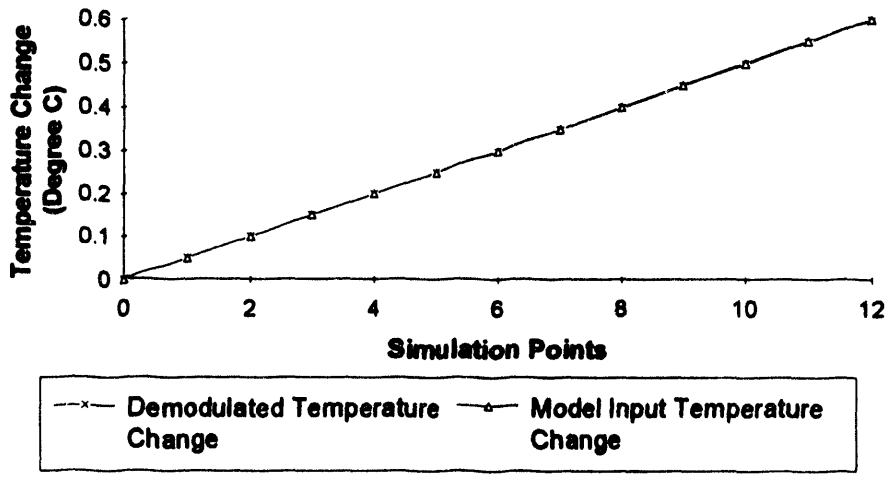


Figure 17. Comparison between simulation input and demodulated temperature changes.

Figures 18 and 19 show the sensitivities of the optical fiber interferometer to force and temperature acting on the beam. The fiber sensor is linear over the ranges investigated. The sensitivity to changes in temperature is negative because this parameter depends on the differential coefficient of thermal expansion between the glass fiber and the composite beam. If the fiber were not embedded in the beam, then the sensitivity would be positive.

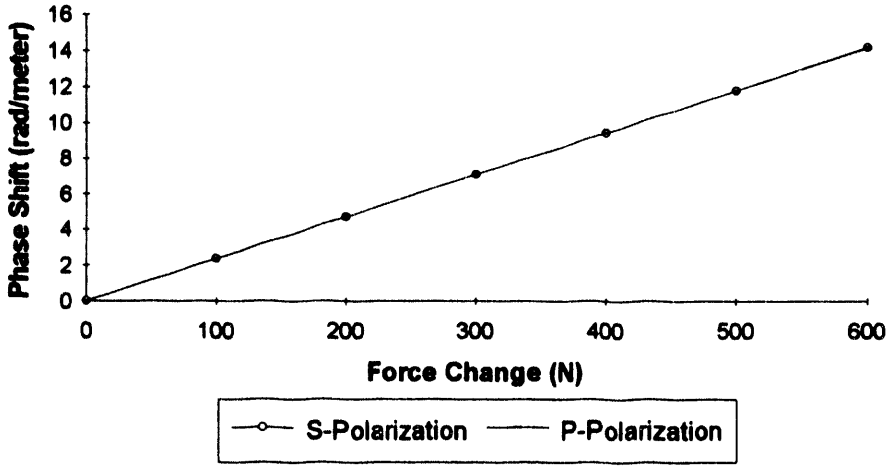


Figure 18. Sensitivity of the fiber sensor to force changes as predicted by the simulation.

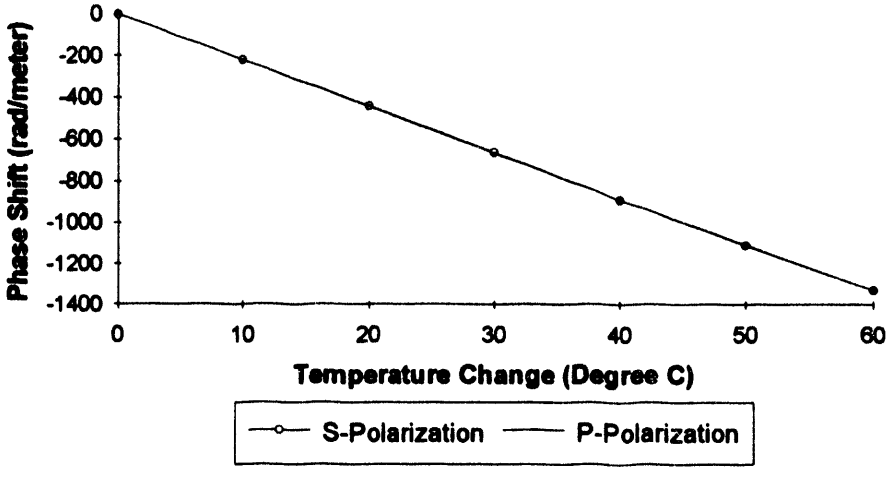


Figure 19. Sensitivity of the fiber sensor to temperature changes as predicted by the simulation.

Summary

The output of the fiber interferometric sensor simulation successfully agreed with the force and temperature inputs to the simulation. Currently, experimental measurements are being made and correlated with simulation predictions. Figure 20 shows a schematic of the experimental setup in which heat and strain are applied simultaneously to the sensing portion of the fiber. Both static and dynamic measurements at frequencies up to 1000 Hz are being made. For dynamic measurements, the translation stage is replaced with a shaker. Figure 21 reveals the excellent agreement between measured and predicted axial strains. Experimental work is continuing.

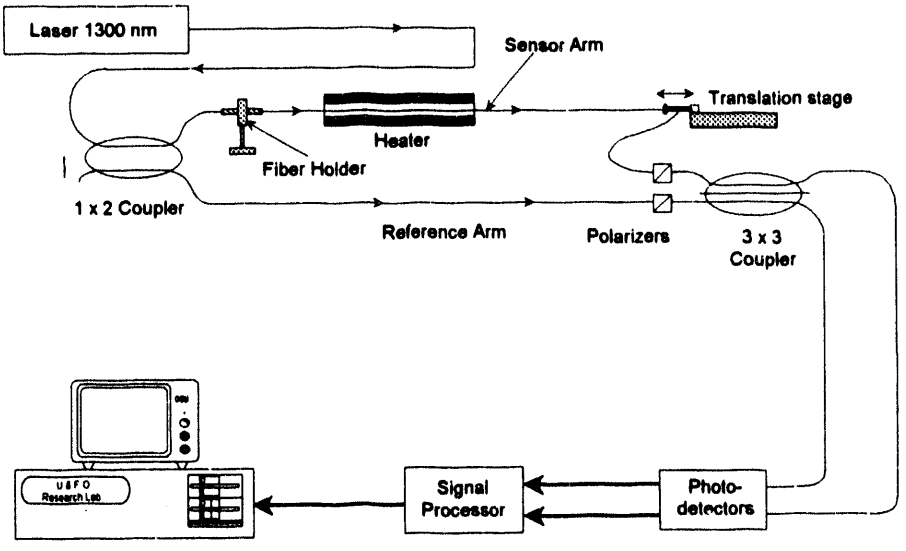


Figure 20. Schematic of experimental setup for PM fiber interferometer with passive homodyne demodulation.

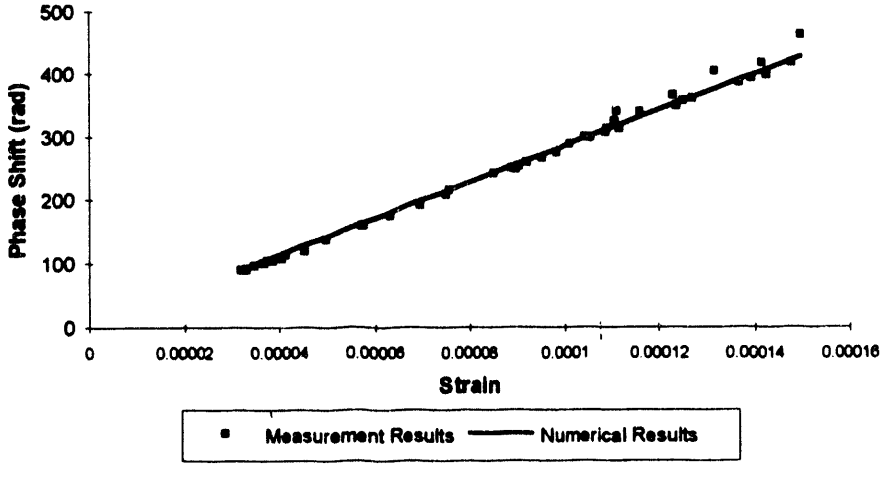


Figure 21. Correlation between measured and predicted phase shifts for *p*–polarization axial strain.

CONCLUSIONS AND RECOMMENDATIONS

Preliminary results from computer simulations developed for microbend and Mach–Zehnder interferometric fiber sensors indicate the potential for useful computer aided development and design tools. Applicable computer models could be used to reduce empirical iterations during sensor development, and diagnose problems and failures after installation in the field. The long–

term goal is to develop user-friendly software packages that integrate the engineering mechanics with electromagnetic wave theory for use by both sensor manufacturers and end users.

ACKNOWLEDGMENTS

Mr. David Nippa and Mr. Bornain Chiu, graduate students at the Ohio State University, developed the software for the microbend and interferometric sensor simulation programs, respectively, and experimentally verified the output. They also contributed many of the figures. In addition, AT&T donated the multimode optical fiber for the microbend sensor study.

REFERENCES

ANSYS ver. 5.0 (1993), Swanson Analysis Systems Inc., Houston, PA.

Chung, Y. and Dagli, N. (1990). An assessment of finite difference beam propagation method. **IEEE Journal of Quantum Electronics, Vol. 26**, No. 8, pp. 1335-1339.

Davidson, R. and Roberts, S. S. J. (1992). Finite element analysis of composite laminates containing transversely embedded optical fiber sensors. *Proceedings of the 1st European Conference on Smart Structures and Materials*, Glasgow, pp. 115-122.

Feit, M. D. and Fleck, J. A. (1978). Light propagation in graded-index optical fibers. **Applied Optics, Vol. 17**, No. 24, pp. 3990-3998.

Hadley, G. R. (1992). Transparent boundary condition for the beam propagation method. **IEEE Journal of Quantum Electronics, Vol. 28**, No. 1, pp. 363-370.

Hocker, G. B. (1979). Fiber-optic sensing of pressure and temperature. **Applied Optics, Vol. 18**, No. 9, pp. 1445-1448.

Horsthuis, W. H. G. and Fluitman, J. H. J. (1982). The development of fibre optic microbend sensors. **Sensors and Actuators, 3**, pp. 99-110.

Hughes, R. and Jarzynski, J. (1980). Static pressure sensitivity amplification in interferometric fiber-optic hydrophones. **Applied Optics, Vol. 19**, No. 1, pp. 98-107.

Mavaddat, R. (1984). Ray analysis of microbend fibre sensors. **Sensors and Actuators, 6**, pp. 289-295.

Valis, T., Tapanes, E., Kexing, L. and Measures, R. M. (1991). Passive-quadrature demodulated localized-Michelson fiber-optic strain sensor embedded in composite materials. **Journal of Lightwave Technology, Vol. 9**, No. 4, pp. 535-543.

On-Line Calibration Monitoring for Instrumentation Channels in Nuclear Power Plants

H. M. Hashemian
D. W. Mitchell

Analysis and Measurement Services Corporation
AMS 9111 Cross Park Drive
Knoxville, Tennessee 37923 USA

Phone: (615) 691-1756
Fax: (615) 691-9344

ABSTRACT

This paper presents a review of a research and development (R&D) project being conducted for the U.S. Nuclear Regulatory Commission (NRC) to evaluate the feasibility of on-line monitoring techniques for instrument calibration reduction in nuclear power plants. The project has shown that the calibration drift of most process sensors can be identified on line by monitoring the DC output of the sensors while the plant is at normal operating conditions. This can help identify the sensors that must be calibrated during refueling outages and limit the calibration effort to those sensors that have shown a significant drift.

1. INTRODUCTION

This paper reports on the progress of an R&D project which has been underway since October 1991 to determine the validity and accuracy of on-line monitoring techniques for detection of calibration drift in the instrumentation channels of nuclear power plants. A feasibility study has been completed under a Phase I project and the results have been documented in NUREG/CR-5903 published in January 1993. A comprehensive Phase II project is underway and is due for completion in the fall of 1994.

The Phase II project includes both laboratory and in-plant validation work on typical nuclear plant sensors and signal conditioning equipment. The laboratory validation tests are being performed in a test loop in which a number of nuclear grade temperature and pressure sensors have been installed. They are connected to a Westinghouse Model 7300 instrumentation system of the type used in Pressurized Water Reactors (PWRs). The study includes the comparison of data from empirical and physical models developed as a part of this project with data measured in the test loop. More specifically, the loop is used to determine if simulated drift in the sensors can be effectively detected by on-line monitoring methods. It is also used to perform verification and validation of the on-line monitoring software packages being developed for the commercial aspects of this project. The commercial aspect of this project involves implementing drift monitoring techniques as a means of reducing the hands-on surveillance and calibration activities currently conducted in nuclear power plants.

The in-plant validation work is a joint effort with Duke Power Company and is being performed at the McGuire Nuclear Power Station where 170 process signals are continuously monitored. These signals include the primary coolant RTDs, core exit thermocouples, neutron flux detectors, the reactor

vessel level indicating system (RVLIS), and pressure, level and flow transmitters.

The DC data acquired during the most recent fuel cycle at the McGuire plant has been analyzed for calibration drift. Representative results are presented here and compared with the results of the hands-on calibration data, performed during the plant refueling outage.

2. TECHNICAL BACKGROUND FOR ON-LINE CALIBRATION MONITORING

Following the 1979 accident at the Three Mile Island Nuclear Power Station Unit 2, the NRC implemented a number of new requirements to insure that reactor operators are provided with accurate, timely, and reliable information about the status of the plant under normal and accident conditions. In response, the nuclear industry began upgrading the control rooms of the plants using state-of-the-art computer technology, color monitors, and digital and analog display equipment to provide the operators with qualitative and quantitative information on demand. The displays were designed and located in the control room according to human factor principles to make it easy for the operators to determine the status of the plant at a glance. An example of an important operator aid that incorporates these new developments is the Safety Parameter Display System (SPDS) which is used to assess the safety status of the reactor and critical components of the plant. This system uses the existing signals from some of the process instrumentation channels to display the present and past status of the plant in terms of color graphs and simple charts.

To insure that reliable signals are used in operator aids, the Electric Power Research Institute (EPRI) initiated research and development activities in the early 1980s in an area that is now known as "signal validation."[1] Signal validation techniques have been used previously in the aerospace and aviation industries for flight control and space vehicle applications.

Signal validation consists of a variety of signal processing techniques implemented in nuclear power plants to insure that sensor drift, response time degradation, bias, noise, and other sensor or system anomalies do not mislead the reactor operators. Signal validation depends on the redundancy of sensors and the physical relationships between process parameters to check the consistency of the measurements, predict the expected values of process variables, and detect, isolate, and characterize any significant anomaly in the instrument channel.

EPRI's efforts in the signal validation area have not only produced improvements in operator aids, but also have laid the foundation for the development of on-line methods for testing the calibration of instrument channels. In fact, the outgrowth of signal validation techniques for instrument calibration testing has overshadowed its application to SPDS and other operator aids. In addition to EPRI, a number of national and international research and development organizations, universities, national laboratories, and utilities have worked in the signal validation area. As a result, numerous techniques have been developed and documented under a variety of names. A few examples of these methods are listed below:

2.1 Like Signal Comparison (Cross Calibration) Method

The like signal comparison method uses intercomparisons between sensors that are measuring the same process parameter to determine a "best estimate" for the process. Also referred to as cross calibration or DC signal comparison, this method involves scanning the output of a number of redundant instrument channels and determining the deviation of each sensor's output from the average

of the redundant group (Figure 1). In cases where outliers are present, the method includes provisions for removal of the outliers from calculation of the best estimate of the process. Therefore, an accurate estimate of the process can be made without the influence of a sensor in need of calibration.

The like signal comparison method is normally used for analysis of steady-state (normal operating condition) data, but can also be used with transient data to provide a better estimate of the calibration of sensors over a large portion of their calibrated span. More specifically, the majority of data collected during a fuel cycle is for normal operating conditions which comprises a small portion of the total calibrated span of a sensor. Using an on-line monitoring system, data acquired during the fuel cycle will also include at least two transients where the entire span of the sensor is used. In most cases, these transients occur when the plant is heating up from cold shutdown conditions after a refueling outage or a reactor trip, and when it is proceeding toward cold shutdown at the end of a fuel cycle or during a reactor trip.

Like signal comparison methods are easy to incorporate in a calibration monitoring system, but cannot be used to isolate common-mode drift. For this reason, a newly calibrated sensor is included in the analysis or another method, such as analytical redundancy (described below) is used to provide an independent estimate of the process parameter.

2.2 Analytical Redundancy

Analytical redundancy, also referred to as diverse signal comparison, is used to identify common-mode calibration drift within redundant groups of sensors. As its name implies, analytical redundancy depends on theory to produce fictitious sensor outputs, providing additional redundancy to a group of measurements. To accomplish this, empirical or physical relationships between independent sensors are used in development of analytical models to calculate a process parameter. For example, steam generator level can be estimated based on measurements for feedwater flow, hot leg temperature, cold leg temperature, steam pressure, and steam flow. Analytical modeling results are then compared to values recorded from sensors within a redundant group as shown in Figure 2. Since the inputs to the analytical models are independent of the process parameter being predicted, common-mode drift is usually identified.

Analytical models are data driven, meaning that measurements from other independent sensors in different systems are used as inputs. One problem with this approach is that each of these input measurements have an uncertainty, and depending on the number of inputs used in the model, the accuracy of the model prediction can be compromised when the uncertainties from all the measurements are combined.

2.3 Parity Space

Similar to the like signal comparison method described above, parity space uses the redundancy of instrumentation channels to determine the consistency between a group of redundant signals. The common components of the signals are removed, and the remaining components are compared, two at a time. On the basis of the differences between the residual components in each pair, an inconsistency index is calculated and used for diagnostics. The inconsistency indices are also used as a weighting factor in averaging of the redundant signals to identify the best estimate of the process parameter. Signals with low inconsistency indices are weighted more than signals with high inconsistencies.

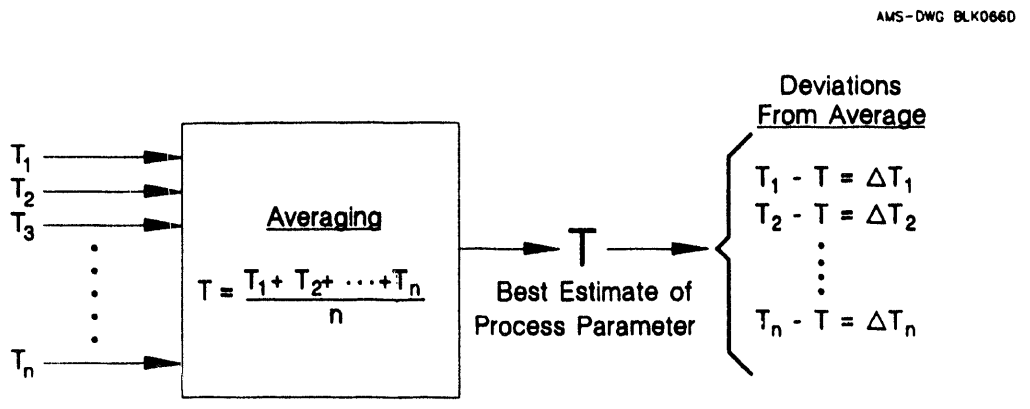


Figure 1. Illustration of Like Signal Comparison Method

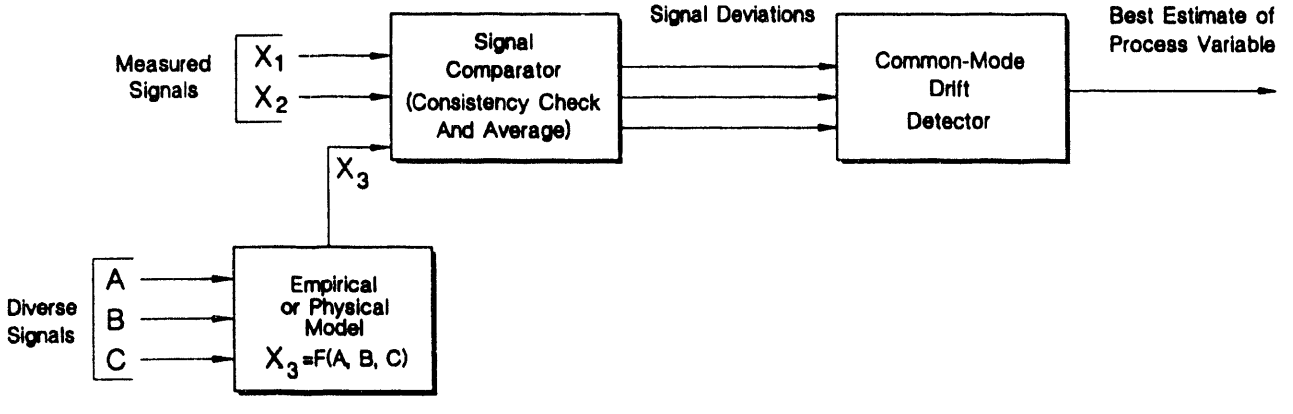


Figure 2. Principle of Analytical Redundancy For Common-mode Drift Detection

3. CURRENT CALIBRATION MONITORING PRACTICES

The nuclear power industry currently practices a very conservative approach with respect to performance testing of safety-related process instrumentation channels. In most plants, these channels are qualitatively checked three times a day, surveillance tested every month, and fully calibrated every refueling outage and whenever a component is replaced.

There are some variations in testing practices throughout the nuclear power industry and some differences in the terminologies used for the tests. For example, the monthly or quarterly surveillance tests are referred to as functional tests in some plants and are performed according to a different set of procedures and acceptance criteria than the surveillance tests. These variations make it difficult to provide a general picture of the nuclear industry's practices. Nevertheless, the following sections present an overview of the majority of current practices.

3.1 Daily Instrumentation Channel Checks

The safety-related instrument channels in most plants are qualitatively checked by the plant operators once every shift. The operators look at the indicators in the control room to insure that the redundant channels agree with one another within a certain tolerance. The resulting information is recorded in the plant's daily logs and any problem is reported to the maintenance staff for corrective action.

3.2 Surveillance Tests

Surveillance tests are usually performed on all safety-related instrument channels once every month while the plant is operating. The purpose of the surveillance tests is to either verify the trip setpoints or test the functionality of the instrument channels.

The surveillance tests are performed at the instrument racks and include all the components of the instrument channel except for the sensor. The sensor is located in the field and is not usually tested during plant operation except for in-situ response time testing as described in Reference 2. There is some concern as to whether or not it makes sense to test an instrument channel without the sensor. The sensor is the one component of the channel that is most susceptible to performance problems because it is located in the harsh environments of the plant as opposed to the rest of the channel which is located in a controlled environment. An on-line monitoring system as a substitute for the surveillance tests, as contemplated by the nuclear industry, has the advantage of testing the whole channel including the sensor. In addition, on-line monitoring is a completely passive approach in contrast to the surveillance tests which require physical interactions with the plant equipment.

3.3 Full-Channel Calibration

All safety-related instrument channels are fully calibrated during refueling outages. The calibration procedures are almost identical to the surveillance procedures except that they include the sensor. Furthermore, in executing calibration procedures, all instrument deviations are usually zeroed, if possible, whether or not a channel meets its acceptance criteria.

The full-channel calibration practice seems to be uniform throughout the nuclear industry except for what is done with the sensors. More specifically, the channels (excluding the sensors) are fully calibrated in all plants and all problems are usually resolved at every refueling outage. In addition,

all safety-related pressure and differential pressure transmitters (including level and flow transmitters) are calibrated in all plants and all problems are resolved at every refueling outage. Thermocouples and neutron detectors are rarely calibrated, except for comparing neutron channel outputs to heat balance data, and the practice is sporadic with respect to resistance temperature detectors (RTDs). A few plants periodically remove and recalibrate their RTDs, some plants periodically install new RTDs with fresh calibrations, many plants perform cross calibration at hot standby conditions, and other plants do not calibrate their RTDs at all. The number of RTDs that are calibrated and the frequency of the calibration are also sporadic across the nuclear power industry.

4. DEVELOPMENT OF ON-LINE MONITORING TECHNIQUES

The nuclear power industry has been interested in implementing on-line monitoring techniques to extend the frequency of calibration of process instrumentation channels in nuclear power plants. Although a significant amount of effort has been spent on development of on-line monitoring equipment and techniques in the last ten years, a systematic effort is yet to be completed on validation of these equipment and techniques. The R&D effort reported in this paper is the first systematic attempt in determining the feasibility and accuracy of on-line monitoring techniques for instrument calibration reduction in nuclear power plants.[3]

4.1 Laboratory Test Results

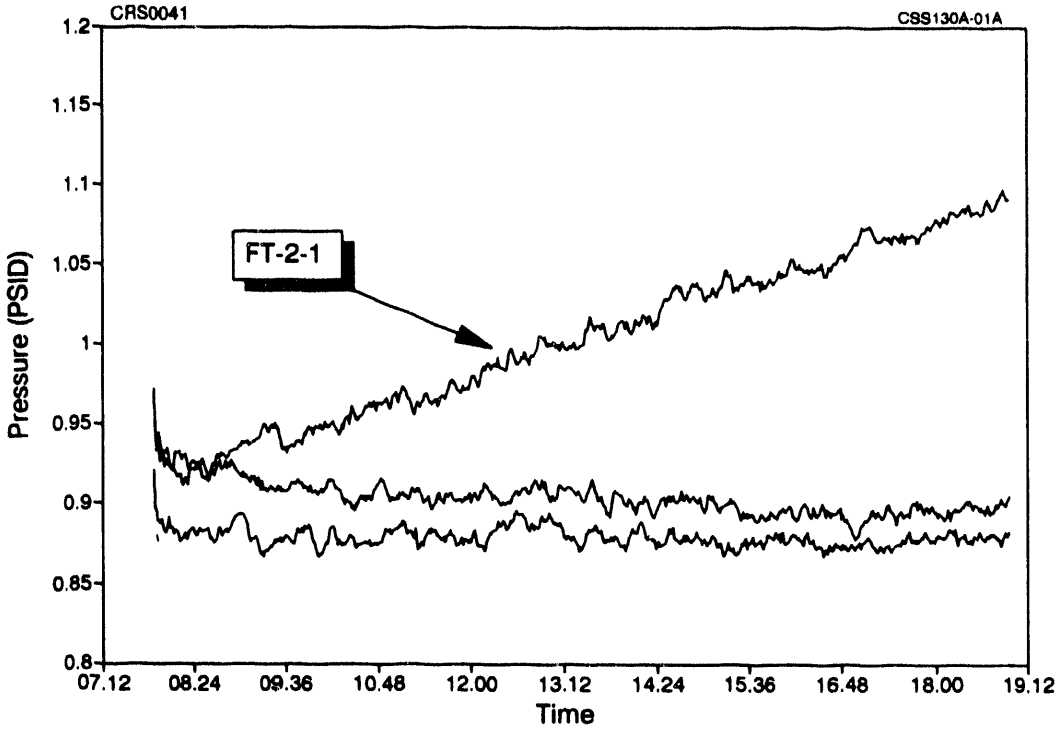
The goal of the R&D project reported in this paper has been to evaluate existing and new techniques for on-line verification of the calibration of sensors, and performing a systematic validation of those methods. To accomplish this, both laboratory and in-plant data is acquired and analyzed for calibration drift. The analysis results are then compared to drift data from hands-on calibrations to determine the validity of on-line drift monitoring techniques.

The laboratory testing has involved the use of a water test loop system with typical nuclear and commercial-grade temperature and pressure transmitters. Figure 3 illustrates on-line monitoring results for three redundant flow transmitters installed in this test loop. As seen in this figure, the calibration of one of the transmitters (FT-2-1) was intentionally drifted over a ten-hour period to show how the drift manifests itself in the deviation plot. The top portion of the figure represents the raw data for the transmitters, and the bottom portion gives the deviations (differences) between each sensor and the average of all three sensors. Note that the drift in the one transmitter causes all three signals to exhibit drift behavior in the deviation plot at the beginning of the data. Also note the sudden shift in the deviation traces at about five hours into the data. This occurs because FT-2-1 is excluded from the average when its deviation exceeds a preset criteria. Once this threshold is reached, the drifting transmitter is identified as an outlier and excluded from the best estimate calculation for the process.

Figure 4 illustrates the use of empirical modeling in detecting common-mode calibration drift. In this figure, two redundant pressure transmitters (FT-1-1 and FT-1-2) were intentionally drifted. The third transmitter within the group (FT-1-3) correctly represented the process condition. This is verified by the empirical model results which are also shown in Figure 4.

4.2 In-Plant Test Results From McGuire Nuclear Power Station

The in-plant validation of the on-line monitoring techniques is the most important aspect of this project. The in-plant work is being conducted at McGuire Nuclear Power Station Unit 2 where 170



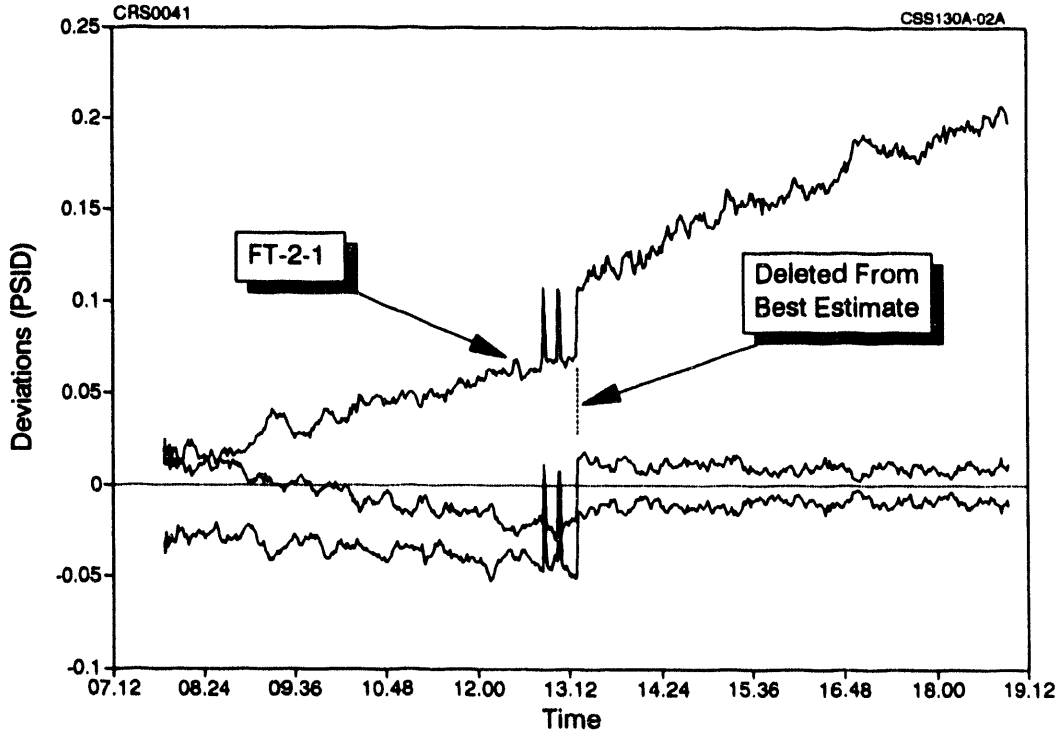


Figure 3. On-line Monitoring Results For Flow Transmitters Installed on the AMS Test Loop

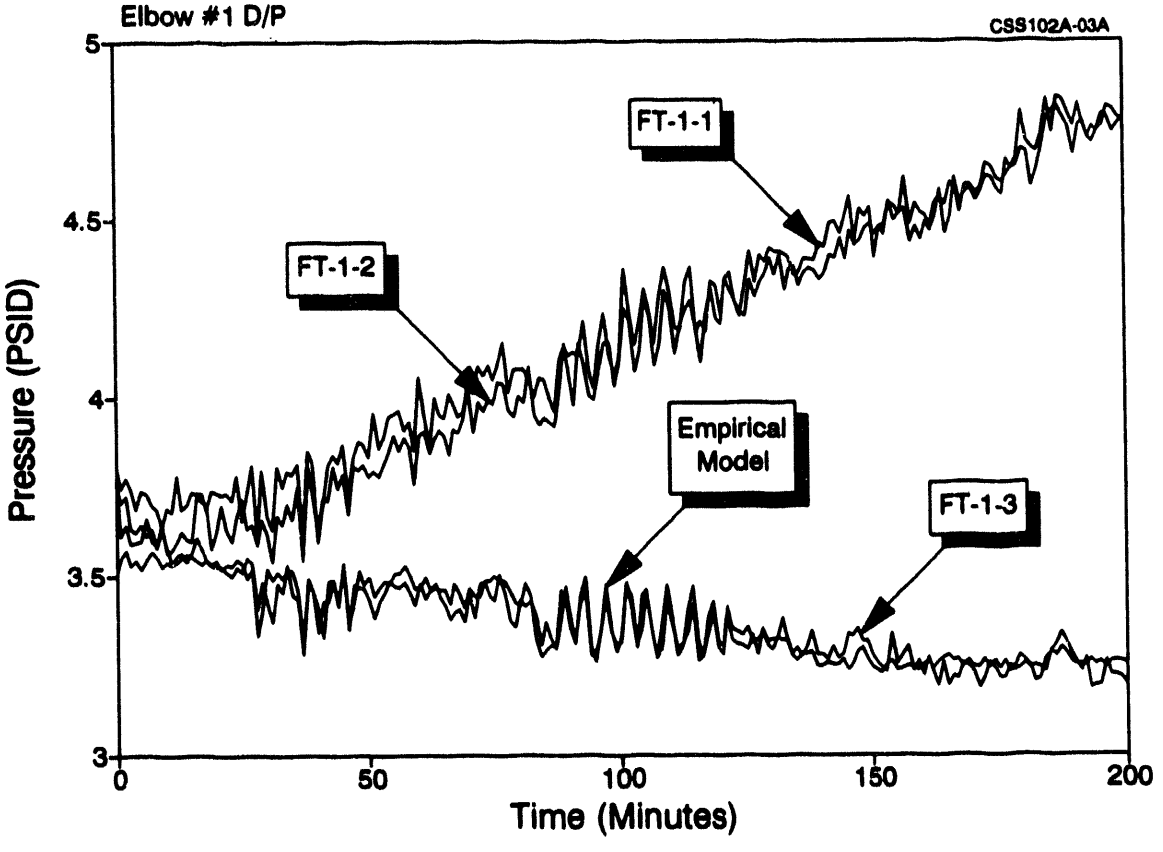


Figure 4. Illustration of Empirical Modeling For Detection of Common-mode Calibration Drift on the Test Loop

signals from the primary and secondary systems of the plant are being monitored continuously, including when the plant is at cold shutdown. The monitoring began in March 1992 at the beginning of the plant's eighth fuel cycle and will continue for two complete fuel cycles. A listing of the signals being monitored is given in Table 1 and includes both safety and non-safety related sensors. An attempt has been made to use all the redundant sensors from each service at McGuire, but in some cases only two out of a group of three or four sensors were available for monitoring.

A problem usually occurs during in-plant data acquisition when large DC fluctuations and spikes or transients appear at the output of sensors due to switching the sensors in and out of service for normal surveillance testing. To account for this, the data must be processed to remove these influences prior to performing the drift analysis. Figure 5 illustrates this step for a group of pressurizer level transmitters.

Figure 6 shows on-line monitoring results for steam generator level transmitters at the McGuire plant. As seen in this figure, one of the transmitters (CFLT6000) is identified with high deviations. On about July 30, 1992 this transmitter was recalibrated, but still exhibited relatively large deviations during the remainder of the fuel cycle and was eventually replaced by plant personnel. This data indicates that the on-line monitoring system has been successful in revealing the channel that has drifted.

Empirical modeling has been used on the McGuire data for detection of common-mode drift. Table 2 is a listing of the signals used in empirical models developed for McGuire. In this table, the models and their required inputs are shown. Figures 7 and 8 illustrate typical results for modeling of feedwater flow and steam generator level signals. In each of these figures, the signal outputs for the sensors are shown with the empirical model results.

As stated earlier, some of the data from the hands-on pressure transmitter calibrations have been compared to results from the on-line monitoring system (Figure 9). Such results attest to the validity of on-line monitoring analysis methods for detection of calibration drift.

5. CONCLUSION

A feasibility study was successfully completed on the validity of on-line monitoring techniques for remote testing of calibration of process instrumentation channels in nuclear power plants. This work involved research with temperature and pressure instrumentation in simulated reactor conditions in a laboratory, and in-plant work at the McGuire Nuclear Power Station Unit 2, a four loop PWR.

The effort described in this paper has successfully laid the foundation for an in-depth study that is underway to quantify the accuracy and reliability of the on-line techniques for instrument calibration reduction in nuclear power plants. Representative results from this work are summarized in this paper.

6. REFERENCES

1. C. H. Meijer and J. P. Pasquenza, "On-Line Power Plant Signal Validation Technique Utilizing Parity-Space Representation and Analytical Redundancy," Electric Power Research Institute, EPRI NP-2110, Palo Alto, California (1981).

Table 1

Listing of Signals Monitored at McGuire Unit 2

Item	Description of Signal	Number of Signals
1	Steam Flow	8
2	Steam Pressure	12
3	Steam Generator Level	20
4	Feedwater Flow	8
5	Auxiliary Feedwater Flow	4
6	Reactor Coolant Flow	12
7	Pressurizer Level	3
8	Pressurizer Pressure	4
9	Wide Range Reactor Coolant Pressure	2
10	Containment Pressure	3
11	Reactor Vessel Level Indicating System (RVLIS)	6
12	Turbine Impulse Pressure	2
13	Neutron Flux Detectors (NI Channels)	12
14	Narrow Range RTDs	16
15	Wide Range RTDs	8
16	Core Exit Thermocouples	40
17	Miscellaneous	10
Total Signals		**170**

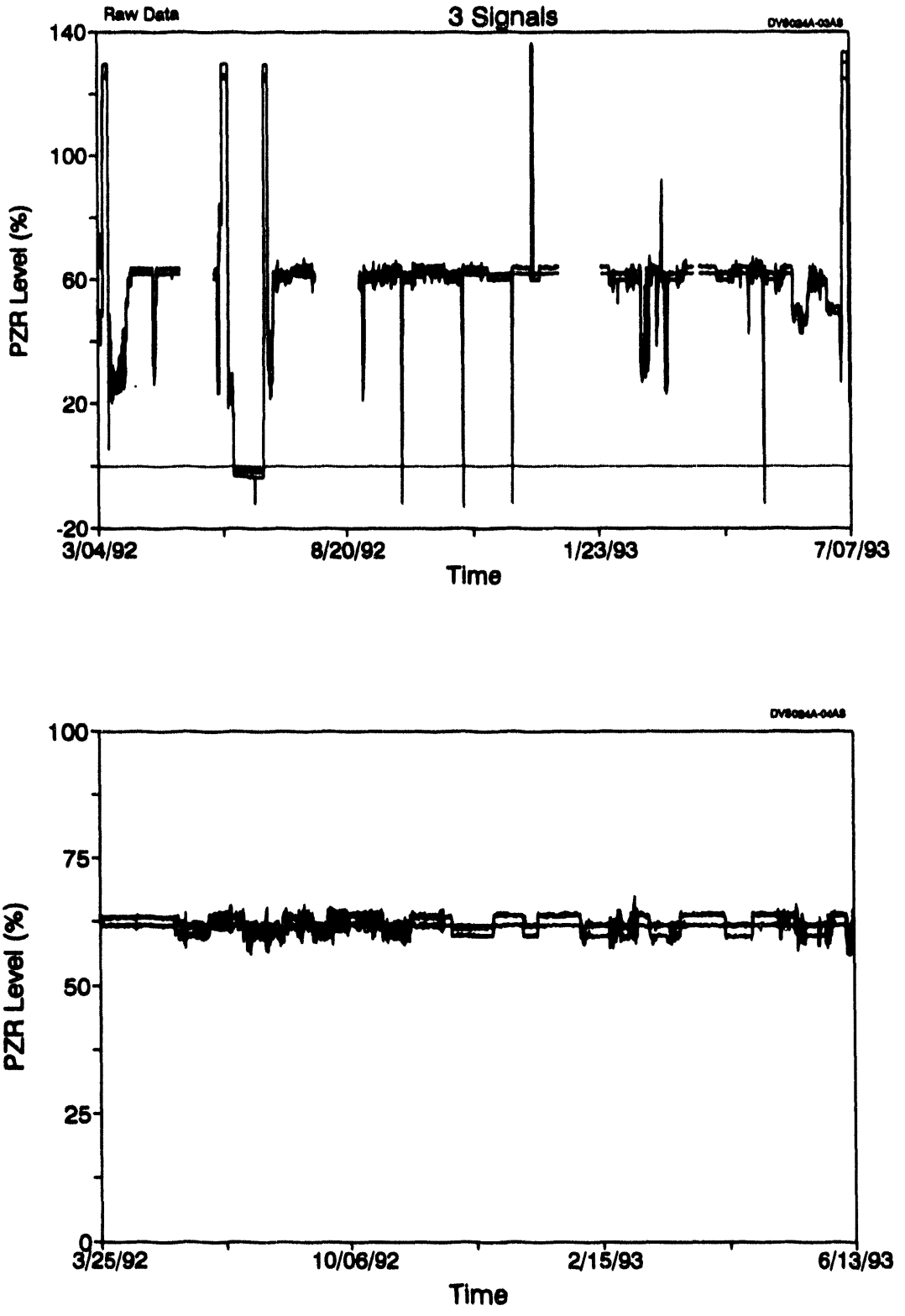


Figure 5. Pressurizer Level Signals Before and After Spike Removal

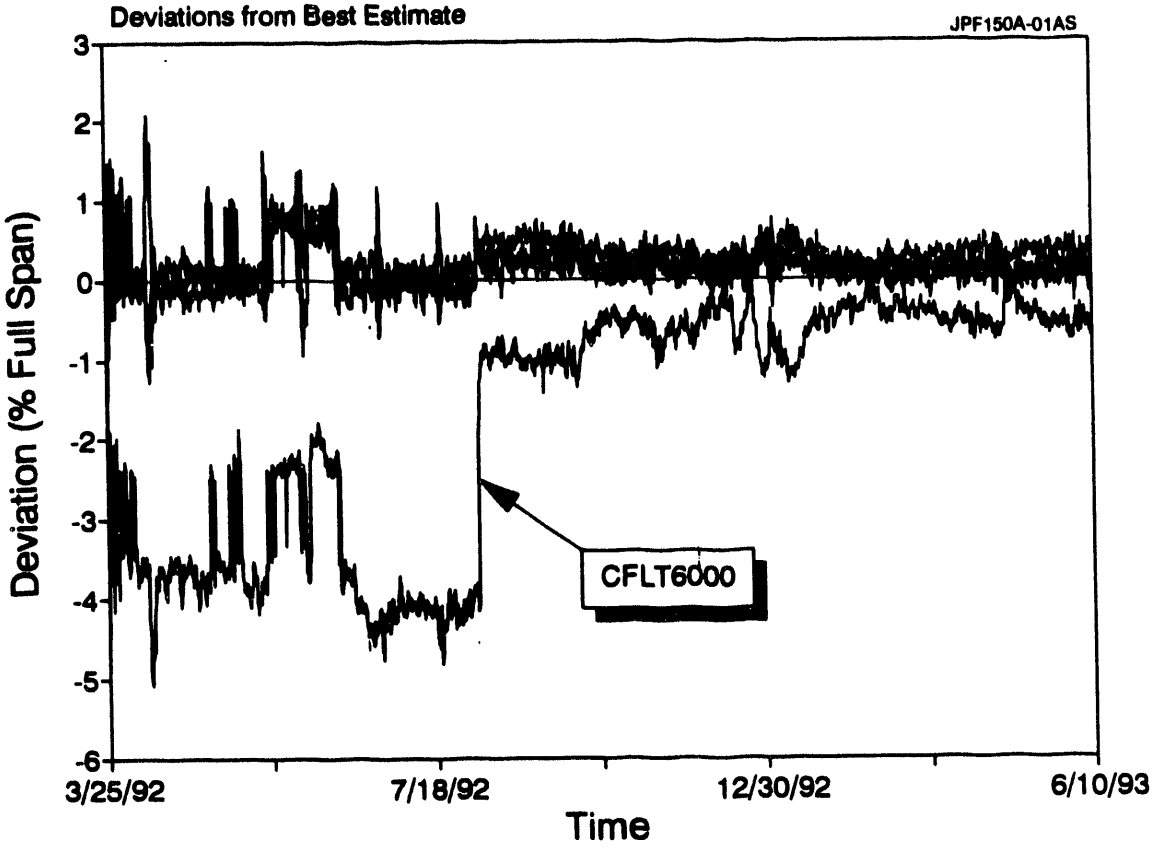


Figure 6. Illustration of On-Line Monitoring Results For Steam Generator Level Transmitters at McGuire

Table 2

Listing of Signals Used for Empirical Modeling of McGuire Data

JPF103A-01A

Model #	Process	# Sensors	Loop	Model Inputs: Feedwater Flow	Reactor Coolant Flow	Reactor Pressure	Power Level	Pressurizer Level	Pressurizer Pressure	Core Exit TCs (note 1)	THot RTDs (note 2)	TCold RTDs (note 2)	Steam Generator Level	Steam Flow	SG Steam Pressure
1	Feedwater Flow	2	A										x	x	x
2	Feedwater Flow	2	B										x	x	x
3	Feedwater Flow	2	C										x	x	x
4	Feedwater Flow	2	D										x	x	x
5	Reactor Coolant Flow	3	A								x			x	x
6	Reactor Coolant Flow	3	B								x			x	x
7	Reactor Coolant Flow	3	C								x			x	x
8	Reactor Coolant Flow	3	D								x			x	x
9	Reactor Pressure	2	N/A					x	x		x				
10	Power Level	4	N/A								x	x			
11	Pressurizer Level	3	N/A			x			x		x	x			
12	Pressurizer Pressure	4	N/A			x		x			x				
13	Core Exit TCs (note 1)	7	Quadrant 1								x	x			
14	Core Exit TCs (note 1)	9	Quadrant 2								x	x			
15	Core Exit TCs (note 1)	13	Quadrant 3								x	x			
16	Core Exit TCs (note 1)	8	Quadrant 4								x	x			
17	THot RTDs (note 2)	4	A							x		x			
18	THot RTDs (note 2)	4	B							x		x			
19	THot RTDs (note 2)	4	C							x		x			
20	THot RTDs (note 2)	4	D							x		x			
21	TCold RTDs (note 2)	2	A							x	x				
22	TCold RTDs (note 2)	2	B							x	x				
23	TCold RTDs (note 2)	2	C							x	x				
24	TCold RTDs (note 2)	2	D							x	x				
25	Steam Generator Level	5	A	x							x	x		x	x
26	Steam Generator Level	5	B	x							x	x		x	x
27	Steam Generator Level	5	C	x							x	x		x	x
28	Steam Generator Level	5	D	x							x	x		x	x
29	Steam Flow	2	A	x							x	x			x
30	Steam Flow	2	B	x							x	x			x
31	Steam Flow	2	C	x							x	x			x
32	Steam Flow	2	D	x							x	x			x
33	SG Steam Pressure	3	A	x	x						x	x		x	
34	SG Steam Pressure	3	B	x	x						x	x		x	
35	SG Steam Pressure	3	C	x	x						x	x		x	
36	SG Steam Pressure	3	D	x	x						x	x		x	
	Total	*134*													

Notes: 1. TC denotes Thermocouple

2. RTD denotes Resistance Temperature Detector

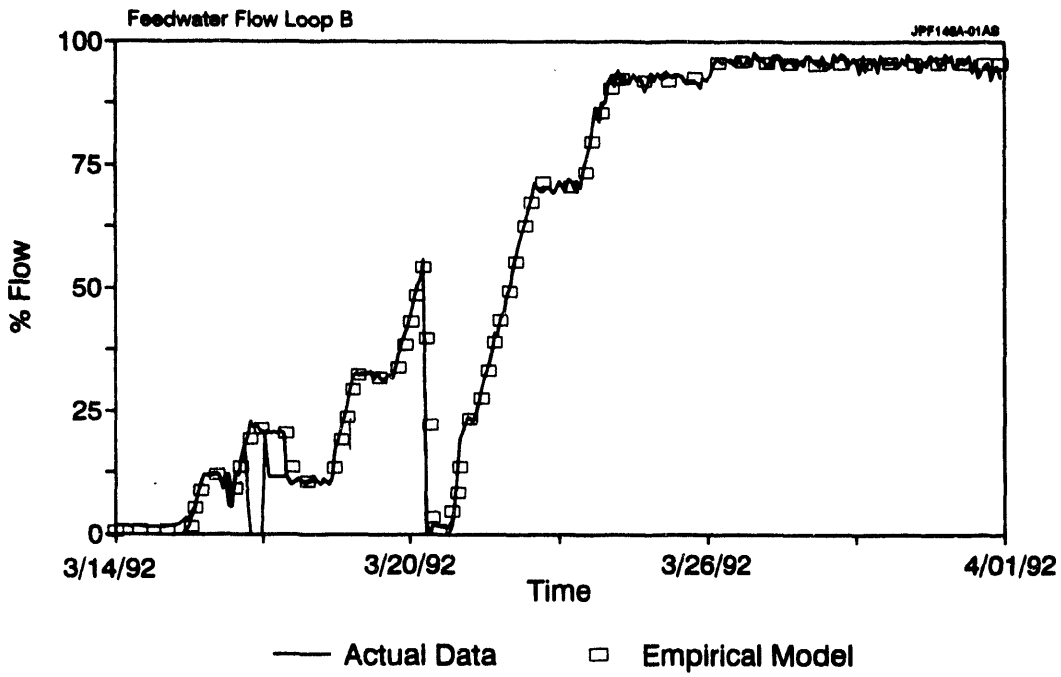


Figure 7. Empirical Modeling of Feedwater Flow at McGuire Unit 2

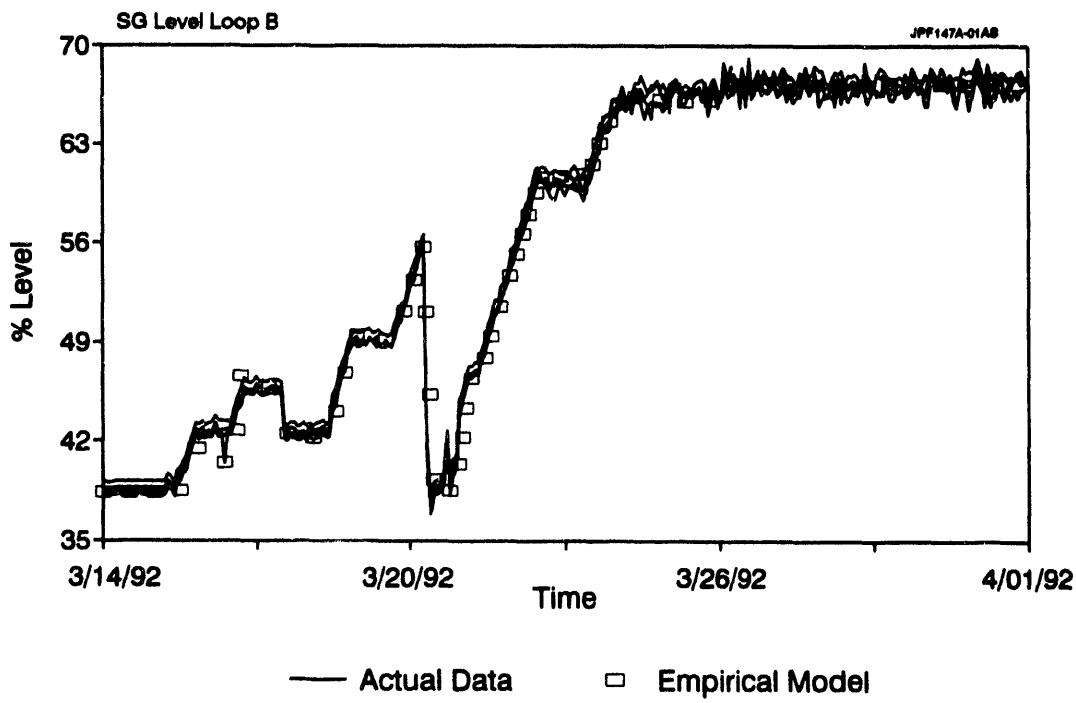


Figure 8. Empirical Modeling of Steam Generator Level at McGuire Unit 2

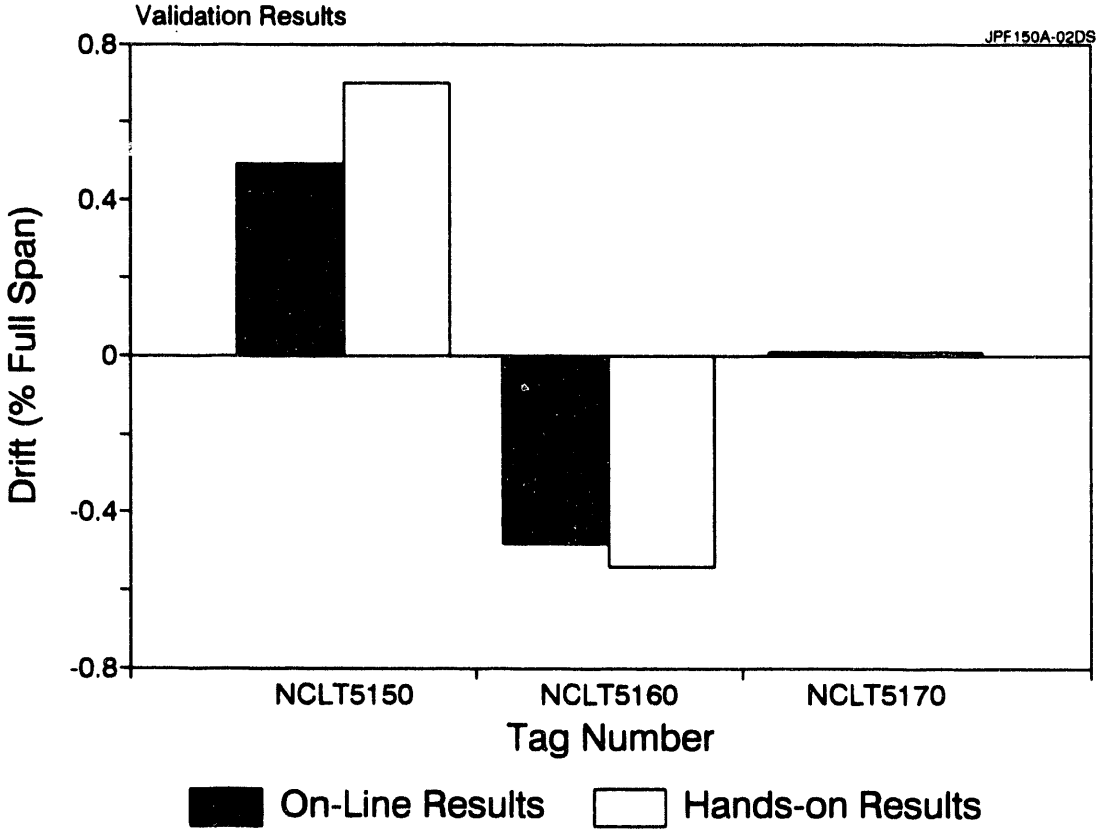


Figure 9. Comparison of Results from On-line Analysis of Calibration Drift and Hands-on Calibration of McGuire Unit 2 Pressurizer Level Transmitters

2. H. M. Hashemian, et. al., "Long Term Performance and Aging Characteristics of Nuclear Plant Pressure Transmitters," NRC Report Number NUREG/CR-5851, Nuclear Regulatory Commission, Washington, D.C. (1993).

3. H. M. Hashemian, et. al., "Validation of Smart Sensor Technologies for Instrument Calibration Reduction in Nuclear Power Plants," NRC Report Number NUREG/CR-5903, Nuclear Regulatory Commission, Washington, D.C. (1993).

ISSUES ARISING WITH THE APPLICATION OF OPTICAL FIBER TRANSMISSION IN CLASS 1E SYSTEMS IN NUCLEAR POWER PLANTS*

Kofi Korsah
Oak Ridge National Laboratory, P.O. Box 2008, Oak Ridge, Tennessee 37831-6010

Christina Antonescu
NRC Office of Nuclear Regulatory Research

ABSTRACT

The application of fiber optic links and networks in safety-critical systems in the next generation of nuclear power plants, as well as in some digital upgrades in present-day plants, will mean that these links must be highly reliable and able to withstand the effect of environmental stressors present at the installation location. This paper discusses the failure modes and age-related mechanisms of fiber optic transmission components and identifies environmental stressors that could adversely affect their reliability over the long term. Some of the standards that could be used in their qualification for safety-critical applications are also discussed briefly.

INTRODUCTION

In some countries, digital technology has been used in nuclear power plant control and protection systems for more than a decade. Here in the United States, several utilities are in the process of upgrading plants with digital instrumentation and control (I&C) systems. However, the extensive use of *microprocessor*-based and other "new" technologies such as multiplexing and fiber optic data transmission—as exemplified in proposed protection systems for light-water reactors of advanced design—has fostered renewed interest in the qualification and reliability of such technologies when applied to the safety systems of nuclear power plants.

---

*Research sponsored by the Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, under Interagency Agreement 1886-8179-8L and performed at Oak Ridge National Laboratory, managed by Martin Marietta Energy Systems, Inc., for the U.S. Department of Energy under contract DE-AC05-84OR21400.

As part of the Qualification of Advanced Instrumentation and Control Systems program being conducted at Oak Ridge National Laboratory under the sponsorship of the U.S. Nuclear Regulatory Commission,[1-3] we reviewed the open literature to identify failure modes and degradation mechanisms of optical fiber cables and transmission components. The purpose of this study was to identify how environmental stressors such as temperature, humidity, and radiation are likely to affect fiber optic transmission systems in nuclear power plant environments. The results of this and other studies regarding multiplexing equipment will be used to develop a framework for the qualification of "new" I&C systems for safety-critical applications in nuclear power plants.

OBJECTIVES OF THE ADVANCED I&C SYSTEMS QUALIFICATION PROGRAM

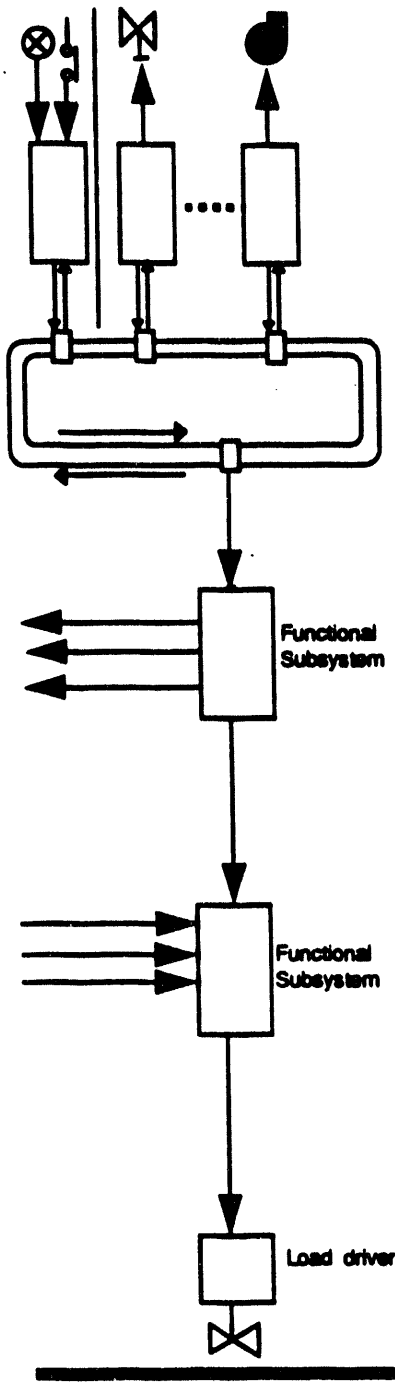
The Qualification of Advanced Instrumentation and Control Systems program is primarily an environmental qualification program and is closely related to the Nuclear Plant Aging Research program.[4] As such, its fundamental concern is that of *common cause* failure of "new" I&C equipment, with an emphasis on exposure to adverse conditions (e.g., elevated temperature, steam, and smoke). However, environmental qualification is part of the broader aspect of aging, which is further concerned with random failures and the use of improved maintenance and surveillance programs to predict or prevent increased age-related *random* and *common cause* failures.[5]

While the technologies for many I&C components (e.g., motors, generators, power supply systems, valves, etc.) are likely to remain essentially unchanged in the next generation of nuclear power plants, the age-related degradation mechanisms and failure modes of "new" I&C components such as optical fibers and multiplexing systems need to be assessed in order to develop a qualification methodology for their application in nuclear power plants. In simplified form, Fig. 1 shows what we have termed a generic template for an advanced light-water reactor (ALWR) protection system. The figure identifies some of the environmental issues involved with the application of such new technologies in safety-critical systems. These issues include the following:

1. Fiber optic transmitters, cables, and receivers are subject to failure modes and degradation mechanisms that are different from those of traditional (copper) cabling. New qualification methodologies for their application in nuclear power plants may therefore be needed.

2. The effect of age-related degradation on analog systems is different from that of their digital counterparts. The impact of such differences on digital subsystems needs to be ascertained. For example, how does lengthy exposure to levels of smoke and chemical contaminants that are below the detectable threshold affect the reliability of digital subsystems?

Other inputs to the development of a qualification methodology include (1) the identification and comparison of stressors affecting the different technologies in older plants, upgrades, and proposed plants; (2) identification of possible modifications to qualification standards for the nuclear industry to reflect the "new" technologies; and (3) a comparison of the functions performed in the older, analog subsystems to those performed in their microprocessor-based counterparts.



Simplified Design	Subsystem Identification and Location	Effect of Environmental Stressors
	Protection system sensors and actuators; located inside containment.	Aging mechanisms in electro-mechanical components and cables are likely to be the same as in existing plants.
	Remote Multiplexing Units (RMUs) use time division multiplexed techniques; located outside containment.	Aging mechanisms and failure modes of micro-electronic packages differ from those of analog components. Fiber optic transmitters, cables, and receivers are also subject to failure modes and degradation mechanisms different from conventional (copper) cabling. New qualification methodologies may be needed.
	Fiber optic, bidirectional, dual-redundant network using token passing techniques.	
	Comparison of measured variables to setpoints are performed here. Functions are performed by microprocessors under program control. Information is sent to other 3 divisions via fiber serial data links.	Microprocessor-based technology has failure modes different from those of analog technology. Need to ascertain how lengthy exposure to levels of smoke and chemical contaminants below the detectable threshold affect system reliability.
	Subsystem performs voting on all trip information from other three divisions to decide if a full reactor trip initiation is required. All functional subsystems for reactor trip (shown here) and engineered safety features (not shown) are in control room cabinets.	All subsystems are subject to the same environmental stressors since they are in the same location. Effects of both normal stressors (e.g., EMI/RFI) and abnormal stressors (elevated temperature, smoke, chemical contaminants) need to be ascertained.
	Output of load driver sends trip signal to pilot valve solenoids to initiate a scram.	

Fig. 1. Generic template of an ALWR protection system illustrating the impact of environmental stressors on new I&C technologies.

The approach we have taken to the development of a qualification methodology is depicted in Fig. 2. It should be noted that software reliability and verification and validation (V&V) issues are not a part of the hardware-oriented qualification program. However, as shown in Fig. 1, both hardware and software data are needed to form the technical bases for the development of acceptance criteria and guidelines for the application of microprocessor-based and "new" I&C equipment in nuclear power plants.

Some of the inputs to the qualification methodology have been discussed in previous papers.[1-3] The emphasis in this present paper is on a discussion of the failure modes and age-related mechanisms of fiber optic transmission components.

OPTICAL FIBER TRANSMISSION SYSTEMS

Proposed ALWR systems are intending to make extensive use of fiber optic transmission in the communication interfaces between safety-critical systems and control room, in the interfaces between protection and engineered safety-feature systems, and also in the distributed control systems. In some cases, communication among the protection divisions necessary for voting will utilize fiber optic serial data links. Fiber optic transmission technology has also been used in the control and communication (non Class 1E) upgrades of some nuclear power plants. We attempted to address qualification issues associated with their application in Class 1E systems in power plants by first identifying failure modes and degradation mechanisms in present-day optical fiber transmission components.

An optical fiber transmission system consists of three major subsystems:

1. E-to-O conversion of electrical signals to optical signals, typically by means of a light-emitting diode (LED) or a semiconductor laser diode.

2. Light transmission by fiber optic cables, typically consisting of glass or plastic fibers having suitable cladding material, a buffer layer (either acrylic or polymide), a strength member (such as Kevlar or steel), and an outer jacket.

3. O-to-E conversion of the optical signals to electrical signals, typically by means of a PIN (Positive-Intrinsic-Negative) photodetector or an avalanche photodetector (APD).

A number of advantages associated with the use of optical fiber transmission, such as the immunity of the fibers to electromagnetic interference/radio frequency interference (EMI/RFI), have been significant motivating factors in their application to the nuclear power plant environment. However, the transmitter and receiver components are quite sensitive to EMI. Also, the cable itself, as well as the transmitter and receiver, is subject to age-related degradation and failure modes that are different from those of conventional copper transmission systems. The most significant of these are listed in Tables 1 to 3. In the tables, failure is defined as a 50% reduction in optical output (LEDs) and a 50% increase in threshold current (laser solid-state devices).[6]

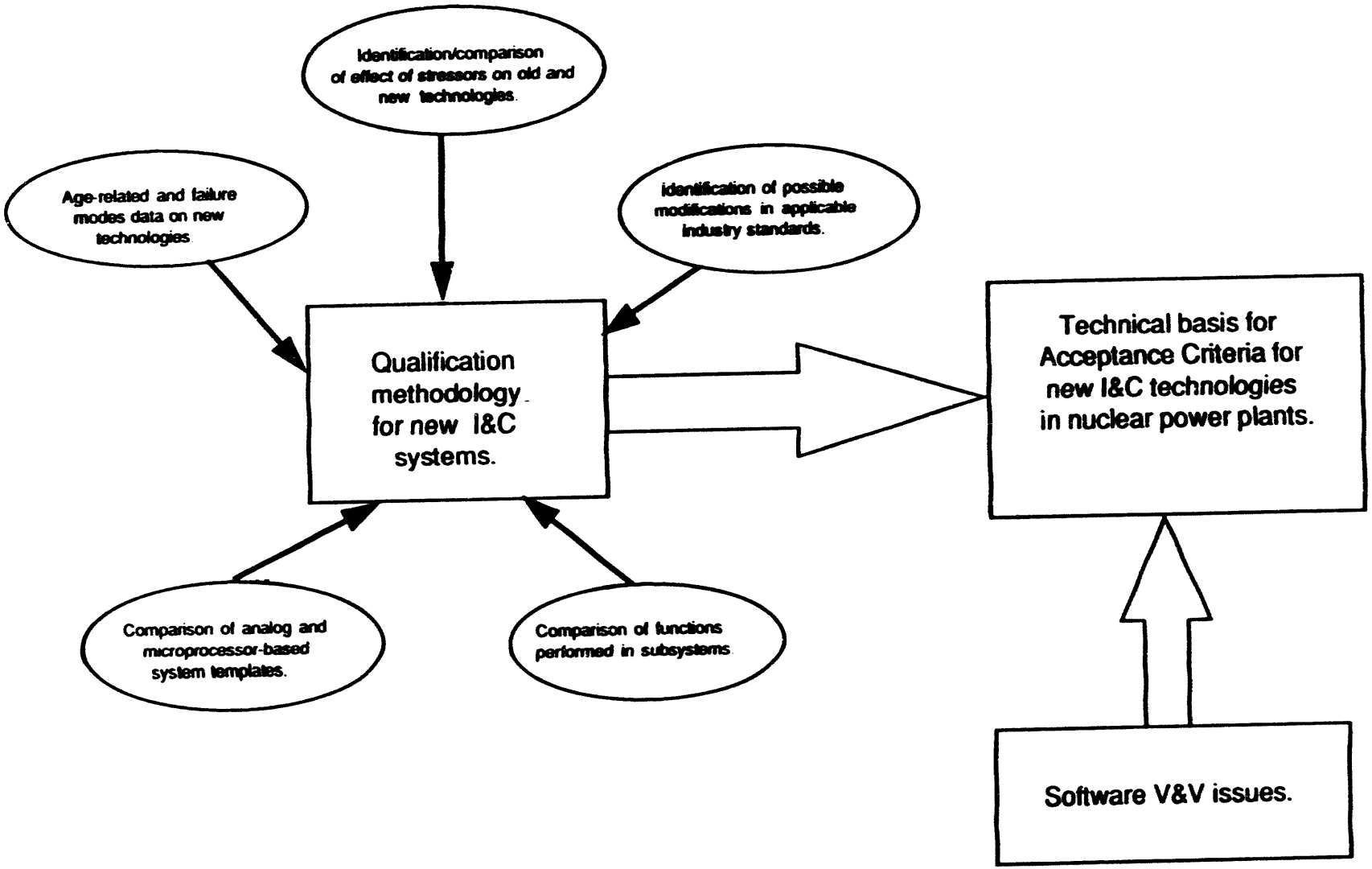


Fig. 2. Developing acceptance criteria for application of "new" I&C technologies to safety-critical systems in nuclear power plants.

Optical Transmitters

As shown in Table 1, the two most frequently used optical sources are LEDs and semiconductor laser diodes. LEDs have the advantages of low cost, high reliability, and good linearity, while laser diodes offer high output power level, efficiency, bit-rate-modulation capability, and very good mode stability of the emitted light.[7] However, both component types are subject to degradation due to formation of dark line defects (DLDs) and dark spot defects (DSDs), which are caused by impurities and crystal lattice defects in the material. These defects give rise to nonradiative recombination in the active region of the device. Other degradation mechanisms in the transmitter include photo-oxidation of facets due to extended high-threshold currents and contact degradation due to temperature stresses across contacting interfaces when ambient operating temperature rises.

With regard to radiation, tests performed with gamma rays[8] on InGaAsP LEDs operating at 1300 nm showed no significant degradation of parameters up to a total dose of 10^5 Gy. The output power decreased by 5% with an irradiation dose of 10^6 Gy. It was estimated that the output power would decrease to 50% of the initial value at a total dose of 2×10^7 Gy.

A study of the effect of neutron irradiation on LEDs[7,9] fabricated from strained-layer superlattice structures in the GaAs/GaAsP configuration showed no significant light output degradation below a neutron fluence of 3×10^{14}.

Optical Fibers

Failure mechanisims of optical fibers are summarized in Table 2. Chemical impurities introduced during the fiber drawing process constitute a major source of changes to optical and physical properties. Factors that affect signal attenuation include hydrogen migration caused by diffusion into interstitial sites in the fiber molecular structure, chemical reaction of hydrogen with the glass constituents to form OH groups, formation of microcracks due to bending stresses, and optical losses due to the formation of color centers in the fiber core. (Color centers are formed primarily by the trapping of radiolytic electrons and holes at defect sites in the fiber when it is exposed to ionizing radiation).

Pure silica-core fibers show the least radiation-induced damage in both mixed neutron/gamma and gamma-only environments. Some tests have shown that such fibers exhibit no performance change following doses of as much as 3800 Gy.[10] On the other hand, some fibers fluoresce enough under irradiation to obscure very low strength signals. Pure silica-core fibers appear to be the most suitable for use in nuclear power plants.

Environmental variables such as high temperature and humidity can result in aging and increased failure rates for certain fiber optic cables. In such harsh environments (e.g., inside containment, certain areas outside containment, and during accidents), the fiber coating material is of primary importance. In the presence of high temperature and humidity, some degree of hydrolytic degradation in fiber coating will occur. If the coating is not designed to take this into account, its properties may degrade severely, and the coating may discolor or lose its adhesion to the glass.[11] Aging tests have shown that, with suitable coatings, present-day fibers can withstand at least 20 years of exposure to an extreme outside-plant climate.[11]

Optical Receivers

Failure mechanisms of optical receivers and connectors are summarized in Table 3. The predominant failure mode in optical receivers is an increase in dark current due to elevated ambient temperature and possible electrical shorts due to electrochemical oxidation when the system is operated above a relative humidity of 85%. With regard to radiation, optical receivers are sensitive to ionizing radiation as well as to optical radiation. The same physical processes that make the detector sensitive to radiation are also responsible for the detector's responsitivity to ionizing radiation. However, ionizing (gamma) radiation interaction is a bulk effect, meaning that charge carriers (electron-hole pairs) are generated throughout the bulk of the semiconductor material.

Table 1. Failure mechanisms of optical sources

Subsystem	Possible components	Mode of failure	Cause	Prevention methods
Transmitter	Light-emitting diodes (LEDs): (InGaAsP/InP; AlGaAs/GaAs; AlGaAs/Si).	Dark line defects; Dark spot defects.	Nonradiative recombination caused by impurities and crystal lattice defects in the material.	1. Choice of material 2. Fabrication and wire bonding methods 3. Quality control
	Solid state laser devices: (AlGaAs/GaAs; InGaAsP/InP).	Increase in threshold current. Decrease in laser power at a given bias level.	Increase in terminal current and temperature result in rise in leakage current in active region of device. Increase in leakage current contributes to formation of dark spot defects.	Fabrication methods: Application of a passivation layer helps reduce surface contamination and in-migration of atoms from contact deterioration (dark spot defects).
		Laser wear-out.	1. Contact degradation due to temperature stresses across contacting interface when ambient operating temperature rises. Results in an increase in threshold current.	Decrease operating temperature and current density. Improve contact material compatibility.
			2. Photo-oxidation on facets due to extended high-threshold currents. Reduces reflectivity. Occurs most frequently when device is operated in high humidity/moist environments.	Fabrication techniques: Typically, a thin coating of silicon dioxide (SiO_2), aluminum oxide (Al_2O_3), or silicon nitride (Si_3N_4) is applied.
			3. Lattice defects in material result in the formation of dark line defects over a large surface area of active device. Eventually causes optical output power to decrease.	1. Choice of material: (Select one with low lattice defects). 2. Quality control: (Helps in testing for quality materials).

Table 2. Failure mechanisms of optical fibers

Subsystem	Possible components	Mode of failure	Cause	Prevention methods
Fiber optic cable	**Fiber material:** Silica or plastic.	Signal attenuation in fiber.	Hydrogen migration into fiber due to:	Design cables with materials that do not generate hydrogen. (See note 1.)
	Secondary buffer: polyester elastometer.		1. diffusion into interstitial sites in the silica molecular structure;	
	Strength member: polymer (Kevlar), steel, or carbon fiber.		2. chemical reaction of hydrogen with the glass constituents to form OH groups.	
	Outer jacket: Plastic sheath, flame retardant chlorinated polyethylene.		Formation of microcracks due to:	
			1. bending radius of the cable;	Bending and handling radius must be specified and inspected during installations.
			2. cable handling during installation;	Use coating materials that can prevent/reduce shrinking, cracking, or swelling.
			3. differences in the thermal expansion coefficients of coating materials and fiber.	Good cable handling practices.
			Optical losses due to ionization in the fiber from:	Design to be radiation-hardened. (See note 2.)
			1. gamma radiation;	
			2. neutron radiation.	
			Fiber may become temporarily opaque or may experience permanent discoloration.	
		Fiber fracture.	Stress corrosion or fatigue due to microcracks.	Residual tension should be less than 33% of the rated proof-tested tensile strength.

[1]The hydrogen may be generated from degradation of polymers in the cable. It can also be generated by galvanic action between two dissimilar metals or by the action of sea water on cable sheaths. However, these sources are negligible in control room environments in power plants.

[2]In noncontainment environments, optical loss due to radiation damage is negligible. Pure silica-core fibers are much more radiation resistant than plastic fibers or phosphorus-doped fibers.

Table 3. Failure mechanisms of optical receivers and connectors

Subsystem	Possible components	Mode of failure	Cause	Prevention methods
Receivers	**Technology:** PIN (Positive-Intrinsic-Negative) photodetector Avalanche photodetector (APD) **Material:** PIN: silicon, InGaAs, germanium APD: silicon, germanium	Increase in dark current (reverse current in the absence of incident radiation).	1. Thermally generated charge carriers (PIN photodiodes). 2. Thermal deterioration of the metal contacts (APD).	**Fabrication techniques:** Thin layer of In or InGaAs grown onto active region. **System design techniques:** 1. Choose detector with inherently low dark current. 2. Operate device at low environmental temperature.
		Possible electrical short circuits when device is operated above a relative humidity of 85%.	Electrochemical oxidation.	Use hermetically sealed devices if they are going to be operated in such environments.
Connectors		Signal attenuation or complete signal loss.	Insertion loss due to angular misalignment, core misalignment, end separation, reflections, end preparation quality. Aging of index-matching fluid due to: 1. changes in viscosity due to temperature stresses; 2. maintenance handling (mating/unmating over time).	Various connector design techniques are used to reduce mating losses. In applying index-matching fluid, care should be taken to avoid dust and dirt.

On the other hand, photons generate carriers only in the small, active region. Therefore, the contribution of ionizing radiation to total photodiode current can be reduced by

1. reducing the volume of the optically nonactive region and
2. reducing the volume of the active region while maintaining a high optical response (i.e., using a material with a large absorption coefficient at the wavelength of the optical radiation).

Research data[7,9,12] show that double heterostructure AlGaAs/GaAs devices are far superior to silicon radiation-hardened photodiodes. In one study,[9] GaAs devices were able to operate reliably with dose rates up to 10^6 Gy/s, which is several orders of magnitude above the tolerance of silicon PIN photodiodes. Data on neutron irradiation effects on photodiodes show that the leakage current increases by about a factor of 10 in AlGaAs/GaAs photodiodes and a factor of 10^3 in silicon PIN photodiodes after exposure to a neutron fluence of 7×10^{14} n/cm^2. Degradation of optical responsitivity at this level of neutron fluence is negligible for AlGaAs/GaAs photodiodes, while silicon devices may experience as much as 60% reduction in responsitivity compared to preirradiation levels.

This brief review has shown that quite a number of age-related degradation and potential failure mechanisms are associated with fiber optic transmission components. Some of these potential failures are exacerbated by environmental stressors such as temperature, humidity, and radiation. Thus the environments in which the transmission subsystems will be used are significant. ALWR protection system cabinets will typically be located in a control room environment, where radiation, temperature, and humidity levels are much more benign than in containment. For example, integral gamma dose levels in a pressurized-water reactor containment over a 60-year period may be on the order of 3×10^6 rads, while the integral gamma dose levels in the control room over the same period are estimated to be less than 10^3 rads.[2,3] Average temperature in containment may be 120°F, while an estimated average value for the control room is 65°F. Tests have shown that optical signal power loss under either of these conditions is negligible. Therefore, it appears that given good design choices and installation procedures, fiber optic components are likely to perform reliably in their proposed operating environments.

NETWORK REQUIREMENTS

The simplified reactor trip system (one division shown) in Fig. 1 is typical of proposed ALWR designs. Protection channel process variables are acquired by a multiplexing unit, which then converts the input signal to a digital format for multiplexing. The digital multiplexed signal is then converted into an optical signal and transmitted further to various locations via the fiber optic network. Discussions with cognizant industry personnel suggest that the network is a dual redundant, FDDI (fiber distributed data interface) network. (This network is an outgrowth of the IEEE 802.5 Token Ring Network.)

The token ring access method used should make the ring deterministic and predictable. The choice of optical fiber transmission eliminates the network's potential susceptibility to radiated noise from high-voltage conductors, high-frequency motor control drives, and transient pulses created by switching devices. However, the "weak links" are still the optical transmitting and receiving components, and their reliability over the long term—as well as the susceptibility of the multiplexing equipment itself to EMI/RFI—needs to be addressed. Also, one of the requirements of a reliable communication system is that it must be able to isolate any faulty element in order that the overall system reliability is not compromised. Such isolation requires an optical bypass,

which is typically accomplished by an optical switch connected between the node and the fiber optic ring. Many commercial bypass elements are of the moving mirror type, whose reliability degrades considerably in high-vibration environments. On the other hand, solid-state bypass switches (such as lithium niobate) have high losses when used in multimode fiber configurations.[13] Reliability issues dictate that such details be considered in the choice of optical fiber networks for safety-critical applications in nuclear power plants.

CONCLUSIONS

In this paper, a review of failure modes and age-related degradation mechanisms in fiber optic transmission components has been presented. The potential for failures in some cases (e.g., dark line defects, threshold currents) can be reduced considerably during the fabrication process. Others (e.g., cable bending, shrinking and swelling) can be prevented by appropriate choice of materials during the fabrication process, proper design control, and control of the environment.

While environmental conditions can adversely affect optical fiber systems, ALWR protection system cabinets will typically be located in a control room environment, where radiation, temperature, and humidity levels are considerably less harsh than in containment; hence the adverse effect of these stressors on the transmission system is likely to be minimal. However, for safety-critical applications, the overall qualification of the optical fiber system needs to be addressed. For example, the ability of removable connector terminals and cable assemblies to withstand stresses similar to those which may be expected by inserting and removing terminals during maintenance should be ascertained. Current regulatory guides do not address qualification of fiber optic systems. A number of industry standards, such as EIA-455-17A, "Maintenance Aging of Fiber Optic Connectors and Terminated Cable Assemblies," and ANSI/EIA-455-88, "Fiber Optic Cable Bend Test," could perhaps be endorsed by appropriate regulatory guides for application to nuclear power plants.

REFERENCES

1. Kofi Korsah, R. Kisner, R. T. Wood, and C. Antonescu, "Environmental Qualification and Functional Issues for Microprocessor-Based Reactor Protection Systems," *Transactions of the 20th Water Reactor Safety Information Meeting*, NUREG/CP-0125, Bethesda, MD, October 21–23, 1992, p. 11-5.

2. Kori Korsah and Christina Antonescu, "A Survey of Issues Associated with Microprocessor-Based Reactor Protection Systems Hardware," *Second International Conference on Nuclear Engineering (ICONE-2)*, March 21–24, 1993.

3. Kofi Korsah and Christina Antonescu, "Qualification Issues Associated with the Use of Advanced Instrumentation and Control Hardware in Nuclear power Plants," IAEA Specialists meeting on Experience in Aging, Maintenance and Modernization of Instrumentation and Control Systems for Improving Nuclear Power Plant Availability, Rockville, MD, 1993.

4. *Nuclear Plant Aging Research (NPAR) Program Plan*, NUREG-1144, Rev. 1, U.S. Nuclear Regulatory Commission, September 1987.

5. M. J. Jacobus, *Aging of Cables, Connections, and Electrical Penetration Assemblies Used in Nuclear Power Plants*, NUREG/CR-5461, Sandia National Laboratory, July 1990.

6. R. A. Hyle and Griffiss, "Fiber Optics—Failure Modes and Mechanisms," pp. 379–388 in *Proceedings of the Annual Reliability and Maintainability Symposium*, 1992.

7. Branko Leskovar, "Radiation Effects on Optical Data Transmission Systems," *IEEE Transactions on Nuclear Science*, 36(1) (February 1989).

8. H. Okuda et. al., "Radiation Effects on InGaAsP/InP DH LEDs (λ_p = 1.3 μm)," *46th Meeting of the Japan Society of Applied Physics*, 3a-N-1, p. 209, 1985.

9. C. E. Barnes, "The Effects of Radiation on Optoelectronic Devices," *Proceedings of SPIE—Fiber Optics in Adverse Environments III*, Vol. 721, pp. 18–25, 1986.

10. *Optical Fibers in Radiation Environments*, EPRI-TR-100367, Electric Power Research Institute, 1992.

11. *Lightguide Digest*, Issue No. 1, AT&T Network Systems, Morristown, NJ, 1992.

12. B. H. Rose and C. E. Barnes, "Proton Damage Effects on Light-Emitting Diodes," *J. Appl. Phys.*, 53(3), 1772–1780, 1982.

13. Richard M. Bailly, "Survivable Fiber Optic Networks for Military Applications," *Vitro Technical Journal*, 8(1), 70–78 (Winter 1990).

A DYNAMIC FAIL-SAFE APPROACH TO THE DESIGN OF COMPUTER-BASED SAFETY SYSTEMS

I C Smith
AEA Technology, Winfrith, Dorchester, Dorset, DT2 8DH, UK

M Miller
Duke Power Company, Oconee Division, PO Box 219, Seneca, S. Carolina 29679, USA

ABSTRACT

For over 30 years AEA Technology has carried out research and development in the field of nuclear instrumentation and protection systems. Throughout the course of this extensive period of research and development the dominant theme has been the achievement of fully fail-safe designs. These are defined as designs in which the failure of any single component will result in the unit output reverting to a demand for trip action status.

At an early stage it was recognised that the use of dynamic rather than static logic could ease the difficulties inherent in achieving a fail-safe design. The first dynamic logic systems coupled logic elements magnetically. The paper outlines the evolution from these early concepts of a dynamic fail-safe approach to the design of computer-based safety systems. Details are given of collaboration between AEA Technology and Duke Power Company to mount an ISAT™ demonstration at Duke's Oconee Nuclear Power Station.

1. INTRODUCTION

For over 30 years AEA Technology has carried out research and development in the UK in the field of nuclear instrumentation and protection systems. Throughout the course of this extensive period of research and development the dominant theme has been the achievement of fully fail-safe designs. These are defined as designs in which the failure of any single component within a unit will result in the unit output reverting to a demand for trip action status.

™ ISAT is a registered trademark of AEA Technology

At an early stage it was recognised that the use of dynamic rather than static logic could ease the difficulties inherent in achieving a fail-safe design protection system. A dynamic logic system is one in which an output signal alternating between logic 1 and logic 0 is a healthy state and a static output either logic 1 or logic 0 is a tripped state. The alternating state is a higher energy system than the static one. Since faults tend to move the system to a lower energy state the use of dynamic logic is preferred when designing fail-safe systems.

This paper outlines the evolution of a dynamic fail-safe approach to the design of computer-based safety systems.

2. HARDWARE-BASED SYSTEMS

A system of dynamic trip logic which has been in use on nuclear power plants in the UK for over two decades uses coupled magnetic cores. Trip logic systems, which combine the binary outputs of a number of trip parameter bistable instruments using a logic OR function, are known in the UK as guardlines.

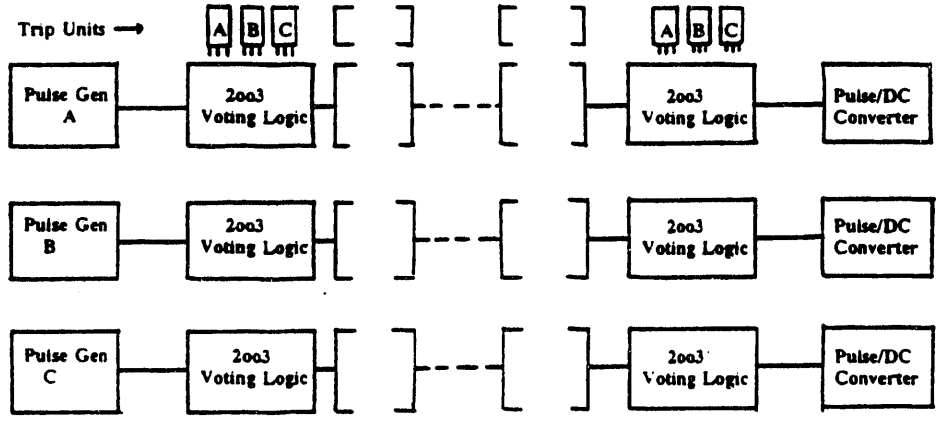


Figure 1. Typical Guardline Trip Logic System

The guardline system, which uses coupled magnetic cores, has a pulse generator prior to the first logic unit. Each logic unit functions as a 2 out of 3 voter. A sequence of set and reset pulses are generated by the pulse generator. The set and reset pulses passing through the set and reset windings cause the magnetic flux in the specially fabricated ferrite core to switch direction.

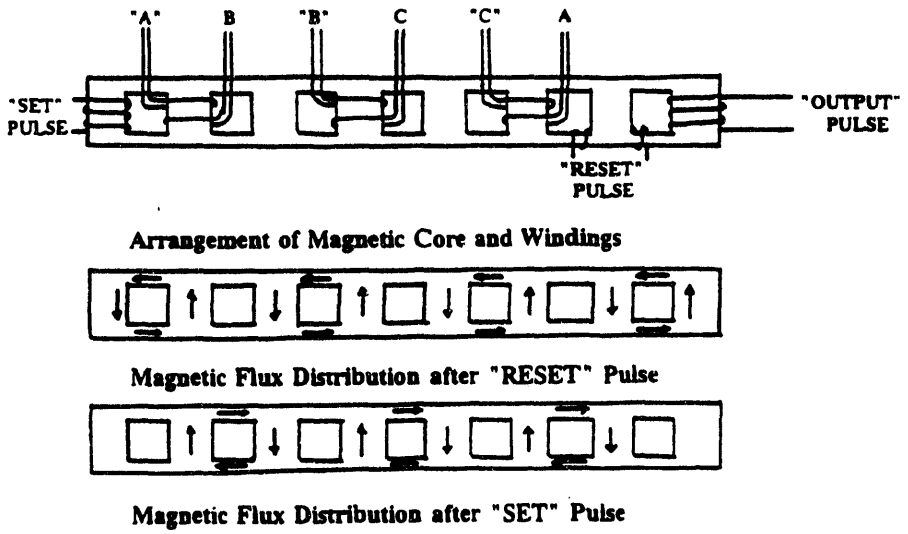


Figure 2. Typical Magnetic Logic Unit

The successful setting and resetting of the magnetic circuits in the first logic unit generates an output pulse which passes onto the second logic unit to provide a reset pulse for that unit. An output pulse will only be generated if currents are present in at least two of the current outputs of the trip instruments. If the output current is lost from two or three of the trip instruments feeding the coils the magnetic circuit is broken and so an output pulse will not be generated. Thus pulses will continue to be propagated along the guardline if, and only if, for each trip parameter at least two trip instruments are supplying a healthy excitation current to their respective windings in the ferrite core logic unit. At the end of the guardline the emerging pulses generate an alternating output which is passed through a pulse to d.c. converter to produce an excitation current which holds in reactor control rod breakers. If, for any trip parameter, two or more trip instruments fail to generate an output excitation current then the pulses will not propagate beyond that logic unit. In which case, the alternating output from the guardline logic will cease to be generated and the excitation current holding in the control rod circuit breakers will collapse. The basic magnetic core design caters for 2 out of 3 voting logic. Cores can, however, be interconnected to provide 2 out of 4 voting logics.

The Pulse-Coded Logic system (PCL) developed by AEA Technology is a later development of this concept in which solid-state components are used in place of the specially fabricated magnetic cores. With the PCL approach a further feature is added. The pulse generators at the start of the logic sequence output coded pulse trains in addition to the sequential set and reset pulses. Each pulse generator outputs its own unique code.

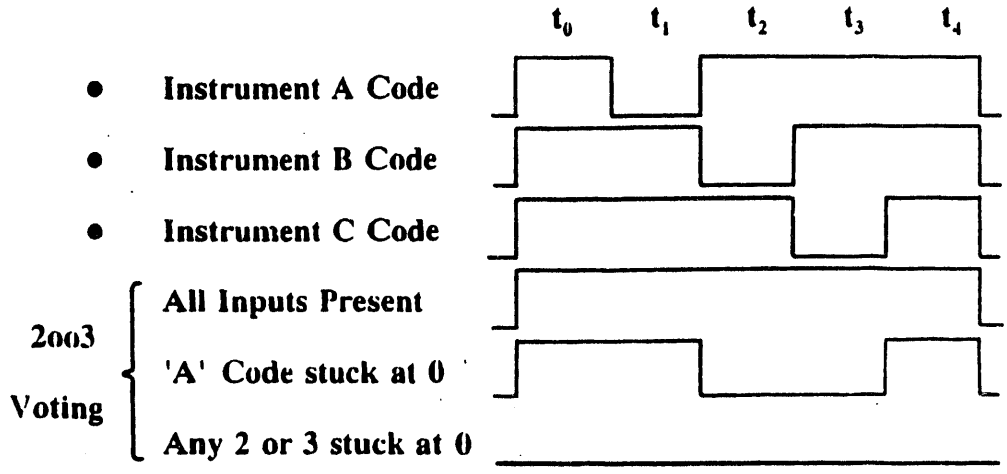


Figure 3. Output Codes for 2oo3 Trip Logic

The output code from pulse generator A are passed through the closed output contacts of all the A trip instrument bistables. The codes from B, C and D pulse generators are likewise passed through the closed output contacts of all the B, C and D trip instruments respectively. After exiting from the closed contacts of the trip instrument output relays the coded pulses are passed to the voting logic. The nature of the coded patterns are such that they exhaustively test all eight input combinations for a two out of three logic unit (16 in the case of a two out of four logic unit). If this exhaustive test fails, then again the set and reset pulse will not be propagated beyond the faulty unit. Through this process, all faults in the logic units are revealed by causing the output to revert to a tripped or safe state. This removes the need to carry out periodic proof tests on the logic units. PCL-compatible bistable instruments can be incorporated into the safety system. These instruments pass the coded patterns through the comparator circuits to include these within the testing loop.

The existence of the coded patterns confers a further important benefit. If a trip instrument fails to a tripped state this will produce a unique corruption of the coded pattern. Provided only one instrument fails out of the 3 or 4 redundant instruments associated with any one trip parameter the set and reset pulses will continue to be propagated and the train of trip logic will not go into a tripped state. However, decoding circuits can interpret the corrupted pattern giving immediate indication of which instrument has failed. This greatly aids diagnosis and reduces significantly overall repair times.

Since each of the unique coded patterns is generated by a separate pulse generator, it is a necessary condition that all 3 or 4 pulse generators run in synchronisation. This was not a requirement for the earlier linked magnetic cores system. Clearly this requires a robust design of a synchronisation mechanism - one which allows continuous synchronised running of the remaining healthy pulse generators should a pulse generator fail.

PCL dynamic safety systems are currently being installed on four Advanced Gas-Cooled Reactors (AGRs) in the UK. These are the two Nuclear Power Plants at Hinkley Point 'B' and the two Plants at Hunterston 'B'.

3. COMPUTER-BASED SYSTEMS

Following the successful development of this fail-safe approach to the design of dynamic safety systems using only hardware components when interest grew in the use of computer-based systems for safety applications, a similar approach was adopted. The aim, as before, was to achieve a design which operated dynamically rather than statically and which generated as its output a holding current which would collapse if (a) a genuine trip demand existed, (b) a faulty component had been revealed by a built-in testing mechanism or (c) the testing mechanism itself had failed. The dynamic safety system developed by AEA Technology to meet these objectives is known as ISAT™ (Inherently Safe Automatic Trip) system.

In a computer-based plant protection system the various input parameters are scanned in using a multiplexer (MUX) and analogue to digital converter (ADC). The output from this data collection system (DCS) is passed as a serial digital data stream to a microprocessor. Using specified trip algorithms computer codes within the microprocessor determine whether any single input parameter or group of input parameters has breached the trip boundaries. In a static system the output of the microprocessor would remain in a logic 1 or healthy state until a trip boundary was breached, whereupon the output would switch to a logic 0 or tripped state.

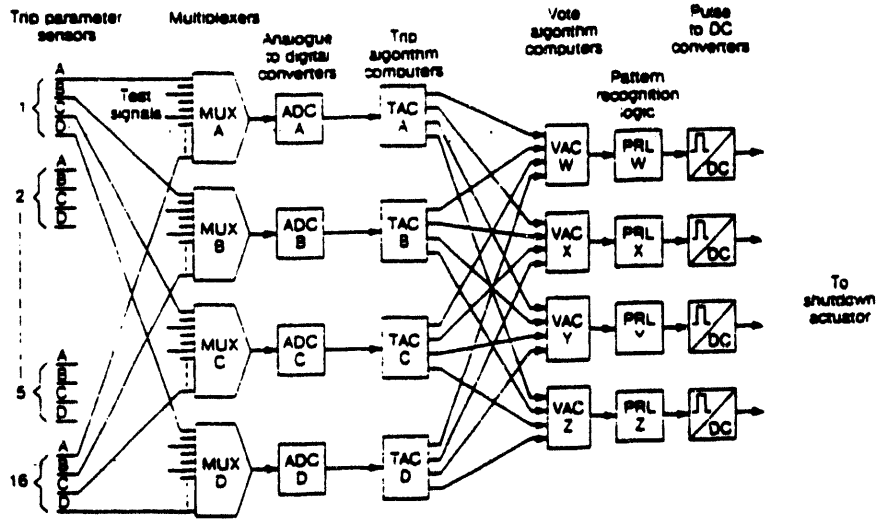


Figure 4. Typical ISAT™ Dynamic Fail-Safe Computer-Based Protection System

The testing mechanisms can be designed to impose a unique pattern on this alternating output sequence. The correctness of this pattern can then be checked by passing it through a hardware verifier. If each successive block of eight output states differs from the proceeding one, then the hardware verifier can receive the first block of eight from the microprocessor and search to find a match within its sequence of reference patterns. If it then receives a second block from the microprocessor it should register a mismatch when checked against the already selected reference pattern. By sequencing on to its next reference block of eight it should, however, again find a match.

A third block of eight from the microprocessor checked against the second reference pattern should again produce a mismatch and when checked against the next block in the reference pattern should produce a match. A correct output sequence from the microprocessor should therefore result in an alternating sequence of match and mismatch states occurring within the hardware verifier. This alternating sequence produces a square wave output signal from the verifier which is then passed to a pulse to d.c. converter to generate the holding current for control rod contactor. If the verifier detects a mismatch when it should have had a match or a match where it should have had a mismatch, the output latches to a static state and the output holding current from the pulse to d.c. converter collapses. Clearly, the hardware verifier is a key unit in such a system. Its design must be such that if any component fails within the verifier the output latches to a static state.

A computer-based reactor protection system using ISAT™ technology has been installed in two UK Nuclear Power Plants on Dungeness 'B' in the UK. These systems have been operating for over 2 years. A detailed report on the operator's experience of this digital upgrade and of the first 18 months' operation of both systems has been reported elsewhere.

Software Aspects

The aim of having good verification and validation (V&V) procedure is to produce high quality software. Quality is defined as fitness for purpose. The customer requirements specification should ideally contain a definition of the desired attribute profile and the final software product should be judged against how closely its actual attribute profile fits the profile specified. In addition to understandability, maintainability, etc., a key attribute commonly focused on is the minimisation of errors made during the software production process. It should be noted that not all errors made during the production process cause fault conditions to occur when the software is operating and not all fault conditions cause the system to fail. System failures due to hardware or software faults can be safe or dangerous. For a plant protection system, the aim should be to minimise the probability of a fail-to-danger fault condition occurring.

There are well established approaches to minimise the number of errors present in the final software product.

Error Avoidance

In order to reduce the probability of making errors which may give rise to faults in operation, appropriate tools and techniques should be used. Of particular importance is the skill and experience of software team members.

A strictly enforced QA regime should be established with clearly written work instructions and procedures to be followed by all team members. A key requirement is to have in place a tightly controlled Configuration Management System (CMS).

Error Removal

Despite the foregoing, errors may still have been made. Procedures exist for error detection (inspections, reviews, walkthroughs, etc). The existence of a fully independent V&V team is a key element in the error detection process.

Extensive testing should also be carried out. The objective of testing is both to reveal residual errors which could give rise to fault conditions in operation and to give increasing levels of confidence in the fitness for purpose of the product. Once an error has been revealed it should be removed using corrective maintenance procedures.

Fault and Failure Management

In order to defend against the very low possibility that errors may still remain despite having thoroughly covered both the above, failure management features can be incorporated both within the software and at the system level. Diversity can be used as a mechanism to reveal faults and avoid dangerous system failure. N-version programming with some form of adjudication mechanism can be incorporated into the design. However, both of these approaches are expensive to implement.

The dynamic fail-safe approach to the design of computer-based safety systems outlined in this paper provides a powerful and cost-effective methodology for fault and failure management, providing as it does a mechanism for assuring fail-safety at the system level. Armed with the knowledge that a hardware verifier exists, the software team is well placed to build in defensive features to trap errors/faults in a manner which assures a fail-safe outcome.

Common Mode or Common Cause Failures

A limitation may be placed by an assessor on the claimed reliability of any system employing redundancy through the use of identical components, measurements or actions. The UK regulatory body (NII) states that for safety system equipment the limitation should be in the range corresponding to one failure per 10^3 to 10^5 demands. A powerful defence against common cause or common mode failures is to have a fully fail-safe system design. If a system design is such that it has no identified fail-to-danger modes then there is a high probability that any unidentified failure modes such as might occur in the presence of CMF or CCF would result in a fail-to-safety outcome. Provided other factors relating to the overall quality of the product and process warrant it, a fully fail-safe design, such as that of the dynamic safety systems described in this paper, may justify a cut-off approaching or even equalling 10^{-5} failures per demand.

Human Factor Aspects

Human errors made while carrying out periodic proof testing can cause faults to be introduced into the system leading to system failure. By building in frequent proof testing as an inherent element of the dynamic functioning of the system, the need for manual testing is greatly reduced or even eliminated. This brings both economic and safety benefits.

Human errors can also occur while carrying out maintenance activities. As a result a testing programme has to be carried out after maintenance to check that the maintenance activity has been correctly performed. A key feature of the ISAT™/PCL dynamic safety systems is that if a fault is present in a channel, that channel will remain in the tripped state until the fault

is removed. A faulty channel cannot accidentally be returned to service. This removes the need for extensive re-testing before return to service after maintenance. It also reduces the amount of confirmatory testing required during initial installation, thus reducing the changeout time.

By decoding and interpreting the corrupted pattern the plant operator is automatically provided with a continuously updated status on the health of the individual sub-modules within the safety system. This reduces repair time and effort, reducing further the already low probability of spurious scrams.

4. COLLABORATION ACTIVITIES IN THE US

For completeness the dynamic fail-safe design concepts should be extended to include both the sensors and the actuators. Currently AEA Technology is collaborating with Ohio State University in an EPRI R&D programme on Dynamic Safety Systems. One aim of this work is to research whether the dynamic safety principles can be applied to input sensors.

AEA Technology and Duke Power Co. are also collaborating on an ISAT™ demonstration at Duke's Oconee Nuclear Station. Duke and AEA plan to install the ISAT™ dynamic safety system approach in the control interface portion of the Oconee Reactor Protection System (RPS). ISAT™ will replicate a complete protection channel to demonstrate the dynamic safety approach in an operating Pressurized Water Reactor (PWR) environment. This installation is planned for the spring 1994 refuelling outage for Oconee Unit 1.

Oconee Unit 1 Demonstrator

Oconee Nuclear station is a three unit Babcock & Wilcox (B&W) Nuclear Steam Supply System-based generating station. Each of the three units are rated at 886 Megawatts (MW) gross electrical generating capacity. The first Oconee unit began construction in 1967. Oconee Unit 1 started commercial operation in July 1973, with Unit 2 following in September 1974 and Unit 3 beginning commercial operation in December 1974.

The original Reactor Protection Systems (RPSs) provided for the Oconee units is based upon the Bailey Meter Company 880/881 electronic module line. These modules reflect the electronic technology available in the late 1960s for safety-related nuclear power plant applications. The 880/881 produce line is used solely by utilities which purchased B&W nuclear steam supply systems using reactors with 177 fuel assemblies. Presently, only the five operating B&W plants utilise the Bailey 880/881 RPS. This RPS design (Bailey/B&W) has performed very reliably for the B&W plants.

Bailey Meter Company (Bailey Controls Company) no longer markets the 880/881 products. Because of the limited application of the 880/881-based systems and their reliable

performance, pro-active manufacturer repair and replacement support has dwindled over the years. To combat this limited manufacturer support, the owners of the operating B&W plants recently purchased and distributed the RPS and Safety Features Actuation System (SFAS) from the shutdown Rancho Seco plant previously operated by the Sacramento Municipal Utility District (SMUD) for additional spare parts inventory.

The planned installation of ISAT™ in the RPS at Oconee is primarily aimed at evaluating various RPS replacement designs and strategies without being forced into selecting a replacement due to age-related obsolescence or catastrophic system failure. The evaluation of various replacement strategies coupled with the purchase of additional Bailey 880/881 analogue electronic modules also allows Duke Power Company and Oconee to bridge the presently uncertain and exhaustive regulatory process for digital replacement systems until the issues associated with digital retrofits are clarified and resolved.

The AEA/Duke Power collaboration effort provides mutual benefits. Duke benefits by evaluating, observing and operating a modern digital replacement system equivalent which offers a step forward from the existing strategies used for most domestic Reactor Protection systems. AEA benefits by gaining audience with the US Regulatory environment for Topical Report review and having an installed ISAT™ demonstrator for evaluation by US utilities investigating RPS replacement options.

5. REFERENCE

1. Jones, C. D. and Smith, I. C. "Experience in Installing a Microprocessor-Based Protection System on a UK Nuclear Power Plant", IAEA Specialists' Meeting: Experience in Ageing, Maintenance and Modernisation of Instrumentation and Control Systems for Improving Nuclear Power Plant Availability, Rockville, MD, USA, May 1993.

[d:\ian\papers\wrnm-pub.93]

AN EXAMINATION OF HUMAN FACTORS IN EXTERNAL BEAM RADIATION THERAPY: FINDINGS AND IMPLICATIONS

Kerm Henriksen, Ronald D. Kaye, and Robert E. Jones, Jr.
CAE-Link Corporation

Dolores S. Morisseau and J.J. Persensky
U.S. Nuclear Regulatory Commission

NOTE: The views expressed in this paper are those of the authors and not necessarily those of the Nuclear Regulatory Commission

ABSTRACT

To better understand the contributing factors to human error in external beam radiation therapy, the U.S. Nuclear Regulatory Commission has undertaken a series of human factors evaluations. A team of human factors specialists, assisted by a panel of radiation oncologists, medical physicists, and radiation technologists, conducted visits to 24 radiation oncology departments at community hospitals, university centers, and free-standing clinics. A function and task analysis was initially performed to guide subsequent evaluations in the areas of human-system interfaces, procedures, training and qualifications, and organizational policies and practices. Representative findings and implications for improvement are discussed within the context of a dynamic model which holds that misadministration likely results from the unanticipated interaction of several necessary but singly insufficient conditions.

1.0 INTRODUCTION

External beam radiation therapy (or teletherapy) is a multi-disciplinary, multi-phased treatment methodology for treating cancerous and other tissue through selective exposure to a beam of ionizing radiation delivered from a source external to the patient. A radioactive isotope, typically cobalt-60, or a linear accelerator capable of producing very high energy x-ray and electron beams are the principal sources of radiation. Treatment typically takes place on a daily basis in fractional doses over a period of weeks and is planned and administered by a team of specialists, including a radiation oncologist, radiation physicist, dosimetrist, and radiation therapy technologists. Effective treatment requires a concern for precision and consistency of human-human and human-machine interactions throughout the duration of therapy. Records maintained by the U.S. Nuclear Regulatory Commission (NRC) have identified instances of teletherapy misadministration where the delivered radiation dose has differed from the radiation prescription

(e.g., instances where fractions were delivered to the wrong patient, to the wrong body part, or were too great or too little with respect to the defined treatment volume). Both human error and machine malfunction have led to misadministrations. Misadministration above the prescribed dose runs the risk of destroying healthy tissue and organs; misadministration below the prescribed level can result in ineffective treatment. Either way, the consequences of misadministration can be life threatening.

The present paper reports on a series of human factor evaluations sponsored by NRC's Office of Nuclear Regulatory Research to identify the factors that contribute to misadministration in the radiation therapy environment. The six major parts of the overall study include: 1) a function and task analysis of the teletherapy activities, 2) evaluation of human-system interfaces 3) evaluation of the procedures used by teletherapy staff, 4) evaluation of the qualifications and training of teletherapy staff, 5) evaluation of organizational practices and policies, and 6) identification of human factors priority areas for NRC and industry attention.

2.0 BACKGROUND TO THE RADIATION THERAPY PROCESS

Figure 1 identifies the key staff functions in radiation therapy as recognized in a report to the National Cancer Institute, National Institutes of Health entitled *Criteria for Radiation Oncology in Multidisciplinary Cancer Management* (1981). Once malignancy is confirmed, the oncologist conducts a clinical evaluation to "stage" the disease to determine its extent. After clinical evaluation, a therapeutic decision is arrived at for determining the intent of therapy. A curative intent seeks to eradicate the tumor; a palliative intent seeks to relieve suffering and prolong life to the extent possible. Tumor localization defines the tumor volume and is the first step in defining the treatment volume. The treatment volume is always larger than the tumor volume in order to cover microscopic extensions of the tumor and other factors such as movement during treatment caused by the patient's respiration. This phase also identifies the safe limits of normal tissue and structures that will be exposed to radiation. Treatment planning specifies the best configuration of beams and dosage for a specific patient in order to effectively target the tumor and minimize damage to surrounding healthy tissue. The oncologist specifies the overall dose to the tumor and critical normal tissues. The physicist then designs the potential treatment delivery approaches in conjunction with the oncologist for satisfying the treatment requirement. Patients are measured, body contours are drawn, and isodose curves are generated either manually or with the aid of treatment planning computers. To achieve maximum accuracy, the treatment set up is first simulated on a separate device that resembles the treatment machine and enables precise and accurate location of the treatment fields. Radiographic films are taken to position the fields appropriately. Treatment fields or portals are marked for subsequent treatment by applying tatoos or dyes to the patient's body. Simulation thus allows for verification of the treatment approach and resolution of treatment planning issues before actually using the treatment machines. Figure 1 shows that special treatment aids are likely to be needed. The fabrication of custom lead alloy blocks (for shielding radiosensitive structures from the beam) and immobilization devices (for keeping the patient in the same position treatment after treatment) are quite common.

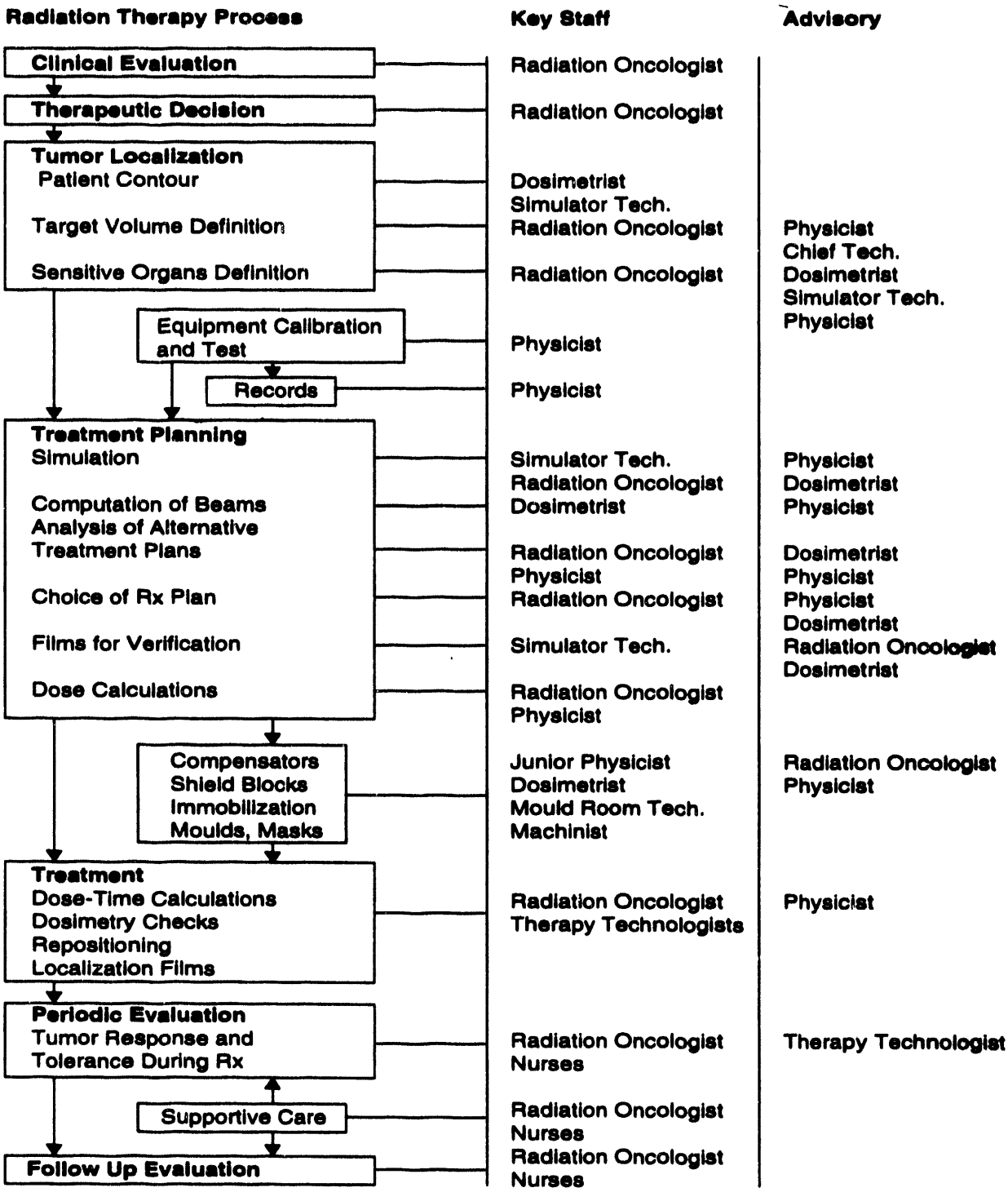


Figure 1. Key Staff Functions In Radiation Therapy

(Adopted from *Criteria for Radiation Oncology in Multidicisplinary Cancer Management*, National Institutes of Health, 1981.)

After all the details of treatment planning have been worked out, the patient begins a course of treatment that will include daily treatment doses or "fractions" over a period of weeks. The radiation therapy technologists now have the greatest degree of contact with the patient. Their workload varies with respect to organizational setting; however, patients need to be positioned accurately, numerous machine parameters entered, treatment accessories put in place, patients monitored while the beam is on, accurate daily records of administered dose kept, and the unique needs of individual patients need to be attended to in a compassionate manner. Steps are taken to avoid any deviation from the treatment plan since the possibility of human error—treating the wrong patient, leaving out a block, entering a wrong machine parameter, imprecise patient positioning, failing to record a treatment—is always present. Patient evaluation and follow up are the last phases and involve assessment of tolerance to treatment, evaluation of tumor response, and assessment of complications.

3.0 METHOD

A site sampling strategy for visiting departments of radiation oncology within the continental U.S. was developed to ensure geographic dispersion and representation of different types of facilities to accommodate differences in treatment practices, management style, personnel, patient load as well as other factors likely to vary among facility sites. Three different types of facilities were visited:

- large community hospitals and satellite facilities
- university-based centers
- free standing facilities

Efforts also were made to focus on centers with Cobalt-60 units because of NRC's by-product regulatory responsibilities. Interviews were conducted at 24 sites throughout the U.S. with radiation physicists, dosimetrists, radiation ocologists, chief technologists, staff technologists, training coordinators, and administrative personnel. The interviews were supplemented with observations of on-going treatments, examination of equipment controls and displays, and a review of the radiation oncology literature.

A function/task analysis database was the first phase of the project that was completed and served as a useful inventory of essential teletherapy activities for performing subsequent phases (Kaye, Henriksen & Jones, 1993). At most locations, site visits were scheduled on the basis of one center a day. Structured interview and data collection forms were prepared and approved by a panel of oncologists, physicists, and technologists serving as consultants to the project. Because of the small sample and use of open-ended interview questions, no attempt was made to analyze the collected data statistically.

Human factors issues were derived on the basis of: 1) comments from two or more respondents during site visits, 2) information contained in incident reports, 3) treatment-related observations made during site visits, 4) findings from the radiation oncology and human factors

literature, and 5) information provided by the panel of radiation oncology therapy experts. All issues identified are based on at least two corroborating sources of information.

4.0 MODEL OF CONTRIBUTING FACTORS

To provide a framework for making sense of the findings, a model specifically suited to the teletherapy environment was constructed. Adapted from the work of Sanders and Shaw (1988) and Reason (1990) on accident causation, Figure 2 shows the major contributing factors and individual factors in each category that are likely to influence the occurrence of a misadministration. Since the occurrence of a misadministration is a focal point in the model, it requires a definition. A treatment misadministration in external beam radiation therapy as currently ruled by the NRC (*Federal Register*, Vol. 56, No.143, July 25, 1991) has the following meaning.

A radiation dose:

- Involving the wrong patient, wrong mode of treatment, or wrong treatment site,
- When the treatment consists of three or fewer fractions and the calculated total administered dose differs from the total prescribed dose by more than 10 percent of the total prescribed dose,
- When the calculated weekly administered dose is 30 percent greater than the weekly prescribed dose, or
- When the calculated total administered dose differs from the total prescribed dose by more than 20 percent of the total prescribed dose.

Given the above definition and the fractionated manner in which external beam therapy is administered, it is clear that not all treatment administration errors result in misadministrations. Many treatment administration errors can be compensated for in subsequent treatments if detected early enough.

The first block in the figure shows a sliding scale or relationship between acceptable human performance and human error and is intended to connote the somewhat arbitrary nature of how human error is sometimes defined. As noted by Rasmussen (1987), when system performance is outside the limits of some specified standard, an effort is made to backtrack the causal chain to find the causes. How far back to go or when to stop the backtracking process is an open question likely to vary among different investigators. In radiation therapy, one could stop at the technologist's actions and claim operator error, or one could seek to identify other reasons—incomplete procedures, confusing controls and displays, malfunctioning components, mistakes by management—that may have served as contributing factors. Rasmussen notes that the search for causes will stop when we come across one or more factors with which we are

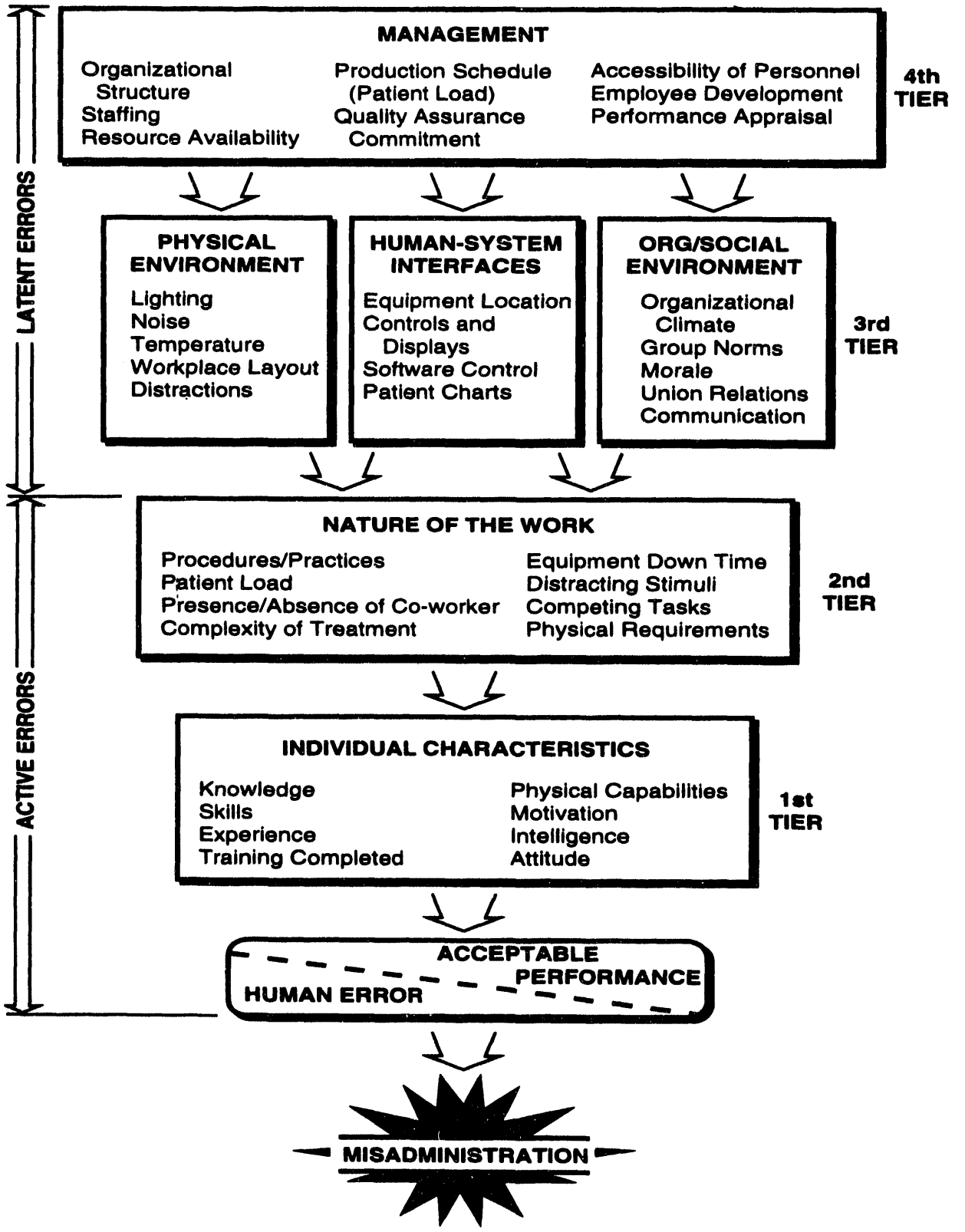


Figure 2. Contributing Factors To Human Error in Radiation Therapy

familiar and therefore find as acceptable explanations, and for which there is an available correction or cure. Since there is no well-defined "start-point" to which we are progressively working backwards through the causal chain, how far back we are willing to go also depends on pragmatic factors such as resources, time constraints, and internal political ramifications. Also in radiation therapy, the significance of a deviation in treatment delivery is frequently a clinical judgment based on the parameters involved, the anatomical location of the field, and the treatment technique. For example, a field size error of half a centimeter that borders a critical structure (e.g., lens, spinal cord) is significant; bordering a non-critical structure, the same magnitude of error would not be considered significant (Mohan, Podmaniczsky, Caley, Lapidus & Laughlin, 1984).

The successive tiers of contributing factors in Figure 2 are arranged in a progressively distal relationship from the occurrence of human error. Each successive tier is shown as having a direct influence on the factors of the preceding tier. Although not portrayed in the figure, the influence of the contributing factors need not be conceived solely in unidirectional terms, but may interact in bi-directional or other intricate patterns. It is very likely that the factors in the figure do not exert their effects in an isolated, singular fashion, but instead combine with one another to lead to complex and difficult-to-decipher interactions.

The first two tiers, labelled *individual characteristics* and *nature of the work*, reflect the individual qualities of technologists and other staff members (e.g., knowledge, physical capabilities, training completed, and motivation) and the nature of their more immediate work environment (e.g., patient load, complexity of treatment, distracting stimuli). These first two tiers focus, to a large extent, on the individual competencies and immediate task environment of the technologists. As front line workers in the teletherapy system, they are called upon to set up patients on the treatment couch, enter the necessary machine parameters to deliver the correct dose to the treatment fields, turn the beam on, and record the administered daily fractionated dose and accumulated dose for each field. Errors that can be traced to factors in the first two tiers are called active errors; their occurrence is associated with the delivery of treatment and they are frequently discovered immediately or in the near term.

Further upstream in Figure 2, in tiers three and four, are the broader scale workplace environment and managerial factors. Errors that can be traced to these tiers are propagated by those in decision-making positions (e.g., architects, equipment designers, department heads). Far removed from the daily treatment activities of the technologists, these are the fuzzy, difficult-to-trace, and often unrecognized errors that lie dormant for some time in the greater socio-technical system. A poorly designed interface on a treatment console or a lack of adequate staffing are examples of latent errors at tiers three and four. As noted by Reason (1990), the adverse consequences of latent errors may remain inert for some time in the overall system, only to breach the systems defenses when they combine with other factors in unanticipated ways. A systems perspective leads one to suspect that the difficult-to-recognize latent errors that are made upstream by system designers and organizational policy makers permeate the system and contribute to the downstream active errors made by technologists.

5.0 FINDINGS AND IMPLICATIONS

The section that follows summarizes representative findings and implications for improvement organized in accordance with the major contributing factors of the model. A fuller discussion of these findings is currently in preparation as a five volume set to be submitted to the NRC.

Individual Characteristics

Figure 2 identifies *individual characteristics* as a first tier major factor that has a direct impact on the likelihood of acceptable performance or human error. Individual characteristics include knowledge, skill level, adequacy of training, maturity, and organismic states such as alertness, motivation, physical capabilities, and fatigue. Wiener and Englund (1990) examine many of these characteristics in a review of factors affecting anesthetic vigilance and monitoring performance in the operating room environment. Such a review does not need to be repeated here. The individual characteristic of training, however, is a key factor of interest in the present study. The formal training or schooling that radiation therapy technologists, dosimetrists, and physicists receive prior to employment constitutes the major component of their preparation and readiness to perform teletherapy services. The typical preparation for RTTs is a two year program at a community college that combines classroom instruction with clinical experience at a near-by hospital. Many radiation therapy facilities require that RTTs be certified or eligible for certification through the American Registry of Radiologic Technologists at the time of hire. With respect to dosimetrists, many hospitals train their own (usually an experienced RTT), while radiation physicists have a master's or doctoral degree with a concentration of coursework in radiologic physics, anatomy, physiology, oncology, and radiobiology.

Once hired, most of the training that occurs in departments of radiation oncology is on-the-job (OJT) training. Unfortunately, when training is done on an informal OJT basis, it amounts to little more than a newly hired employee working side-by-side with a senior employee for a few months. Accountability is frequently absent with respect to establishing specific training objectives or to structuring the trainee's work environment such that it systematically promotes learning. With many OJT programs, it is very difficult to determine what is being learned despite the good intentions of the person in charge of training. Despite these limitations, OJT is the principal means of training RTTs for a variety of requirements: orienting new personnel to department, orientation to new equipment and software, and orientation to new procedures.

While some industries with complex and hazardous work environments (e.g., military, commercial aviation, nuclear power plant) have developed systematic training procedures for responding to unexpected problems and for reducing human error, there was no evidence of the use of systematic training procedures in the departments of radiation oncology that were visited. For example, a machine malfunction that can have serious consequences with some Cobalt-60 units is for the source to unexpectedly get stuck in the unshielded position. The likelihood of such an occurrence can be minimized by good design and by a conscientious program of preventive maintenance. When a stuck source does occur, the radiation therapy technologists have to intervene decisively to minimize radiation exposure.

The probability that technologists are able to perform what may appear to be a simple sequence of activities would be considerably greater if they had first received a systematic performance-oriented training program where they actually practiced these activities. Posting these procedures on the wall in the form of a job aid, as was observed at several facilities, may not be sufficient when such a stress-producing incident happens. Rather than waiting for human error to compound the adverse consequences of such an incident, a more active strategy would be to design training that specifically trains technologists for responding to critical high-pressure and unexpected circumstances. Through realistic simulation exercises, similar to airline cockpit emergency procedures training, technologists could be trained in scenarios that involve equipment failures, patient complications, or any combination of infrequent circumstances.

Table 1 lists several potential problem areas specific to training that the study identified along with some implications for improvement. In addition to informal on-the-job training and emergency training, the table addresses new equipment training, more extensive training in dosimetry, and training on the multiple contributing factors to human error.

Nature of the Work (Task Variables)

The second tier factor in Figure 2, *nature of the work* or *task variables* refers to characteristics of the work itself and includes the extent to which written and unwritten procedures are utilized, the production schedule or number of patients treated per day on a given treatment machine, the presence/absence of a co-worker, equipment down-time, distracting stimuli or competing tasks, treatment difficulty (e.g., very ill patients or children), and perceptual-motor requirements. Although empirical studies are frequently non-existent or in conflict, all of these variables can potentially influence human performance and human error. A study by Swann-D'Emilia, Chu and Daywalt (1990) reports a disproportionate number of errors as patient production schedules increase. The number of patients treated per day with a given treatment machine depends on a number of factors, but one of these factors is the efficiency and quickness by which technologists can set up, treat, and then get ready for the next patient. To maximize the use of the technologically sophisticated and costly treatment units and to be of service to as many patients seeking treatment as is possible, the existing practice in the U.S. is to schedule patients back-to-back, with as many as four to five an hour. As a consequence, technologists perceive a need to work as efficiently as possible. Making efficient use of resources constitutes good management practice, but only up to a point. If management personnel become overly ambitious in the number of patients they decide to treat, work conditions are likely to become stressful for technologists and errors more likely to occur. Swann-D'Emilia et al. (1990) recorded both frequencies of occurrence of the average monthly census across successive intervals of patient load (e.g., 20-24, 25-29, 30-34, 35-39 patients per day per machine) and misadministrations occurring within those intervals for the treatment machines in operation at their facility in 1988 and 1989. For both their 1988 and 1989 data, there was a disproportionate number of misadministrations at the higher census intervals even though these higher census intervals occurred less frequently.

In the present study, human error was readily acknowledged at the facilities visited. Clerical and calculation errors were by far the most frequently cited errors. For the most part, clerical errors refer to charting (e.g., confusing monitor units with the fraction dose) and simple arithmetic errors made by technologists, while calculation errors refer to a variety of computational errors made by dosimetrists and physicists. Given the large number of steps and

Table 1. Potential Problem Areas and Implications for Improvement Specific to Training

Potential Problem Area	Implications for Improvement
Extensive reliance on informal on-the-job (OJT) training for newly hired technologists makes it difficult to determine if employees have acquired the necessary skills and knowledge for unsupervised job performance.	On-the-job training programs at hospitals should be more structured, meaning that training objectives need to be established, work assignments scheduled for promoting mastery of objectives, and a formal evaluation procedure for assuring that the required standards of performance have been achieved.
When new equipment is purchased at a facility, the training received by staff members who will operate the equipment is sometimes less than adequate (i.e., left to individual initiative, an operator's manual, or the vendor's ability to provide training).	The training requirements for new treatment and treatment planning equipment should be carefully considered by teletherapy facilities at the time of purchase. Feedback from employees is very useful for assessing the adequacy of provided training.
Physics department personnel have indicated that technologists need to have a better conceptual understanding of dosimetry in order to facilitate communication.	The two-year centers and schools that train technologists need to examine the extent to which dosimetry is covered. Such an examination needs to be coordinated with dosimetry and physics representatives to ensure a reasonable division of labor with respect to assigned duties.
None of the respondents indicated they received any special training (e.g., emergency training) for responding to machine malfunctions such as stuck sources in Co-60 machines.	Rather than waiting for human error to compound the potential adverse consequences of stuck sources or patient complications, realistic simulation exercises, similar to airline cockpit emergency procedures training, could be implemented to insure that technologists decisively follow the correct sequence of activities during an emergency.
Most teletherapy personnel focus on the active errors that technologists are likely to make to the neglect of the latent role that management decisions, environmental factors (both physical and social), and organizational policy have on human error.	Greater awareness of these latent contributing factors to human error from a system's perspective is needed by all teletherapy personnel, especially those in management positions. Training programs at centers and schools, presentation of human factors papers at radiation oncology conferences, and training pamphlets distributed to radiation oncology departments are approaches for increasing awareness.

the number of people involved in the teletherapy process, errors due to inaccurate transfer of information can be systematically passed along to each subsequent step and have undesirable effects on treatment. Independent double-checking and weekly chart checks catch most of these errors, but not all of them. Leunens and associates studied the frequency and sources of transfer errors for 464 new treatments over a nine month period (Leunens, Verstraete, Bogaert, Van Dam, Dutreix & van der Schueren, 1992). Erroneous data transfer was detected in less than 1% of the transferred parameters; however, this affected 26% of the checked treatments. It was estimated that each new treatment involved about 52 data transfers. The origin of the transfer errors were traced to one of five places in the treatment preparation chain: 1) procedure used in treatment simulation, 2) during the input of data in the treatment planning system for calculating the dose distribution and the monitor units, 3) when preparing the treatment chart, 4) during the input of parameters in the record and verify system, and 5) technologists' modification of the parameters introduced in the record and verify system.

The next most frequently cited class of error was failures of communication. Communication failures refer to both breakdowns in verbal communication (e,g., inadequate transfer of clinical information to appropriate personnel) and ambiguous written instructions. The attending oncologists were frequently cited as a source of inadequate communication. Errors concerning the omission or improper use of blocks and wedges were mentioned several times as were errors associated with patient alignment and positioning. Despite the use of immobilization and positioning devices, achieving the same patient position for each successive treatment represents a very persistent source of error (e.g., intricate head and neck treatments can be especially troublesome). Setting the wrong field size also was mentioned. Here the technologist may simply reverse the X-Y coordinates of the field (e.g., setting 12 cm X 14 cm rather than 14 cm X 12 cm). Other reported errors include setting the wrong monitor units or treatment times, selecting the wrong energy level, using the wrong tatoos, machine misalignment, using a previous patient's settings, and giving one or more extra treatment fractions. Software errors, made by software development personnel far removed from the front-line activities of the technologists, also were cited and have received separate attention in the literature (e.g., Jacky, 1989).

Most of the errors that dosimetrists and technologists make are the slips and lapses of skill-based performance. Slips and lapses, according to Reason (1990), are actions which deviate from current intention and usually involve momentary interruptions of highly practiced, automatic routines. Slips are generally observable as external actions not-as-planned (e.g., slips of the tongue, slips of action), whereas lapses are errors that do not overtly manifest themselves in behavior. They largely involve failures of memory. In the teletherapy setting, inserting the wrong block would be an example of a slip, while failing to record a treatment would be considered a lapse. Since technologists are quite proficient at inserting blocks and recording the daily treatment, the need for further training on these tasks is questionable. On those occasions where there is a slip or lapse in skill-based performance, it makes more sense to remove the environmental and organizational factors that contribute to the error, rather than try to improve task performance that is already at an asymptotic level. On the other hand, errors of judgment or mistakes that are made by managers and decision makers are frequently equivalent to gaps in knowledge structures. Although there is much that needs to be learned about knowledge-based mistakes, they appear to be more amenable to training interventions.

Table 2 summarizes some of the potential problem areas associated with the nature of the work and implications for addressing the problems.

Physical Environment

The benefits of a work environment that is purposefully designed for the nature of the work that is performed have been well understood by the military and aerospace industries for a number of years. Other professions, including the various medical disciplines, have more recently begun to appreciate the relationship between workplace variables (e.g., design of jobs, equipment, and physical layout) and employee performance (e.g., efficiency, reduction of error, and job satisfaction). Intelligent design of the workplace environment will not only eliminate unnecessary effort in the actual execution of jobs, but also can improve the way information is transferred from people to people and between people and machines. As we become more aware of the latent or less recognized contributory factors to human error, the more we appreciate the role of factors that make up our immediate work environment. Harrigan (1987) identifies a number of questions that should be answered if one intends to design work environments from the perspective of user requirements and expectations. What individuals and groups exchange information and what is the nature and frequency of this exchange? What are the recommended circulation patterns for facilitating information, users, equipment, and material flow between spaces? What provisions with respect to users should be made for temperature, humidity, airflow, lighting, noise, distraction, hazards, and climatic conditions?

There were no obvious deficiencies in terms of the more traditional physical factors at the sites visited. Lighting was considered adequate. Nobody complained about noise levels. Although ambient noise measures were not taken, noise levels were perceived to be slightly higher at the busier facilities. Internal furnishings and wall and floor treatments appeared to attenuate noise levels at several facilities. Only one university-based facility appeared noisy with the most distracting aspect of the ambient noise coming from frequent paging of individuals on the public address system. At another facility, a physicist noted that many teletherapy departments are in the basements of hospitals where it is more difficult to control temperature. Staff bring in space heaters which can be tripped over and patients may be less able to hold still when placed on a cold treatment couch.

In some of the older radiation therapy facilities visited, inappropriate spacial arrangements were found with respect to personnel that need to be close to each other. Physicists and oncologists need to be located close to the workstations of technologists (or at least be accessible) to respond to questions regarding treatment. When these personnel are located on separate floors or in out-of-the-way locations, questions regarding treatment clarification are frequently left unasked.

In another facility, the physical layout was such that patients reporting for treatment descended from an elevator and entered the facility first through the workstation area occupied by technologists who were administering treatments. On several occasions the attention of the technologists would be diverted from a given treatment to respond to a question that a patient or the transporter of a non-ambulatory patient would have. Sources of distraction and competing

Table 2. Potential Problem Areas and Implications for Improvement Specific to the Nature of the Work.

Potential Problem Area	Implications for Improvement
Excessive workload and patient treatment schedules can bring about treatment related errors. Workload fluctuates between facilities and time of day; however, workloads sometimes exist at levels which increase the likelihood of treatment delivery errors by technologists.	The function of patient scheduling needs to be reexamined by department heads at some facilities. Recommended alternatives for workloads conducive to high quality treatment include a more distributed method of scheduling patients to avoid periods of peak load, reassignment of non-treatment related duties of technologists during treatment hours to other personnel or times of the day, insuring that staffing is adequate, and that all equipment is maintained in good working order.
Transfer of information errors during charting and dosimetry computations occur despite prevalent practices of independent double checking and weekly chart checks. The redundant checking sometimes focuses on mechanical arithmetic operations to the neglect of the appropriateness of the parameters.	Increasing attention to detail is difficult to achieve. One facility initiated an incentive program with encouraging results by monthly rewarding the staff members who detected the most errors. Experimentation and evaluation of alternative checking procedures should be encouraged. *Post hoc* investigations into the process by which errors were made after being missed by previous checks is another suggestion. An examination of the sources of transfer error (e.g., misleading spacial and orthographic cues) in charts and tables also merits closer investigation.
Technologists sometimes do not notice changes in the patient's chart pertaining to the planned termination or modification of treatment, thereby administering extra treatments, or administering more or less dose than what is prescribed.	Charting procedures need to indicate the point in the chart for entering data for final treatment. Likewise, termination cues for fields for which treatment will be completed prior to other fields needs to be clearly indicated.
A number of routine treatment set up errors (e.g., omission or the wrong selection of blocks and wedges, reversal of X-Y coordinates for field sizes, setting the wrong monitor units or treatment times, selecting the wrong energy level, treating the wrong anatomy, and using the wrong tatoos) occur and appear to be related to the repetitive nature of the work and rushed treatment schedules of technologists.	Treatment set ups should start with an examination of the patient's chart rather than relying on memory or cues associated with previous treatment (e.g., old field marks). Although a high priority is placed on daily examination of the patient's chart, other organizational factors may contribute to error. Facility management needs to take steps to ensure reasonable staffing levels and treatment schedules so that short-cuts are not taken with chart checking and treatment set-ups.
Approximately 25% of the visited sites were understaffed by one technologist. Inadequate levels of staffing increase the workload (i.e., with one rather than two technologists assigned to a machine) and encourage short-cuts to be taken with routine checking procedures.	Dedicated efforts to insure adequate staffing need to be taken by facility management at those hospitals that are understaffed. By having two technologists assigned to a machine, treatment set up and patient positioning errors could be reduced through double checking procedures.

tasks (i.e., responding to phone queries) need to be held to a minimum in the technologist's work area during treatment hours. Most of the newer facilities had separate entrance and waiting areas and, in general, reflected a more intelligent design of the workspace. Periodic Examination/Re-evaluation of Patient Status (on Treatment Visits (OTV))

Another physical environment attribute is the visual attractiveness of the facility. There was considerable variation with respect to the attractiveness of the decor, ranging from poorly lighted and poorly furnished departments in drab basements to very pleasant surroundings with an abundance of light, green plants, attractive furniture, and wall decorations. Although opinion is divided on the importance of an attractive visual environment, many respondents considered it conducive to maintaining good morale for patients and employees alike. The above problems and implications for change are summarized in Table 3.

User-System Interface

The user-system interface refers to the manner in which two sub-systems, humans and equipment, interact or communicate within the boundaries of the entire system. As the proliferation of automated systems has dramatically changed the user-system interface, concerns about the role and level of understanding required of the human operator have been expressed (Bainbridge, 1987; Norman & Draper, 1986; Reason, 1990). Some investigators view today's operator as little more than a passive custodian for a complex system he or she poorly understands. Others maintain that automation has actually relieved operators of the drudgery of repetitive and error-prone tasks, thereby freeing them to use their higher level cognitive and supervisory capacities to respond to unanticipated system anomalies and failures. Typically operators receive very little practice in responding to system anomalies. Because effective responding to dynamic system anomalies requires knowledge-based problem solving and extensive practice, Reason (1990) notes that operators are likely to suffer performance deficiencies in precisely those activities that justify their marginal existence.

In radiation therapy, improved user-system interfaces can prevent errors that would otherwise go unnoticed. In setting up a patient, as many as 15 to 20 machine parameters may need to be entered for each field that is treated. To detect and prevent deviations in the delivered radiation dose, manufacturers have started to offer computerized record and verify (R&V) systems. These systems inhibit a machine from being turned on when the parameters set on the machine do not agree with the prescribed ones to within specified tolerances. In one study, 416 significant deviations (e.g., verification failures involving monitor units, collimator angle, blocking tray, gantry angle, energy, field size, and wedges) occurred over a one-year period on three treatment machines that would otherwise likely go undetected (Mohan et al., 1984). Based upon their verification failure rates, approximately 60% of the patients would have encountered one significant deviation throughout their course of treatment. About a third of the facilities were using R&V systems at the time the authors visited, with many of the non-using facilities expressing interest.

Table 3. Potential Problem Areas and Implications for Improvement Specific to the Physical Environment

Potential Problem Area	Implications for Improvement
Inappropriate spacial arrangements of workstations and offices were found in older facilities among personnel who need to work in proximity (i.e, physicists and technologists; oncologists and technologists).	Redesign of a radiation oncology department is a major undertaking that would likely exceed the budgets of many hospitals; however, if redesign programs are projected or if options exist with respect to physical arrangement of personnel, those personnel who need to have frequent access to one another need to be proximately located.
One finds a variety of chairs and stools used by technologists and other personnel. Not much consideration appeared to be given to seating requirements; however, differently styled chairs and stools have different effects on posture, circulation, pressure on the spine, and amount of effort to maintain a position.	Seated tasks that occur on a repetitive basis should be supported by a backrest that moves up and down and backward and forward. The backrest helps to maintain the inward curve of the lower spine (lumbar) and encourages good sitting posture which results in even pressure on the spinal discs.
Unnecessary workplace distractions stemming from poor physical layout of the workplace were found at some facilities (e.g., workstations in heavily trafficked aisle-ways or near entrance areas for patients).	Workspace design for technologists needs to keep sources of distraction to a minimum during treatment hours.
Unnecessary competing tasks brought about by placement of phones at technologist's workstations were observed. Technologists were expected to answer calls from other hospital departments regarding patient treatment scheduling. They considered such interruptions disruptive to treatment administrations and record keeping.	Interruptions and tasks that compete for the technologist's attention during treatment administration and record keeping should be avoided during treatment hours. Such tasks can be performed during non-treatment hours or assigned to other personnel.
Departments varied considerably with respect to visual attractiveness. The less attractive facilities were in drab and poorly furnished basements, creating a less than optimistic atmosphere.	Visual attractiveness admittedly is a subjective phenomenon and while not everyone agrees with its importance, one is likely to attribute positive qualities to (and perhaps have greater confidence in) those hospitals that provide an attractive treatment setting.

A primary concern with R&V systems is the correctness of the initial entered parameters that will be used throughout the course of treatment. It is not unusual for automated systems to reduce or eliminate small errors while creating the potential for large ones (Weiner and Curry, 1980). Leunens et al. (1992), in a study of the relative distribution of major errors detected after the first treatment, found that initial entry errors in R&V systems were more common than other types of errors found (e.g., chart preparation, dose distribution/calculation of monitor units, and treatment simulation). Errors associated with the entry of treatment parameters into R&V

systems before or during treatment have the potential to result in serious departures from the intended treatment. Leunens and associates observed that technologists are not likely to question data when it is presented on monitors located in the treatment room.

The present investigators also observed that technologists tend to set up treatment parameters with few questions regarding the accuracy of the displayed data. Since it is easier to look at the monitor while setting up the treatment, rather than glance down at a chart or ask another therapist for set up information, technologists typically position the treatment table, collimators, and gantry until the preset tolerances of the R&V system enable an "OK" to be displayed on the monitor. Setting up the treatment in accordance with the R&V system's tolerances can result in losses of precision and systematic errors since R&V tolerances can be set less precisely than tolerances that can be set on the treatment machine. For example, field sizes can be set to the single millimeter on most treatment machines; however, current R&V systems are designed such that tolerances can be set to as much as 5-10 millimeters. A systematic error of even 2 or 3 millimeters throughout the duration of treatment would not be acceptable when the irradiated volume borders a radiosensitive structure such as the spinal cord (J.A. Deye, personal communication, August 11, 1993).

Part of the challenge for users of computer systems comes from the opaque nature of those systems. Unlike simpler electro-mechanical systems, the functionality of computer systems cannot be easily discerned by looking at the system. Relegated to a monitoring function, the user is removed from the actual storage, processing and transfer of information. Very few things need to be "tweaked." Given the opaque nature of computerized systems, operators frequently do not have a good understanding of the system's full functionality or even what state the system is in. Weinhous (1991) notes that the control system of today's linear accelerator is concealed in proprietary software, making it very difficult to ensure their effective and safe operation. Despite continued improvements in software quality assurance techniques, some software errors are likely to remain buried and only discovered through actual clinical use.

A recent lesson on the perils of opaque computerized systems comes from computer-based treatment planning. Treatment planning typically involves extensive use of a treatment planning computer to provide a graphic view of the treatment beams and the resulting total dose to the area undergoing treatment. The major advantage of a computer generated treatment plan is the ability to incorporate measurements of the patient's internal and external anatomy into the process of positioning intersecting beams for maximum treatment of the target and minimum exposure to healthy tissues. Treatment planning computers contain data corresponding to the treatment machines for which plans are developed. For Co-60 treatment machines, the activity of the source housed in the machine is a very important data element. Because sources are changed every five years or so, an older source will be much less active (requiring longer exposure times) than a source that is relatively new. In an incident reported to the NRC, treatment files corresponding to an older source were used mistakenly for calculation of patient treatments. Because many treatment planning computers automatically compute exposure times for a given dose, the times computed in this case were incorrect and 33 patients received doses 75% in excess of the prescribed dose. In this case, the [chief oncologist] directed the physicist not to

update the output parameter data for using beam trimmers (special accessories that shape the beam). The [chief oncologist] later decided to use beam trimmers for brain tumor therapy, and the old files were used in treatment planning. As noted in Table 4, procedures need to be established for maintaining consistency between changes to treatment equipment and accessories that alter the beam and the parameters entered in treatment planning computers.

The last two problem areas reported in Table 4 are of a less opaque nature. A fairly common problem with Co-60 control equipment is the degree of inaccuracy inherent in many of the original spring-loaded circular timers. An inherent disadvantage is the tendency for the spring-loaded timer wheel to lashback after setting it to the desired setting. In other words, when the technologist sets the timer on the 30 second marker, it gives slightly or lashes back to perhaps 28.5 seconds upon releasing the wheel. Kartha, Chung-Bin, Wachtor and Hendrickson (1977) reported error rates for Co-60 timers that were approximately double the rate for digital devices counting monitor units for linear accelerators, and concluded that Co-60 timing errors could be reduced by digitizing the timer.

The source reshielding failures listed in Table 4 typically result in a small amount of radiation delivered to the patient in excess of what was planned. The physical cause of the stuck source varies with respect to equipment model and manufacturer; however, the concern from a human factors perspective is how quickly the technologist becomes aware of the stuck source condition and how decisively the treatment staff react after the stuck source condition is known. Incident reports and observations indicate that technologists react to the mechanical click sound made by the timer after the treatment counts down to "0." After the click, technologists may not respond as rapidly as they should to the source status indicator display on the control console or the flashing red light above the treatment room door given a source reshielding failure. Unnecessary exposure to the patient and to the treatment staff could be avoided if sufficiently unique information, such as an audio alarm, is provided that indicates treatment time has elapsed and the source is unshielded.

Organizational/Social Environment

Until recently, errors that could be traced to the organizational/social environment were poorly understood due, in large measure, to their diffuse and difficult-to-assess nature. Although the importance of organizational and social factors have been intuitively obvious for many individuals who report every day to organizations for their livelihood, empirical studies which clearly demonstrate the effects of these factors are less easy to cite. Nevertheless, the significance of organizational factors has been underscored in an increasing number of studies on human error, accidents and safety (Headrick, 1986; Reason, 1990; and Sanders and Shaw, 1988). For this reason, respondents in the present study were asked if they could identify any organizational characteristics, administrative decisions, or management practices that were less than desirable and likely to contribute to human error or misadministration of dose. Table 5 lists the organizational and managerial factors that were mentioned (Henriksen, Kaye & Jones, 1993).

The table combines organizational and managerial factors even though the present paper treats these factors separately. Several comments, starting with threatening environment and ending with lack of team spirit, all seem to be related to the presence of an inappropriate organizational climate. Team spirit is very much likely to suffer in organizational climates that are threatening and where management is aloof from daily operations. A total team commitment to quality patient care and the elimination of errors is unlikely unless management fosters a very

Table 4. Potential Problem Areas and Implications for Improvement Specific to Human-System Interfaces

Potential Problem Area	Implications for Improvement
As indicated in an NRC incident report, treatment planning files corresponding to older Co-60 sources have been used mistakenly for calculation of patients' treatments, resulting in incorrect doses to all patients treated with the invalid treatment planning file.	Departmental quality assurance efforts need to establish consistent procedures for maintaining consistency between changes or modifications on treatment machines or accessory devices that alter the beam and the parameter files in treatment planning computers that are used for exposure time calculations.
Treatment parameters entered initially into record and verify systems may contain errors—a situation where an initial error can go undetected and affect subsequent treatments.	Facilities using record and verify systems should ensure that a double check of initially entered parameters is performed before entering the first treatment.
Since it is easier to look at the monitor while setting up the treatment rather than the patient's chart, technologists rely extensively on the monitor. Failure to use the chart in setting up patients precludes detection of data entry errors in the R&V system as well as other errors.	Technologists should be discouraged from setting up treatment parameters solely on the basis of the displayed data on the R&V monitor in the treatment room.
Due to the lashback characteristic of the circular spring-loaded timing wheels on many Co-60 operator consoles, it is difficult to set treatment times as accurately as could be achieved using another type of device.	An acceptable after-market replacement, such as a digital input device, should be considered for circular clock treatment timers that demonstrate the lashback characteristic.
Therapists frequently react to the mechanical click sound made by the timer after the treatment time counts down to "0." Given a source reshielding failure, technologists may not respond to other cues (e.g., flashing red light over treatment room door, source status indicator display on control console) corresponding to the source being unshielded until excess time has elapsed.	Because technologists do not always notice the source indicator display on the control console or the radiation indicator light above the treatment room door, an audio alarm also should be considered. It would be activated whenever the timer counted down and the source remained exposed.

Table 5. Organizational and Managerial Factors Contributing to Human Error

- Staffing levels
- Reliability of equipment
- Threatening environment
- Management not in touch with daily operations
- Failure to ask questions
- Management setting the wrong organizational climate
- Lack of team spirit
- Assignment of wrong technologist to simulation
- Salaries not competitive with national average
- Complexity of cases
- Turnaround time in dosimetry
- Union-entrenched problem employees
- Uncooperative physicians/not available enough
- Schedules with too many patients per hour
- Use of only one qualified RTT

supportive climate. Assigning the wrong technologist to simulation is a personnel placement issue that has widespread implications for quality patient care. Also having an impact on patient care, but in a less obvious manner, is the department's salary structure which influences management's ability to attract highly qualified personnel. According to respondents, if management establishes a salary structure below the national average, it may be attracting less qualified personnel. Incompetent or problem employees that are protected by unions or other organizational systems are best addressed on an individual one-to-one counseling basis. Concerns about physicians that are unavailable or that lack effective communication skills are probably best addressed within the context of a comprehensive quality assurance (QA) program. Just as QA measures have been developed for the physical and clinical aspects of radiation oncology therapy, similar QA measures need to be devised for the human-to-human interfaces that occur or should occur. Table 6 summarizes a few of the potential problem areas associated with the organizational environment along with implications for improvement.

Management

Management as a contributing factor to human error is placed purposefully at the top of Figure 2 (introduced earlier) since it sets the stage and is ultimately responsible for all the other factors that follow. As Figure 2 shows, the third tier factors under the headings of physical environment, human-system interfaces, and organizational/social environment directly influence the nature of the work, and these different types of environments, in turn, are directly influenced

by management practices and decisions. Because of their dormant and delayed nature, errors attributable to management also are difficult to trace. Although typically not sufficient to cause system failures by themselves, managerial factors frequently play a necessary yet insidious role when combined with other unanticipated conditions in causing system failure. Reason's (1990) discussion of latent errors and system disasters (Three Mile Island, Bhopal, Challenger, Chernobyl, Zeebrugge and King's Cross underground fire) is very instructive in this regard.

Errors of poor planning, indecision or omission, made by managers and those in decision-making positions, are termed latent because they occur further upstream in the teletherapy setting, away from the front-line activities of the technologists. Decisions (or lack of decisions) are frequently made in a loose, diffuse, somewhat disorderly fashion. Because decision-making consequences accrue gradually over time, interact with other variables, and are not that easy to isolate and determine, those who make organizational policy, shape organizational culture, and implement managerial decisions are rarely held accountable for the consequences of their actions. Yet managerial dictum and organizational practices regarding staffing, communication, workload, patient scheduling, accessibility of personnel, and quality assurance procedures are sure to have their impact. As noted by Reason (1990), the front-line operators tend to be "the inheritors of system defects created by poor design, incorrect installation, faulty maintenance and bad management decisions" (p.173). Operators are actually the last line of defense (and probably the most vulnerable) for it is operators who have to contend with the sins of everyone else who has played a role in the design of the greater socio-technical system. For example, in this context the absence of a credible quality assurance program is a mistake spawned by management. The adverse consequences of ignoring the need for a quality assurance program may become apparent only when this managerial error of judgement interacts with other system variables such as excessive distractions, poorly designed user-system interfaces, low morale and a rapid paced production schedule for treating patients. Table 7 identifies some of the more relevant managerial problems uncovered in the present study.

6.0 CONCLUSION

It has been the contention of this paper that the dynamic quality of human error in radiation therapy that sometimes leads to serious misadministrations results frequently from a unique alignment of several necessary but singly insufficient factors. These factors have been discussed under the major headings of individual characteristics, nature of the work, physical environment, human-system interfaces, organizational/social environment, and management. For each of these areas, representative human factors issues and approaches for improvement have been identified. As with the accident causation research of other investigators (Reason, 1990; Sanders & Shaw, 1988), many of these factors are present in the radiation therapy environment long before the actual occurrence of an incident. Such a view is essentially optimistic, suggesting that something can be done about them.

Table 6. Potential Problem Areas and Implications for Improvement Specific to the Organizational/Social Environment

Potential Problem Area	Implications for Improvement
Differences in organizational climate are likely to have an impact on the self-reporting of errors. Technologists may withhold information on errors if punitive actions are perceived as the consequence. Errors not reported can not be compensated for in remaining treatments.	Departments should make a conscientious effort in fostering a supportive organizational climate based on openness, trust, team spirit and patient care rather than the assignment of individual blame. Organizations with climates conducive to the self-reporting of errors are more likely to understand the underlying conditions that give rise to error.
The accessibility of oncologists and physicists to respond to treatment-related questions that technologists have is an important organizational factor. When oncologists and physicists are not available, questions regarding treatments remain unanswered.	Oncologists and physicists need to ensure that their individual schedules include regular periods of time to respond to treatment-related questions. Issues regarding the accessibility of key personnel could be addressed in monthly quality assurance meetings that most departments have implemented.
Difficulty in terminating a problem employee because of union affiliation was considered a problem in a few departments.	Postponing the handling of problem employees does not help anybody. Other approaches such as counseling and employee assistance programs should be considered before formal procedures are initiated for termination.
Not enough attention is given to the various organizational factors (e.g., interpersonal conflict, rotation of therapists, understanding directions of oncologists, changes in treatment, rushed schedules) that serve to impede effective communication.	Because of the multi-disciplinary nature of teletherapy, failures of communication need to be addressed on a regular basis such as during weekly chart rounds or monthly quality assurance sessions.
Poor employee morale, lack of team spirit, staff's efforts not appreciated, and management not in touch with daily operations were a few of the organizational factors cited as contributing to human error. Patient treatment and care is likely to suffer if technologists (those with the greatest degree of contact with patients) perceive that their efforts are unappreciated.	Many technical professions are starting to realize the role that organizational factors play in contributing to their mission. Organizational climate was generally conducive to high quality treatment at the sites visited; however, structured continuing education programs and quality assurance directives are needed to educate that segment of the treatment staff not fully aware of the diverse effects of organizational factors.

Table 7. Potential Problem Areas and Implications for Improvement Specific to Management

Potential Problem Area	Implications for Improvement
It is not unusual for a single technologist to be assigned to a treatment machine despite "Blue Book" guidelines for two to be assigned. Such an arrangement increases the workload of the single technologist, reducing the likelihood of error checking and clarification of details during treatment set ups.	Further study is needed to determine the consequences of assigning single technologists to treatment machines. If the consequences are undesirable, further efforts are needed by professional societies to help ensure compliance with the guidelines.
In addition to being understaffed, technologists have little difficulty in identifying other conditions that contribute to workload and stress—high patient loads, getting behind schedule, machine downtime, complex treatments, and excessive duties.	Many of these conditions are driven by administrative policy and as such can be alleviated by a change in policy. Educational programs are proposed to help sensitize upper management of the relationship between workload and misadministrations.
There was considerable variation among the sites visited with respect to implementation of quality assurance programs. A number of sites did not show much evidence of a systematic commitment to quality assurance programs (Note: site visits were made before publication of NRC's regulatory guide on quality management programs).	The active commitment of upper management in departments of radiation oncology is a necessary condition for the effective implementation of quality assurance programs. Management needs to initiate and provide the continuing structure for such programs. Training for all treatment personnel in quality assurance processes should follow as well as periodic evaluations of the effectiveness of the program.
Some facilities have reduced the level of support to be provided by qualified physicists. Since physicists play the primary role in ensuring the appropriate physical characteristics of treatment and the proper functioning of equipment, potential for a corresponding reduction in accuracy of treatment and safety exists.	The support requirements for physicists need to be reviewed in teletherapy facilities of varying sizes. A determination is needed as to the appropriateness of "Blue Book" guidelines. If appropriate, alternative mechanisms for ensuring compliance need to be considered.
Some hospitals have difficulty recruiting and retaining well qualified therapists, dosimetrists, and physicists due primarily to their inability to offer wages that are commensurate with the national average.	A review of minimum standards for staffing and equipment at hospitals is needed. Identify existing deficiencies in relation to safety, error commission and quality of treatment. Pursue possibilities of providing hospitals with budgetary restrictions with the means of competing in the job market for well qualified personnel.

7.0 REFERENCES

Bainbridge, L., "The Ironies of Automation." In J. Rasmussen, K. Duncan & J. Leplat (Eds.), *New Technology and Human Error.* Chichester: John Wiley & Sons, pp. 23-30, 1987.

Harrigan, J.E., "Architecture and Interior Design." In G. Salvendy (Ed.), *The Handbook of Human Factors.* New York: John Wiley & Sons, pp. 742-764, 1987.

Headrick, H.W., "Macroergonomics: A Conceptual Model for Integrating Human Factors with Organizational Design." In O. Brown & H. W. Headrick (Eds.), *Human Factors in Organizational Design and Management.* Amsterdam: North Holland, 1986.

Henriksen, K., R. Kaye & R. Jones, *Human Factors Evaluation of Teletherapy: Volume IV Training and Organizational Analysis*, Falls Church, VA: CAE-Link Corporation, 1993.

Jacky, J.P., "Programmed for Disaster: Software Errors that Imperil Lives." *The Sciences*, 29, pp. 22-27, 1989.

Kartha, P.H.I., A. Chung-Bin, T. Wachtor & F.R. Hendrickson, "Accuracy in patient set-up and its consequence in dosimetry." *Medical Physics*, 2, p. 331, 1975.

Kaye, R., K. Henriksen, & R. Jones, *Human Factors Evaluation of Teletherapy: Volume II Function and Task Analysis.* Alexandria, VA: CAE-Link Corporation, 1991.

Leunens, G., J. Verstraete, W. Van den Bogaert, J. Van Dam, A. Dutreix & E. van der Schueren, "Human Errors in Data Transfer during the Preparation and Delivery of Radiation Treatment Affecting the Final Result: 'Garbage In, Garbage Out'." *Radiotherapy and Oncology*, 23, 217-222, 1992.

Mohan, R., K.C. Podmanoczky, R. Caley, A. Lapidus, & J.S. Laughlin, "A Computerized Record and Verify System for Radiation Treatments." *International Journal of Radiation Oncology•Biology•Physics*, 10, pp. 1975-1985, 1984.

Norman, D.A. & S.W. Draper, S.W. (Eds)., *User Centered System Design - New Perspectives On Human-Computer Interaction.* Hillsdale, NJ: Lawrence Erlbaum Associates, 1986.

Rasmussen, J., "The Definition of Human Error and a Taxonomy for Technical System Design." In J. Rasmussen, K. Duncan & J. Leplat (Eds.), *New Technology and Human Error*, Chichester: John Wiley & Sons, pp. 23-30, 1987.

Reason, J., *Human Error.* Cambridge: Cambridge University Press, 1990.

Report to the Director of the National Cancer Institute, National Institutes of Health, *Criteria for Radiation Oncology in Multidisciplinary Cancer Management.* Bethesda, MD, 1981.

Sanders, M.S. & B. Shaw, *Research to Determine the Contribution of System Factors in the Occurrence of Underground Injury Accidents.* Pittsburgh, PA: U.S. Bureau of Mines, 1988.

Swann-D'Emilia, B., J.C.H. Chu, & J. Daywalt, "Misadministration of Prescribed Radiation Dose." *Medical Dosimetry*, 15, pp. 185-191, 1990.

Weiner, E.L. & R.E. Curry, "Flight-deck Automation: Promises and Problems." *Ergonomics*, 23, pp. 995-1011, 1980.

Weinger, M.B. & C.E. Englund, "Ergonomic and Human Factors Affecting Anesthetic Vigilance and Monitoring Performance in the Operating Room Environment." *Anesthesiology*, 73, pp. 995-1021, 1990.

Weinhous, M.S., "Quality Assurance of Radiotherapy - Accelerator Computer-Control Systems." In G. Starkschall & J. Horton (Eds.), *Proceedings of an American College of Medical Physics Symposium.* Madison, WI: Medical Physics Publishing, pp. 45-60, 1991.

Human Error in Remote Afterloading Brachytherapy

Michael L. Quinn, Jim Callan, Isabelle Schoenfeld', Dennis Serig'

Pacific Science and Engineering Group, Inc.
6310 Greenwich Drive, Suite 200
San Diego, CA 92122 Phone (619) 535-1661

[†]U.S. Nuclear Regulatory Commission , Washington, DC 20555

ABSTRACT

Remote Afterloading Brachytherapy (RAB) is a medical process used in the treatment of cancer. RAB uses a computer-controlled device to remotely insert and remove radioactive sources close to a target (or tumor) in the body. Some RAB problems affecting the radiation dose to the patient have been reported and attributed to human error. To determine the root cause of human error in the RAB system, a human factors team visited 23 RAB treatment sites in the U.S. The team observed RAB treatment planning and delivery, interviewed RAB personnel, and performed walk-throughs, during which staff demonstrated the procedures and practices used in performing RAB tasks. Factors leading to human error in the RAB system were identified. The impact of those factors on the performance of RAB was then evaluated and prioritized in terms of safety significance. Finally, the project identified and evaluated alternative approaches for resolving the safety significant problems related to human error.

The views expressed in this paper are those of the authors and not necessarily those of the U.S. Nuclear Regulatory Commission.

INTRODUCTION

Brachytherapy (Greek: *brachy*, short range + *therapia*, medical treatment) is a cancer treatment process that uses radioactive materials ("sources") to retard or destroy tumors with ionizing radiation. Depending on the area to be treated, radioactive sources are placed within a body cavity adjacent to the tissue to be exposed (intracavitary or intraluminal), externally adjacent to the tissue to be exposed or directly into a tumor or surrounding tissue (interstitial). In general, brachytherapy sources are intended to be removed after the treatment area has received its prescribed dose of radiation.

Several methods for implanting and removing brachytherapy sources have evolved over the years. Manual brachytherapy originated in the early 1900s, shortly after the discovery of radium. In its earliest applications, radium was implanted directly into the tissue to be treated. Subsequently, treatment versions were developed using lower activity and shorter lived isotopes such as gold and cesium. More refined forms of manual brachytherapy then were developed in which sources were loaded into pre-positioned applicators. This approach, termed manual afterloading, reduced the radiation exposure of medical personnel during brachytherapy procedures. Nevertheless, there remained some occupational exposure to radiation during the manual loading and removal of sources and during nursing care.

In remote afterloading brachytherapy (RAB), a remotely controlled device inserts and withdraws the sources from source holders (catheters or applicators) that have been placed in a patient. RAB was developed in Europe during the 1960s and introduced to the United States 10–15 years later. RAB provides a greater degree of safety for medical and staff personnel because a remotely controlled device inserts and withdraws the source material. Medical and staff personnel remain outside a shielded treatment room. This report addresses RAB only.

Two types of RAB are currently practiced in the United States and are classified on the basis of the intensity of their sources: high dose rate (HDR) and low dose rate (LDR). HDR RAB uses a high activity (nominally 10 curies) source such as iridium-192 (^{192}Ir) to deliver a therapeutic absorbed dose of 500–1000 centiGray in 5–10 minutes. HDR treatments can be conducted on an outpatient basis due to their short treatment times. To enhance the biological effectiveness and patient tolerance of a HDR treatment, patients often receive the treatment dosage in 2–3 fractions separated by a few days.

LDR RAB uses lower activity sources consisting of cesium-137 pellets (^{137}Cs) or iridium wire of a few hundred milliCuries of activity, depending on the number of pellets or length of wire chosen. Low dose rate treatments are conducted using inpatient procedures that duplicate manual afterloading brachytherapy treatment times (2–3 days).

Purpose of the Project

Several misadministrations in remote afterloading brachytherapy (RAB) have been attributed to human error. A recent NRC study [Human Error in Remote Afterloading Brachytherapy NUREG/CR-6125] examined factors that contribute to human error in RAB. This paper reports on some of the results of that study.

Misadministrations are defined as radiation that is either:

- delivered to a patient from a source other than the one intended;
- delivered to the wrong patient;
- delivered by a route of administration other than that intended;

or which differs from the prescribed dose by more than 20% (U.S.N.R.C., July 1991).

Misadministrations are often attributed to human error. Their consequences can be severe. On November 21, 1992, a patient who had been treated with an RAB device died after the brachytherapy source was left in an implanted catheter following treatment. In the past five years, other patients being treated with RAB devices have received radiation doses which differed from the prescribed dose or which were administered to the wrong location. All the events involved "human error."

Accident reports often end with a finding that human error was the cause of some event. However, that finding may be only the first step in determining the actual root cause of the event. The purpose of this project was to identify factors (root causes) which contribute to errors in RAB systems, to evaluate the impact of those factors on the performance of functions and tasks essential to meet system goals, and to prioritize function and task performance problems related to human errors in terms of their safety significance. Beyond that, the project was designed to identify and evaluate alternative approaches for resolving safety significant problems related to human errors.

METHODS

This project consisted of an extensive human factors evaluation of remote afterloading brachytherapy. It involved three stages of data collection that focused on RAB functions and tasks, human–system interfaces, procedures and practices, training, and organizational factors.

Sampling Strategy

Since all facilities involved in RAB could not be visited, a representative sample of 23 RAB facilities was chosen for visits to collect data in the first five phases of the study. Two distributors of RAB devices and twenty three facilities using those devices were visited. Data were collected in three stages. During the first stage, the two distributors of RAB devices and a

sample of seven facilities using those devices were visited to collect data for a function and task analysis of the RAB process. During the second stage, another eight facilities were visited to identify and evaluate the human–system interfaces and the procedures and practices used in the RAB process. During the third and final stage of data collection, an additional eight facilities were visited to determine the training and organizational support provided for RAB.

Although organized into three data collection stages with different emphasis in each stage, relevant data for prior analyses were also collected as the study progressed to increase the data sample for those analyses. In particular, data collected on procedures and practices in the second stage were augmented with data collected in the third stage to provide a sample of 16 sites for that evaluation. Facilities were chosen by RAB device manufacturer, geographic region, dose rate, licensing authority, caseload, and RAB experience.

Data Collection

A comprehensive data collection protocol was devised prior to the site visits. In addition, several data collection tools were developed to allow human factors analysts to gather information about the characteristics of each medical facility (e.g., personnel employed, equipment used, training and organizational factors, and practices and procedures used during remote afterloading). Unique aspects of each facility were also noted. These included its physical layout, potential distractors, organizational and administrative structures, jobs performed by various categories of workers, and local organizational, training, and treatment goals. Emphasis, throughout, was on identifying factors that could lead to misadministrations or inadvertent staff exposure.

A typical site visit involved 2–3 project team members for 2–3 days. Data were collected from the following sources:

- Documentation supplied by the manufacturers and distributors of the remote afterloaders, including operating manuals, equipment specifications, training manuals, and journal articles;
- Documentation used on site by the people performing the RAB activities including user manuals, written procedures, checklists, or other written job performance aids;
- Interviews with afterloader distributors;
- Interviews with all available RAB personnel at each site including department chairs, radiation oncologists, nurses, medical physicists, radiation therapy technologists, dosimetrists, receptionists, and patient transporters. These interviews covered individual background and training information as well as discussion of local problems and practices;
- Direct observation and recording of various aspects of remote afterloading while they were being performed or demonstrated at each site;
- Directed walk-throughs in which staff were asked to perform their usual functions on simulated cases while being observed and questioned by members of the site visit team.

Analysis

Data collected during the site visits were analyzed after each visit to characterize the way in which the RAB system operated at the site. The data and evaluations of human performance and task requirements from each site were then combined and evaluated after each data collection stage to identify potential human errors in RAB and their consequences to the RAB process. This systematic approach to human factors analysis included the following six phases.

Phase 1 -RAB Functions and Tasks

Phase 1 was designed to characterize the RAB process and establish a framework for both data collection during Phases 2 through 5 and integration of findings during Phase 6. Following Phase 1 data collection, a comprehensive function and task analysis was conducted to identify the functions, tasks, and task steps performed by people in delivering RAB. The functions and tasks were analyzed and modified during subsequent project phases to provide a description of both the tasks performed by RAB staff and the performance requirements for each task.

Phase 2 - Human–System Interfaces

Data collected on workspaces, equipment, software, user manuals, control panels, and other human–systems interfaces at the sites were evaluated against relevant human factors engineering standards and guidelines. The evaluations concentrated on aspects of the workspaces in RAB facilities which could affect function and task performance and on the fundamental components of the interface (e.g., display size, button spacing, reach envelope). Deviations from relevant human factors engineering standards and guidelines were noted in detail.

Phase 3 - Procedures and Practices

In this phase, the procedures and practices used to perform the RAB functions and tasks were evaluated. The term 'procedure' has various meanings in human factors analysis, medicine, and training contexts. For this project a 'procedure' was defined as:

> Procedure: An ordered sequence of tasks or steps that has been designed, approved, and documented for some purpose.

The steps in the procedure must be documented in a form that permits its use as a reference for task performers and allows deviations from the approved sequence to be detected. Approval of such a procedure may be informal. There may be more than a single procedure approved for a particular purpose. In this project, 'practices' were defined as:

> Practice: Any ordered sequence of tasks or steps used repeatedly for some purpose. Practices may differ between individuals and may or may not conform to the approved sequence set out in a procedure.

Thus procedures and practices both govern the performance of tasks, but procedures are documented while practices are not. The analysis also identified the methods used to link the tasks together and the communications procedures used to pass information and material between the tasks.

Phase 4 - Training

In the fourth phase of the study, eight additional medical facilities were visi J to collect data on the training provided to the staff in the procedures and practices necessary to accomplish RAB. Information regarding training and qualifications was collected at each of the 23 sites. Data analysis concentrated on two areas:

(1) the training and qualifications of RAB staff, and

(2) the training programs and materials available to the RAB staff.

RAB training programs were evaluated against a model training system specified by the "systems approach to training". This model requires that training needs be defined, that training objectives be stated, that specific knowledge, skills, and abilities be identified, and that those requirements be addressed with training material and testing methods designed to meet specific learning objectives.

Phase 5 - Organizational Practices and Policies

Directed interviews with RAB administrators and task performers during Phase 5 covered the following organizational topics:

- Goals of the RAB program;
- Facilities and resources provided for RAB;
- Composition of the staff and their qualifications;
- Medical and administrative structures used to direct RAB task performers;
- Communications structure set up between task performers and administrators;
- Methods used to allocate RAB tasks to staff and evaluate their performance;
- Training provided and required for RAB staff;
- Employee motivation methods used at the site;
- Workplace safety monitoring performed at the site;
- Methods used to report and resolve safety problems at the site.

Since production, approval, and communication of procedures is an important organizational function, the person responsible for the definition and communication of procedures for performing each RAB task was interviewed (when available) regarding:

- Task performance procedures that were being used for each task;
- Problems that had been considered in designing the task performance procedures;
- Linkage and verification procedures designed for the RAB tasks;
- Methods used to monitor conformance with procedures.

Phase 6—Identification of Areas for Recommended NRC or Industry Action

Phase 6 was designed to build upon information gained during the first five phases of the project to accomplish four objectives:

(1) Identify the factors which can contribute to human error in RAB;

(2) Evaluate the impact of these factors both singly and in combination, on the performance of the functions and tasks essential to meet RAB goals;

(3) Prioritize function and task performance problems related to human errors caused by those factors in terms of their safety significance;

(4) Identify and evaluate alternative approaches for resolving safety significant problems related to human error.

Factors contributing to human error in RAB

Data collected in each of the previous phases were evaluated during Phase 6 to help identify factors which could contribute to human error in RAB. These factors included the demands placed on staff during task performance, the interfaces used by staff to perform those tasks, the procedures and practices used in task performance, and the training, feedback, and organizational support provided for staff to enable them to assess, improve, and correct their performance.

Demands Placed on Staff During Task Performance

The demands placed upon a person performing each RAB task were identified and evaluated to determine the mental and physical effort required to perform the task, and the time pressure and stress reported by staff during task performance. Potential human errors in the performance of each step were identified and the likelihood of such an error was estimated.

Human–System Interfaces

Interfaces were evaluated for their adherence to human factors guidelines and for the way in which they supported the performance requirements of each function and task. Potential errors due to inadequate interfaces were identified. The feedback provided to staff to allow them to detect interfacing errors was then identified and evaluated.

Task Linkage Procedures and Practices

Procedures and practices used to carry information and material between tasks, workstations, and individuals were evaluated so that potential linkage errors could be identified. The information required to detect these linkage errors was determined, and the practices used to correct the errors and to address their consequences were evaluated.

Staff Training and Organizational Support for RAB

Data on training and organizational support for RAB were used to identify the effect on the RAB system of factors related to the way in which tasks were allocated to staff, workspaces and equipment were provided and maintained, and procedures were designed to support, monitor, and control the performance of the RAB tasks. Methods used by RAB facilities to assess staff performance, and methods used to provide and assess training in task performance, task linkage, and QA procedures were also evaluated.

Evaluation of the Impact of Factors Contributing to Error on RAB

The impact of each of these factors was evaluated to identify the impact of human error on the safety and efficacy of the RAB system. Data from misadministrations were evaluated to identify documented effects of human error on RAB. A conceptual model of the RAB process was then designed to evaluate the impact of errors and problems which might not yet have been associated with misadministrations.

Misadministration Data

Misadministration and problem data from the following sources were reviewed to identify the impact of human error on RAB.

- U.S. Nuclear Regulatory Commission, Office for Analysis and Evaluation of Operational Data (NUREG 1272): 1982–1991;
- Radiological Health Bulletin, FDA Center for Devices and Radiological Health: August 1989–June 1991;
- Medical Devices Bulletin, FDA Center for Devices and Radiological Health: August 1989–June 1991;
- Medical Device Problem Reporting Program, FDA Center for Devices and Radiological Health.

Conceptual Model

A conceptual model of the RAB process was developed to evaluate the impact of latent errors (i.e. those which had net yet resulted in misadministrations) on RAB. The model linked RAB functions and tasks together by specifying the order in which tasks were performed and the linkages between the tasks. The conceptual model was then used both to describe different RAB treatment delivery systems and to analyze the mechanisms for the propagation of error consequences in those systems.

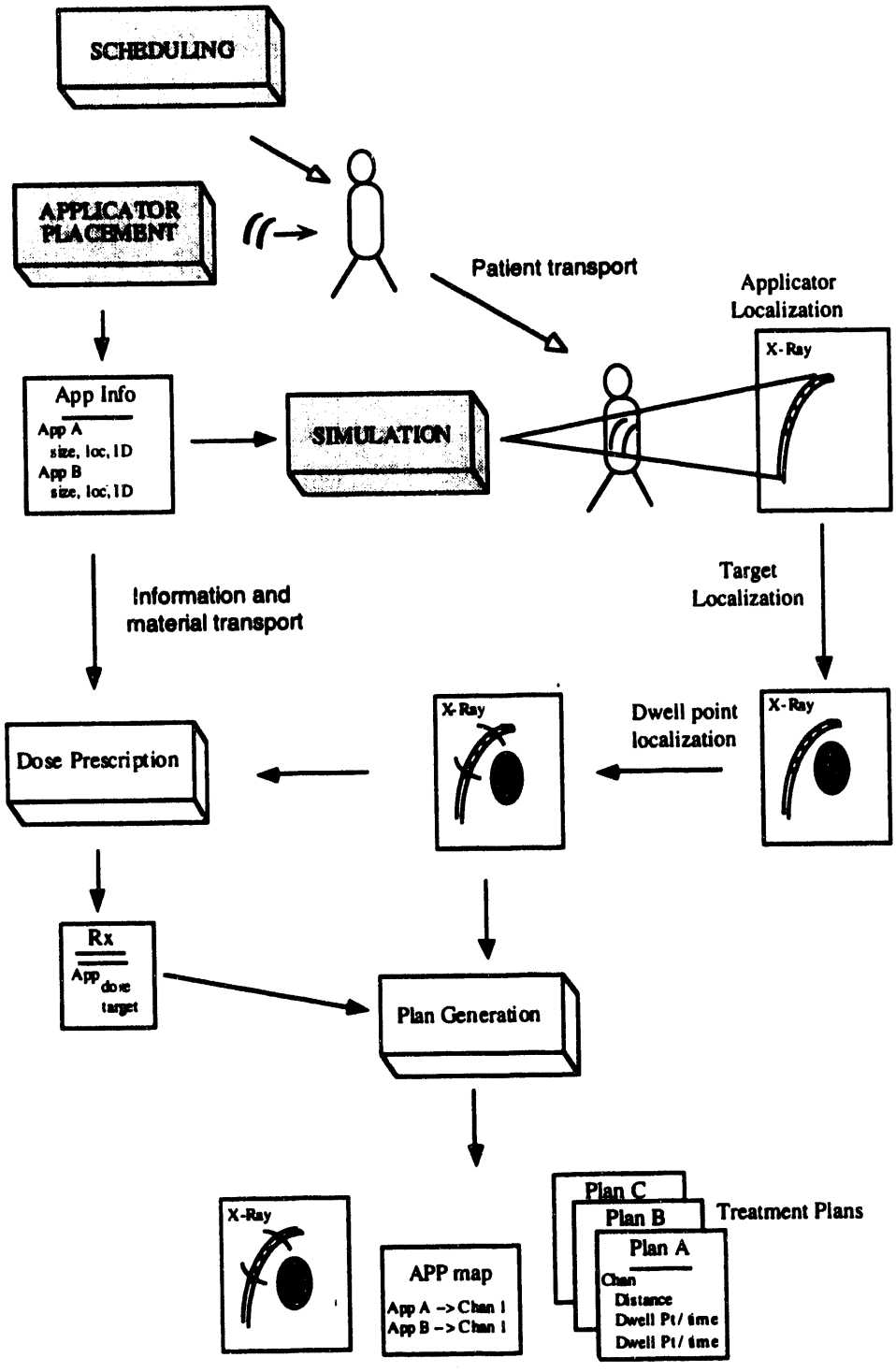
The following figure shows some of the elements in the conceptual model for treatment planning in which applicators are placed in a patient and then information on the position of the applicators is acquired from simulation x-ray negatives. That information is then used to plan where sources will be placed to deliver a prescribed dose of radiation to a target in a patient's body.

The impact of various factors on RAB system performance was estimated by analyzing the way in which each factor could affect other elements of the conceptual model. The errors which could occur in different systems were identified. The methods needed to detect each error and to limit its consequences were determined.

Error Detection and Correction Analysis

The conceptual model was then used to determine the information that would be needed to detect and correct potential errors at different stages of the RAB treatment delivery process. The procedures collected at each site were then used to determine whether that information was transferred from task to task so that it would be available for verification of task performance and task linkages. If either no information was provided to allow an error to be detected, or no detection procedure was specified for a particular transfer point, the consequences of the error could propagate through the model into subsequent tasks.

The conceptual model was also used to evaluate error correction in RAB. Once an error is detected, additional information is usually needed to correct the error. For example, lack of a label can be detected easily, but more information is required to determine the missing label's contents. As with error detection, the information needed to correct errors in task performance or task linkage must be carried by the system to the place at which it is needed. Once the information required to correct potential task performance or task linkage errors was identified, the conceptual model was used to determine whether that information would be likely to be preserved and utilized.



A conceptual model of the flow of information during treatment planning

Identification of Safety Significant Problems

Safety significant problems were defined as those weaknesses or deficiencies in human–system interfaces, procedures, practices, training, or organizational support that could result in task performance or task linkage errors whose consequences could propagate through the system and cause unintended radiation exposure to the patient or the RAB staff.

Safety significant human factors problems were identified by a focus group composed of ten subject matter experts (SMEs) on RAB and human factors. The SMEs included a physician/physicist, a physicist, a dosimetrist, specialists in training and organizational procedures, and the five members of the site visit teams

The group reviewed errors, potential errors and tasks susceptible to error using the function and task analysis as a guide. Errors were classified and characterized by detectability, frequency, likelihood, and consequence.

The conceptual model was used to identify all incidents in which human errors in task performance or task linkage could lead to inappropriate radiation exposure of the patient or staff. These included incidents which might not be detected by current QA practices as well as those which would be reported as misadministrations or reportable events under current reporting guidelines. Problems unrelated to radiation exposure and those which had no human task performance components (e.g., unexpected equipment failures) were not evaluated in this study.

Prioritization of Error Consequences

A second meeting of the SMEs was used to review and discuss the contributions to critical task performance and error significance of: human–system interfaces, procedures and practices, training and qualifications, and organizational practices and policies.

The SMEs were asked to identify critical tasks in which a performance error was likely to result in a misadministration or other undesirable consequence to the patient or staff. The SMEs used their own mental models of the RAB process to gauge and assess the effects of task performance and linkage errors on the system. The potential contributions from each area were discussed and prioritized.

Identification of Alternative Approaches for Resolving Safety Significant Problems

Each task or linkage in which an error could propagate through the system to cause a safety significant problem was analyzed to determine modifications to human system interfaces, procedures, training, or organizational policies that would reduce the likelihood of error or which would make errors easier to detect and correct. Alternatives to current practice were formulated and evaluated for their effect on RAB and their utility in reducing human error and its consequences during the RAB process.

RESULTS

Phases 1-5 of the study were data collection and analysis efforts designed to characterize the RAB system as it currently exists. Phase 6 assessed the impact of aggregated Phase 1-5 results on RAB task performance and prioritized potential errors in terms of their safety significance. Phase 6 also identified and evaluated alternative approaches for resolving safety significant problems related to human error in RAB. Some of the findings of these analyses are discussed below.

Phase 1 provided a comprehensive analysis of the functions, tasks, and task steps performed in RAB. This analysis characterized RAB as a process in which staff perform major functions corresponding to discrete stages in the planning, organization and delivery of a single RAB treatment. The findings of the misadministration analysis were confirmed by the preliminary error analysis conducted during the site visits. Brachytherapy personnel cited treatment planning as the most difficult function, rated it highest in workload characteristics—time pressure, mental effort, and stress—and reported that they were most susceptible to distraction during treatment planning. RAB experts also rated treatment planning tasks with the greatest number of medium and high error likelihood scores.

Phase 2 evaluated the human–system interfaces used by RAB staff to perform the RAB functions and tasks. Although most equipment interfaces for RAB were found to conform to engineering guidelines, staff were not familiar with infrequently used interfaces and operators' views of essential displays and controls were often obscured. Feedback on interface performance and system status was not always available to users of the equipment, or when provided, was difficult to understand.

Phase 3 evaluated the procedures and practices used to perform the RAB tasks. This analysis also identified the methods used to link the tasks together and the communications procedures used to pass information and material between the tasks. Very few sites used written procedures to guide RAB task performance. Practices used to verify human performance frequently failed to address important error possibilities . Information needed to perform verifications and to identify and correct the consequences of errors was often not transferred between tasks.

Phase 4 evaluated the training that the RAB staff received in RAB procedures and practices. Most sites had no systematic training program for RAB staff. Training in RAB was usually performed either on-the-job with initial supervision but without a statement of training objectives or formal evaluation of training efficacy.

Phase 5 evaluated the organizational support provided for RAB at each site. Eight organizational functions related to RAB system performance were identified. These functions included definition of goals, design of procedures for communications and task performance, and supervisory monitoring of the performance of the RAB system. Potential problems were identified in the allocation of tasks to RAB staff, in the procedures used to communicate goals and information, and in the methods used to monitor and control the RAB process.

Phase 6 used the information from the prior five phases to build a conceptual model of the RAB process and to identify opportunities for human error in planning and delivering RAB treatments. Ten critical tasks were identified in which a performance or linkage error was likely to result in a misadministration or other undesirable consequence to the patient or staff. Those critical tasks, and the alternatives that were identified in Phase 6 to address factors contributing to human error in the critical tasks are presented below.

Critical Tasks

Critical Task 1: Patient Scheduling, Identification, and Tracking

This task involves the initial identification of the patient and any re-identification that is required as the patient and his records are moved through the RAB system. Errors in these tasks include scheduling the patient for the wrong treatment, bringing the patient to the wrong treatment area, or delivery of treatment to the wrong patient due to misidentification of the patient or the patient's records at some point during the treatment procedure.

Critical Task 2: Applicator Selection, Placement, and Stabilization

This task requires that applicators be selected, placed near a target in the body, and secured to prevent movement after placement. Information on the characteristics of the applicator (e.g., diameter, length) and applicator placement must be transmitted to the treatment planners and to the staff performing applicator connections. Errors in this task include failure to place the applicator so that the desired dose can be delivered to the targets, failure to stabilize the applicator after placement, or failure to transfer accurate information on placement distances and applicator characteristics to other tasks.

Critical Task 3: Target Volume Localization

This task involves identification and specification of the volume that is to be irradiated during treatment. Errors in this task include failure to identify targets, or failure to specify an accurate position and volume for each target that will be irradiated during treatment.

Critical Task 4: Dwell Position Localization

This task involves identification, specification and communication of the positions that sources will occupy in the applicator during treatment. Errors in performing this task include incorrect identification, specification, or transfer of information on the source positions.

Critical Task 5: Dosimetry

This task involves calculation of the dose distribution due to sources placed at specified dwell positions for specified times. Errors in dosimetry include failure to calculate the dose accurately or failure to describe the dose that will be received by each target from sources placed at the dwell positions. Errors in the specification of the target locations or dwell

positions, in the strength of the source, in the specification of the dwell times at the dwell positions, in the calculation of the dose distribution due to the source placements, or in matching the dose distribution to the targets may also occur.

Critical Task 6: Treatment Set-Up

This task involves connection of the patient to the afterloading treatment unit. Errors in treatment set-up include swapping two or more treatment channels so that treatment planned for one applicator will be delivered through another, connection of improper guide tubes so that the planned treatment distance does not correspond to the planned dwell positions, or modification of the spatial relationship between the applicator and the targets so that the dose distribution does not hit its planned targets.

Critical Task 7: Treatment Plan Entry

This task involves transfer of treatment parameters from the treatment plan to the treatment unit. Errors in treatment plan entry include either the use of different values from those contained in the treatment plan or entry of treatment plan values from the wrong treatment plan for the intended treatment.

Critical Task 8: Routine QA and Maintenance

QA in RAB involves testing equipment and procedures to identify malfunctions or potential problems before they adversely affect treatment planning, treatment delivery or patient or staff safety. Maintenance involves changes to equipment or procedures designed to prevent or eliminate either potential or actual problems. Errors in QA and maintenance include either failures to detect, deal with, or communicate problems in equipment, procedures, and treatment delivery mechanisms or the creation of problems in these areas during the performance of the QA or maintenance procedures.

Critical Task 9: Source Exchange

Source exchange involves the scheduled replacement of radioactive sources. Errors in source replacement can result in inadvertent exposure of staff to the source during the replacement procedure, or produce changes in afterloading equipment that can cause problems in source positioning accuracy, equipment integrity, or treatment delivery.

Critical Task 10: Source Calibration

Source calibration involves the measurement of the characteristics of a radioactive source and transfer of that information to other RAB tasks. Source calibration errors include either failure to measure the activity of a radioactive source accurately or failure to transmit the appropriate calibration information.

Alternative Approaches

Once potential errors in critical tasks were identified, alternative approaches involving modifications to equipment, interfaces, procedures, training, and organizational support for RAB were identified and evaluated. The alternatives were designed to meet the following objectives:

- to decrease the likelihood that errors would occur;
- to improve the chances that errors would be detected after they had occurred;
- to block the propagation of error consequences;
- to limit the impact of any consequences which do propagate through the system.

Some of the alternatives that met one or more of these objectives are listed below for each of the modification categories.

Human–Systems Interface and Equipment Modifications

Modifications designed to improve some of the interfaces between humans and the RAB equipment require additional support from equipment manufacturers, software vendors, and the research community . These alternatives include:

- Tag readers for patient ID tags;
- Automatic comparison of patient and treatment plan IDs;
- Permanent labels on applicators that might be misidentified;
- Applicator stabilization aids;
- Digitization aids (e.g., scanners and target superimposition aids);
- Improved feedback and visualization aids for treatment planners;
- Unambiguous data entry formats;
- Dwell positions referenced to the applicator instead of the treatment unit;
- Pre-treatment dose estimation based on treatment plan parameters;
- Direct calibration chambers for RAB sources;
- Improved access to emergency source containment safes;
- Automatic calibration while the source is in its stored position;
- Source position sensors (minimum would detect a source in the safe);
- Measurement of dose delivered (to some reference volume) during treatment;
- Performance certification packages for software and hardware.

Other alternatives involve the provision of job performance aids to staff, and changes in procedures, training, and the organizational support that is provided for RAB. Many of these alternatives do not require support from equipment manufacturers and could be implemented immediately to help prevent human error in RAB or to address its consequences.

Job Performance Aids

- Highly visible identification tags that can be attached to the patient and all the patient's documents;
- Radio-opaque identification labels that can be attached to applicators;
- An applicator–channel map;
- QA checklists that highlight failed or omitted checks;
- Visualization aids for treatment planning.

Procedure Modifications

- Tagging procedures for the patient and his documents;
- Use of an applicator–channel map for treatment planning and treatment setup;
- Standardization of dosage units;
- Target marking in simulation views (when applicable);
- Minimization of patient movement between simulation and treatment;
- Erasure of magnetic media used to transfer treatment plans.
- Multiple source calibrations.

Training Modifications

- Integration of QA with refresher training in emergency and planning procedures;
- Training in local task performance and linkage procedures;
- Training in error detection and allocation of error detection duties.

Organizational Support Modifications

- A multi-tiered quality assurance program stressing early error detection;
- Identification of error opportunities;
- Display of information needed for error detection to all staff;
- Communication procedures that pass redundant information needed for error correction;
- Verification of task linkages prior to treatment;
- Certification of all RAB equipment and software after maintenance;
- Monitoring the efficacy of procedures and training in preventing errors;
- Monitoring the efficacy of RAB error detection and correction.

DISCUSSION

The goal of human factors problem resolution is to eliminate mismatches between what a system requires of people and what those people can be reasonably expected to do. One approach to meeting that goal is to modify the system to eliminate the human task or to reallocate that task to non-human elements of the system which might perform it more reliably (e.g., electronic collection and transfer of data rather than repeated keyboard entry of that data reduces one type of opportunity for human error). Such an approach is necessary when neither the performance required of people in the system nor the performance capabilities of those people can be sufficiently modified to eliminate the mismatch. Even in cases where it is not necessary, it may be preferred.

Other approaches to eliminating mismatches involve modifying the system to reduce human performance requirements or to enhance human performance capabilities. Modifying human–system interfaces to make things which support adequate task performance both available and suitable for the intended use tend to reduce human performance requirements. Modification of task specific procedures and of organizational policies and practices can also reduce human performance requirements. Modifying training or selection qualifications can improve the performance capabilities of people within the system.

A system can be considered robust with regard to human error if the consequences of a human error either cannot effect system performance, or will be detected and corrected by the system or its users before the system's output is degraded. The alternatives suggested above address these goals by decreasing the likelihood of some errors and then making the consequences of the others easier to detect and correct

Decreasing the Likelihood of Human Error

In the combination of approaches suggested above, some human–system interfaces are modified (e.g., direct indication that a radioactive source has returned to its storage position is provided). Procedures must then be developed to use those interfaces, and training must be designed to familiarize staff with the new interfaces and procedures.

Increasing the Detectability of Human Error

Elimination of mismatches between the human performance requirements of a system and what humans working within that system can reasonably be expected to do is not always possible. In such cases, the goal of the human factors problem resolution process is to reduce the impact of the human factors problems. The alternatives which allow early detection and correction of a human error would lessen or eliminate the consequences of those problems.

The ease with which errors are detected and the delay between occurrence and detection determine the effect that errors will have on system performance. An ideal system would be one in which errors are difficult to commit, easy to detect, and which was robust enough to allow recovery from error consequences. Unfortunately, many human errors in RAB are difficult to detect. Thus, major safety gains can be expected from an increase in error detectability. The suggested changes in the human–system interfaces, procedures, training, or organizational practices and policies would increase the chance of detecting errors.

Improving the Timing of Error Detection

If errors in task performance can be detected as the task performer completes a step of the task, the error can often be corrected at that time before it affects system performance. Immediate error detection requires three things:

(1) feedback from the system on the results of the latest step

(2) the expected result

(3) a method to compare the feedback with the expected result

Temporal contiguity with task performance is desirable since an error detected long after a task is completed may require many other tasks, each with its own sequence of steps, to be examined before the locus of the error can be identified. Just as the cost of error correction may rise as detection time increases, the number of things which can be corrected may be reduced. Immediate detection may allow the error itself to be corrected and system performance to continue undegraded. Less prompt detection may permit damage control to mitigate error consequences. Late detection may only allow correction for future operations or, in the worst case, no correction at all.

Improving the Allocation of Error Detection Tasks

If task performers are already burdened to the point that performance errors are likely, the addition of error detection tasks to their workload may increase the potential for performance decrement. Ideally, errors should be obvious to task performers with little or no additional effort expended in error detection. The additional effort can be reduced by providing procedures and training that facilitate error detection, or by allocating the detection of errors to other staff. The burden on task performers can be substantially reduced if hardware and software are allocated the function of detecting task performance errors as they occur and providing timely feedback.

Limiting the Consequences of Human Error

Detection of an error does not of itself guarantee that the error will be corrected or that its consequences will be limited. The consequences of an error depend on when the error is detected, and on what can be done to correct the error and block its effects.

If task performance or linkage errors can be detected before the consequences propagate to another part of the system, degradation of system performance can be limited or prevented. In many cases, a task or linkage can be repeated with only minimal effect on system performance and safety.

Errors which remain undetected make no immediate demands on the system, although they may have undesirable consequences and degrade system performance. Once an error is detected, degradation of system performance can be limited by correcting the error and taking actions to reverse its consequences. Damage control after an error is detected places an additional burden on staff since it requires that any propagating consequences of the error be identified and prevented from compromising other parts of the system.

Quality Assurance

One aspect of quality assurance involves additional procedures that are performed to prevent errors, to detect errors and their consequences, and to prevent those consequences from degrading system performance. A multi-tiered QA program involves steps designed to accomplish these goals sequentially so that each possible error is defined, then steps are designed to prevent as many errors as possible, other steps are designed to detect any errors which were not prevented, and further steps are designed to deal with the consequences of errors after they have been detected.

CONCLUSIONS

Taken together, HSI modifications, job performance aids, procedure modifications, and training modifications could reduce the likelihood of errors in most of the critical tasks. The hardware modifications could also reduce the burden on staff by automatically performing some of the currently difficult procedures, automating error-prone linkages, and providing needed feedback to staff on their performance and on system integrity. The remaining organizational modifications could improve quality assurance and increase the opportunity for detecting and correcting human errors.

These modifications would eliminate many existing opportunities for human error. They would also improve safety by making errors easier to detect, and by providing staff with the information they need to identify and address the consequences of error in the RAB process.

REFERENCES

Handbook of Human Factors, Gavriel Salvendy (Ed), Wiley-Interscience, New York 1987

M.L. Quinn, I. Schoenfeld, D. Serig, Remote Afterloading Brachytherapy: Human Factors in a Partially-Automated Treatment System, in Computer-Based Medical Systems, IEEE Computer Society Press, Los Alamitos CA, 1993

U.S. Nuclear Regulatory Commission, "Analysis and Evaluation of Operational Data, Annual Report," NUREG-1272, (1981-1992).

U.S. Nuclear Regulatory Commission, "Report to Congress on Abnormal Occurrences," NUREG-0090, (1990-1992).

U.S. Nuclear Regulatory Commission, "Quality Management Program and Misadministrations (10 CFR Parts 2, 19, 20, and 35)," Federal Register, Vol. 56, No. 143, July 25, 1991.

U.S. Nuclear Regulatory Commission, "Human Error in Remote Afterloading Brachytherapy," NUREG/CR-6125, (In Press).

Human Factors Issues in Severe Accident Management: Training for Decision-Making under Stress[1]

Randall J. Mumaw, Emilie M. Roth
Westinghouse Science and Technology Center
Pittsburgh, PA

and
Isabelle Schoenfeld
U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, DC

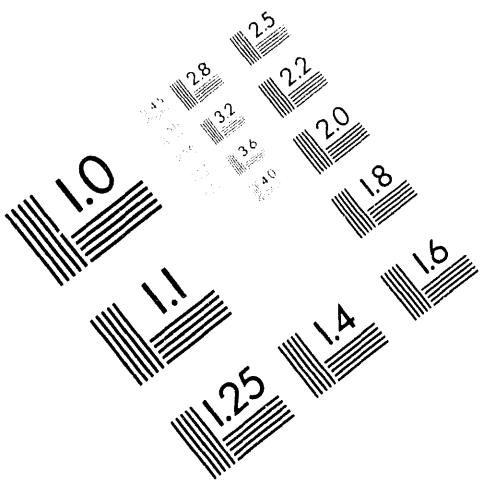
Abstract

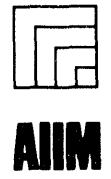
Training for operator and other technical positions in the commercial nuclear power industry traditionally has focused on mastery of the formal procedures used to control plant systems and processes. However, there is a growing awareness that the decision-making tasks required for selecting appropriate control actions, in addition to guidance from formal procedures, also involve cognitive activities commonly referred to as judgment or reasoning. A project was completed to address the nature of the cognitive skills that may be important to decision-making in the nuclear power plant environment, especially during severe accident management. The project identified a model of decision-making that could account for both rule-based and knowledge-based decision-making and used it to identify cognitive skills for both individuals and operational crews. This analysis was then used to identify existing training techniques for cognitive skills and the general characteristics of successful training techniques.

Introduction

Training for operator and other technical positions in the nuclear power industry traditionally has focused on mastery of the formal procedures used to control plant systems and processes. However, there is a growing awareness--e.g., a recent report from the NRC's Office for Analysis and Evaluation of Operational Data (Kauffman et al., 1992)--that the decision-making tasks required for selecting appropriate control actions also involve cognitive activities, commonly referred to as judgment or reasoning. The need for cognitive skills is especially clear in situations where formal procedures may not exist or may not be as detailed, as is the case in severe accident management (SAM). Decision-making under SAM conditions may differ from that which is expected during anticipated abnormal operations. Specifically, there are two critical elements to this type of decision-making that set it apart from decision-making during normal and abnormal situations: the need for cognitive skills due to less prescriptive guidance, and the high likelihood of excessive stress. Therefore, training that addresses decision-making

[1] The views expressed in this paper are the authors' and not necessarily those of the U.S. Nuclear Regulatory Commission. This paper reports on results of research initiated prior to commercial nuclear industry groups taking the lead in the development of severe accident management guidelines.

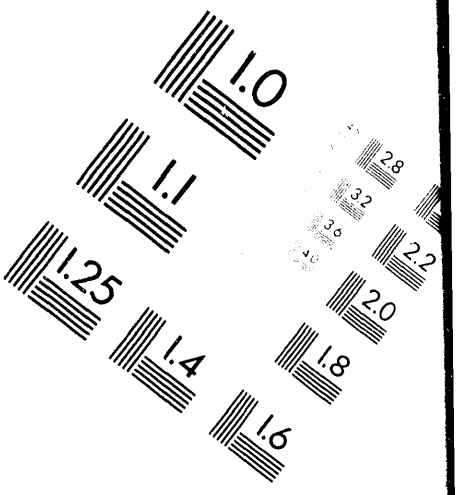


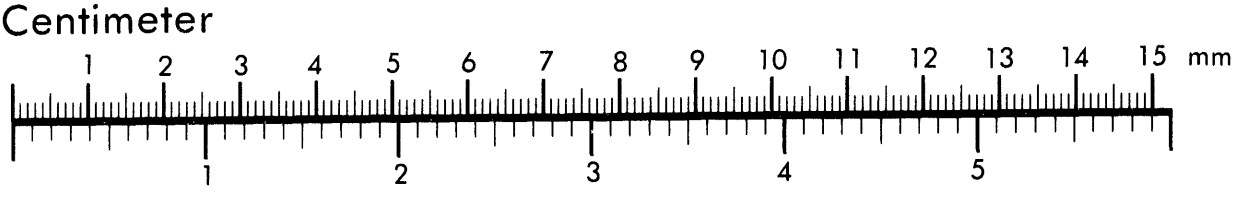


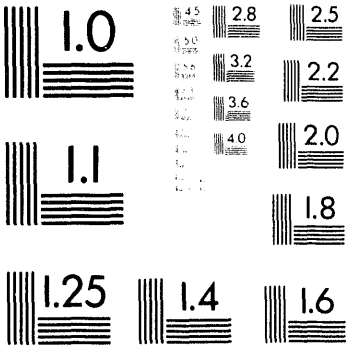
Association for Information and Image Management

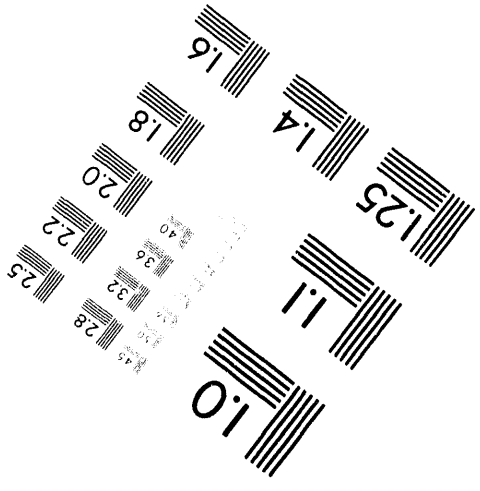
1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910

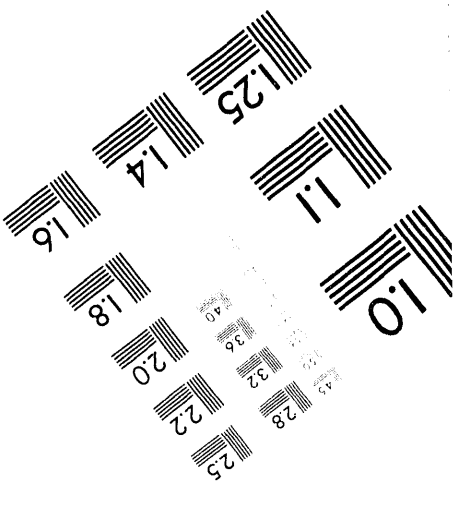
301/587-8202











MANUFACTURED TO AIIM STANDARDS
BY APPLIED IMAGE, INC.

4 of 7

under severe accident situations may be a viable means of improving the effectiveness and reliability of human performance under such conditions.

This paper summarizes the work conducted by Westinghouse Science & Technology Center for the NRC. The project accomplished the following objectives:

- Developed a model of decision-making under SAM conditions.
- Developed 12 SAM scenarios (six PWR and six BWR).
- Identified cognitive skills for each component of the decision-making model, both at the individual and crew levels.
- Reviewed and assessed existing approaches to training cognitive skills to determine the set of characteristics most desirable for cognitive skill training.
- Identified potential sources of stress in SAM and the ways in which that stress is likely to affect cognitive task performance.
- Reviewed and assessed approaches to training that are likely to reduce the effects of stress.

The ideal approach for identifying specific cognitive skills associated with SAM decision-making is to conduct a cognitive task analysis. However, performing an extensive task analysis requires starting with a well-defined job and/or access to practitioners of that job. In the case of SAM decision-making, the job is not yet well defined--that is, job functions or task-subtask hierarchies have not yet been developed. Therefore, a more analytic (i.e., less empirical) approach to identifying the cognitive skills required for nuclear power plant (NPP) decision-making was developed. This approach, illustrated in Figure 1, used as a starting point a model of decision-making, borrowed from Rasmussen (1986), that has been widely applied to NPP operations. This model was modified to capture performance in both standard procedure-guided (primarily rule-based) decision-making (normal and emergency operations) and SAM decision-making, which has a greater likelihood to be knowledge-based.

The model was used to identify cognitive skills. This was accomplished by applying two perspectives on performance to the model. The first perspective brought to bear analyses of skilled performance. In other words, what are the cognitive skills required to perform NPP decision-making tasks? The second perspective applied to the model was a consideration of the factors that can impair skilled performance. The limitations and biases inherent in human cognition and the effects of the stress associated with the NPP setting have the potential to impair performance in NPP decision-making. Therefore, training may need to focus on cognitive skills that mitigate these factors, or training may be needed to make these cognitive skills less susceptible to the deleterious effects of these factors.

Decision-Making Model

The term decision-making refers to the full set of activities required to select and execute appropriate actions in the control room setting. Unlike other domains in which easily isolated decision-making events are defined (e.g., friend/ foe, fire/ don't fire, pick strategy A/ strategy B) or stable alternatives are offered, nuclear power plant control presents a dynamic situation that evolves over time and requires on-going assessment. An emergency or severe accident event can stretch over minutes, hours, or even days before the plant is restored to a safe and stable state. During the course of the event, the operators may determine that plant state has changed significantly and that their current control efforts are no longer appropriate. Hence, they would need to rely more on their decision-making skills. Thus, the model of decision-making represents an iterative cycle that includes nearly all operator activities.

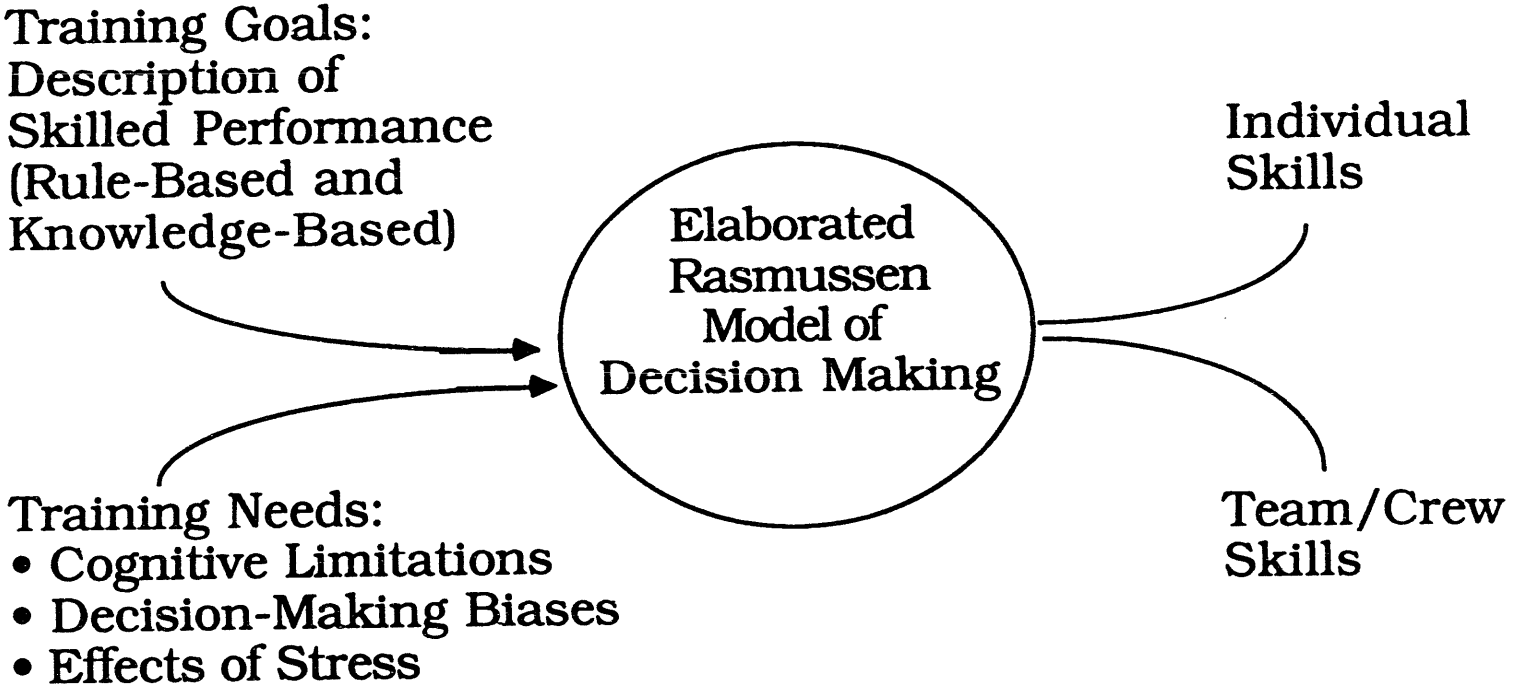


Figure 1. Schematic of the analytic approach to the identification of cognitive skills.

A formal decision-making model, initially proposed by Rasmussen (1986) has been widely adopted in the industry. Figure 2 shows a generic form based on Rasmussen's model, which includes six general processes needed for SAM. Table 1 provides definitions of these six processes.

Table 1. The six processes in the decision-making model.

1. **Monitor / Detect** - Active (monitor) and passive (detect) means for acquiring data about plant state. Sources of data are alarms, indicators, CRT displays, other individuals, etc.
2. **Interpret Current State** - The development of a mental representation of plant status. This representation captures the inferences drawn from plant state indications; it may include interpretations concerning faults, causes of abnormal symptoms, or it may be only a prioritized list of symptoms (e.g., safety violations).
3. **Determine Implications** - The determination of how the current plant state will progress (e.g., potential consequences, side effects). Also, a set of goals is defined in which more important goals are given higher priority and complex goals may be broken down into subgoals.
4. **Plan** - The selection of a response plan, which in most cases is a formal procedure from the EOPs, but may also be a high-level description of some control action that addresses the goal with the highest priority. Operators must understand the intent of procedures.
5. **Control** - The coordination and execution of a specific sequence of control actions.
6. **Feedback** - The information gained from control actions that is used to update understanding.

Figure 3 shows an expanded version of this model created to make explicit certain aspects of performance. Note that this model is not intended to be a detailed cognitive process model that could be converted to a computer simulation of decision-making (although this form of modeling was done in another project; see Roth, Woods, & Pople, 1992). Instead, Figure 3 is intended to be a representation of the critical decision-making processes required by nuclear power plant operators and technical support personnel. The identification of these processes brings to bear what cognitive psychologists have discovered about each process so that the knowledge and skills that may be required for skilled performance and the sources of error that are likely during an emergency or severe accident management (SAM) condition may be identified (see NUREG/CR-6126 for a more detailed description of this model).

Analysis of Severe Accident Management Scenarios in the Context of the Model

Generally, a severe accident is defined as one that involves overheating of the core beyond the plant's design basis. SAM-specific guidelines, which are similar to procedures but less detailed, are currently being developed by the nuclear power industry and are likely to reflect several changes in operations. For many utilities, the control room staff will be supported by engineering personnel in the Technical Support Center (TSC), which is staffed in the event of a serious emergency. This means that decision-making authority may be shared between or transferred from the control room and the TSC. Also, SAM guidelines are likely to be less

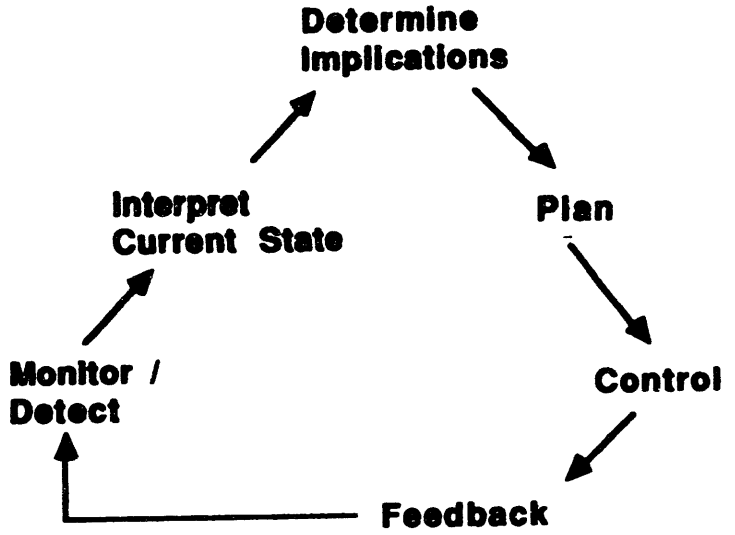


Figure 2. Generic form of the decision-making model.

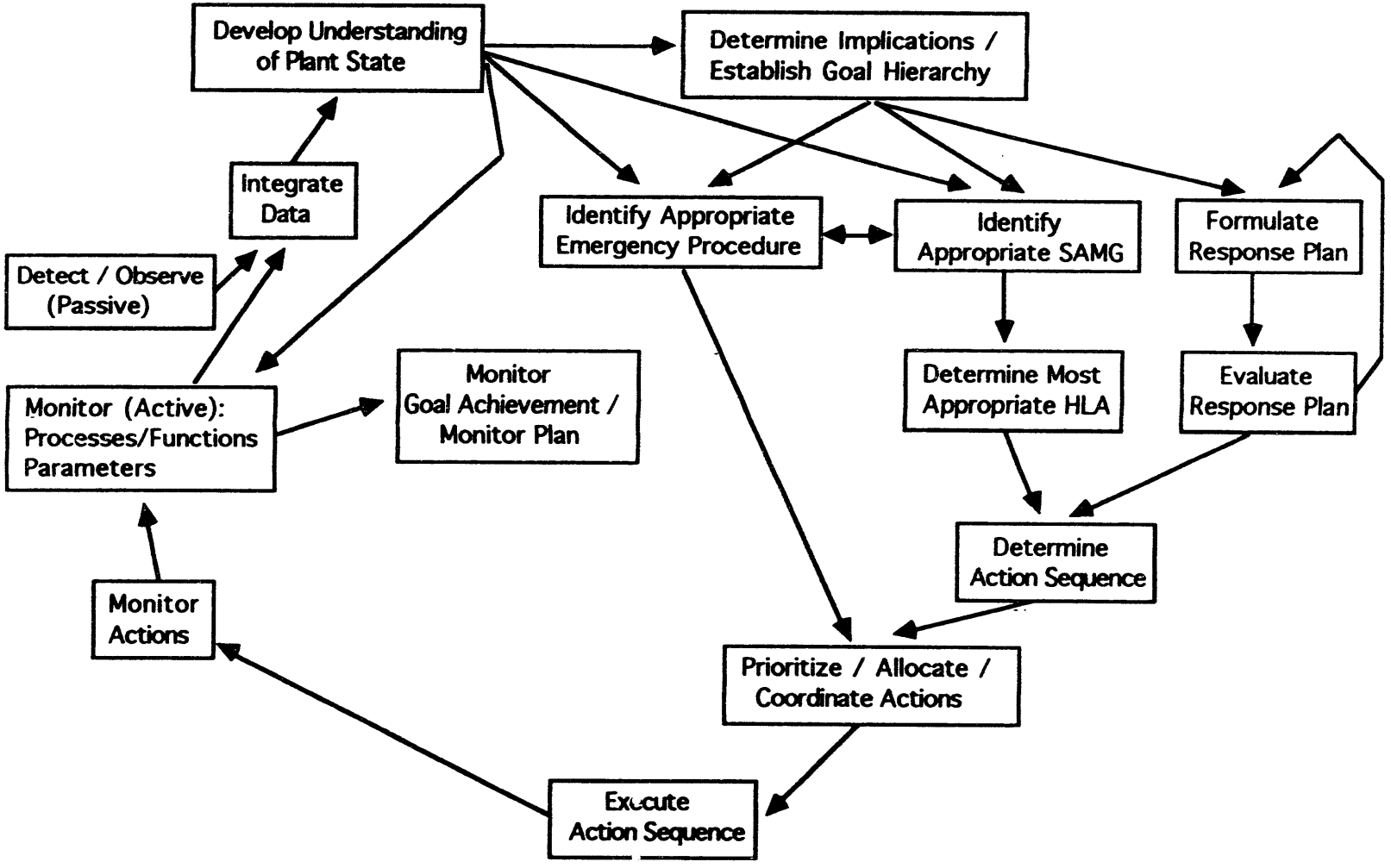


Figure 3. Expanded version of the decision-making model.

prescriptive than the EOPs. Because safety system status and equipment availability cannot be predicted in SAM, the guidelines are less able to specify ideal recovery strategies.

The decision-making model allowed for examination of potentially problematic performance issues in SAM. Further, potential complexities in decision-making were identified by analyzing 12 specific SAM scenarios. In this section, the major types of complexity or errors that are likely to occur in each process of the decision-making model are described, and the types of cognitive skills that may be needed in each process are listed.

Detect/Monitor

The primary concern here is with acquiring accurate and complete indications of the plant state. Plant state conditions can become seriously degraded as a transient evolves into a severe accident, especially when there are significant changes to the core. This evolution can have a significant effect on plant state data. First, data can be lost; instruments, sensors, and indicators can fail (e.g., indicator goes off-scale). Furthermore, indications that may be very useful for SAM are not instrumented (e.g., little information is available on core status).

Second, data can become misleading or unreliable. As conditions move out of instrument boundary areas, there is the threat of false readings or false alarms (e.g., as temperature increases through a certain region, instrument failure becomes more likely). The existence of misleading data or uncertain data (in excess of what is common in control rooms) may reduce confidence in plant state indications. Further, it is possible that if instruments are forced into unusual value ranges, they may not provide sufficient sensitivity or context to support diagnosis. There are examples in which instruments (due to insufficient discriminability) did not support diagnosis as effectively in unusual value ranges (Hoecker, Pople, & Benhardt, 1991).

After TSC personnel have been brought into the event, other issues can arise. First, their access to data may be limited. Instead of having all indicators available, as in the control room, TSC access to plant state indications may be restricted to a small number of parameters at a time. This limited access introduces the issue of data integration, both in time and space. TSC staff may have difficulty integrating individual indications in order to develop a complete picture of the plant. Second, the display devices in the TSC may not provide as much information on data reliability or data context. Changes in display format can also remove information that is easily determined in the control room (e.g., parameter rate of change is lost in digital displays). Finally, the TSC staff, when compared to control room decision-makers, may rely more heavily on data reported through voice communications from the control room or other areas of the plant. This source of data is also susceptible to misinterpretation, false alarms, and lost context. Phoned-in data are also more transitory; if they are not recorded by someone in the TSC immediately, they may be lost or forgotten.

Cognitive skills useful here are:
1. Determining accurate indications of plant state.
2. Integrating plant state indications.
3. Identifying meaningful events.

Interpret Current State

In this process operators may have to develop a fairly complete mental representation of the plant state. It is not always required, but having this representation can make operators more efficient. SAM guidelines may guide this activity.

Diagnosis can be extremely difficult for a number of reasons, including the following:

- Usual evidence or critical evidence can be obscured. For example, in certain plant designs, a loss of off-site power prior to a steam generator tube rupture can eliminate the initial indications (i.e., radiation sensors) of the tube rupture.
- Important indications can be incorrectly "rationalized away." For example, indications that should be diagnostic may be attributed to a consequence of a known but less significant failure or of an automatic action (e.g., shrink and swell).
- Some faults can produce effects at a distance. For example, in some interfacing system loss of coolant accidents, indications can appear in multiple systems that are not commonly associated.

Many of the commonly occurring diagnostic errors and biases can occur here because the system is complex and tightly coupled. For example, garden path interpretations (in which one is mislead by early indications that suggest a familiar problem) and confirmation bias (in which hypotheses about faults are not thoroughly tested before they are accepted) are common. Also, related plant state indications may be widely scattered around the control room.

Cognitive skills useful here are:
1. Making inferences about current plant state.
2. Determining expected influences and relevant data.
3. Recognizing links to existing accident management guidelines.

Determine Implications / Establish Goals

In the EOPs, operators are given an ordering of goal priorities (e.g., core cooling is addressed before containment integrity). The procedures reflect this ordering and operators are not expected to evaluate and shuffle goal priorities. However, evaluating goal priorities may take on more significance in SAM because it may be difficult in SAM to achieve one goal without adversely affecting another goal.

For example, in one scenario, operators are faced with a need to cool containment. A means for cooling containment is to operate the fan coolers and condense steam. However, a second concern is a hydrogen explosion in containment. If hydrogen concentration becomes too high, an explosion can occur, which can breach containment and release radioactivity. One means for reducing the threat of hydrogen explosion is to have a high steam concentration. Thus, the means for cooling (condensing steam) can adversely affect the mechanism that is reducing the likelihood of an explosion (high steam concentration).

In another scenario, operators are asked to find a source of water for cooling the core. Typically, boron is added to core cooling water as a means to control reactivity. In this scenario, the only source of water available is an unborated source. Thus, the means to address the goal of core cooling can adversely affect reactivity. The operators must determine whether the introduction of the unborated water will lead back to a critical core.

Thus, operators and TSC staff may be required to weigh alternative goals and the means to achieve those goals to assess how the pursuit of one goal may affect the status of other goals. Competing goals introduce a complex set of constraints to the decision-making task.

Cognitive skills useful here are:
1. Using mental representation to simulate event's progression and identify goals.
2. Determining goal priorities.
3. Recognizing links to existing accident management guidelines.

Plan

An issue in this process may be that the high-level actions (HLAs, which are general strategies) are not well understood: How will system X react to this type of control action? Because the plant is so complicated, and plant systems are so tightly coupled, it may be difficult for operators to simulate and anticipate mentally the progression of certain actions or phenomena.

In one of the scenarios, reactor core damage occurs and reactor vessel failure is imminent. Under these conditions, operators are asked to consider the value of flooding the reactor cavity. However, there may be a gap in their understanding of how this action would affect the plant. When is the best time to begin flooding? How much water should be used? How long will it take to flood? Again, the SAM guidance documents now being developed may address this issue.

In another scenario, the reactor loses its means for removing heat. If heat removal systems cannot be restored, core damage, melting and reactor vessel failure can result. In this case, operators are asked to consider the value of depressurizing the reactor coolant system before the vessel fails. Again, operators may not understand this phenomenon well enough to simulate it mentally and determine the implications.

Cognitive skills useful here are:
1. Identifying appropriate existing response plans.
2. Formulating response plan.
3. Evaluating response plan.
4. Determining action sequence.

Control

One issue in this process are the effects of uncertainty and stress on decision-making. In general, decision-makers will be asked to select and carry out control actions that have potentially severe consequences in an environment where information may be difficult to obtain and phenomena may not be well understood. There may be less information about plant status ("Maybe if I wait longer I will know the state of X"). There may be less opportunity to implement the preferred course of action ("Maybe if I wait longer I will be able to recover and use system X, which introduces fewer negative side effects"). There is reluctance in any situation to take actions that have known severe consequences ("Maybe if I wait longer I won't have to flood X"). In addition to these sources of uncertainty, a severe accident will bring involvement of personnel from the utility, the community, and state and national agencies. Each representative may bring different influences to the decision-making process.

Any emergency situation introduces stress to operators and technical staff, and high stress levels can impair decision-making performance. There are a number of reasons why SAM will involve

stress levels exceeding those expected from design-basis accidents. First, one primary source of stress is novelty or uncertainty. Research shows that stress levels are high when decision-makers have few or no expectations about the likely progression of an event. Second, high workload and perceived time pressure increase stress levels in performers. Third, the significance of the event and the heightened attention to every aspect of performance can create high levels of performance anxiety. Finally, the physical environment of the plant could become adverse (e.g., high temperatures, reduced lighting). These factors, also, can increase stress levels for performers.

Cognitive skills useful here are:
1. Managing the execution of a response plan.
2. Executing control actions.

Feedback

Similar to the early process of monitoring plant state data to develop an understanding of plant state, feedback can be impaired by difficulties with plant state indications. As a severe accident progresses, indicators may fail or become unreliable. In some cases, the optimal feedback information is not well instrumented or enters an uncommon range where discriminability is poor. All of these problems can reduce the crew's ability to determine whether the control actions are having the intended effects on plant state. Also, there are likely to be data that are less valid or are transitory indications of plant state. For example, in some plant designs there are transitory shrink and swell effects that can mask more enduring changes in plant state.

Cognitive skills useful here are:
1. Using plant state data to determine that control actions are having desired effect.
2. Evaluating appropriateness of response plan.

Crew Skills

The preceding focused primarily on skills of individuals in the SAM setting. However, crews, or teams of decision-makers, must also perform in a skilled manner. For example, in the event that the control room and the TSC share decision-making authority, communication and coordination will be critical. One potential scenario for crew performance is that the control room acquires the initial indications, the TSC then develops a diagnosis and selects a plan, and finally, the control room carries out that plan. It is essential in this type of situation that not only are the outlines of each decision passed from one group to the next, but that the intent is also communicated in some way. In situations that do not separate decision-making functions in this way, communication and coordination are still important. Crew skills have been identified in each decision-making process to support communication and coordination.

Cognitive Skill Training

One approach to reduce the potential for human error is to develop training approaches that provide these cognitive skills to relevant control room and TSC personnel. In general, operators and technical staff may require training on the following elements of cognitive skill:

- Extensive knowledge (e.g., validity of plant state indications, likely SAM phenomena).
- An accurate representation of the plant, including the interconnections between systems.
- An accurate representation of likely physical phenomena and their progressions.

- An understanding of SAM goals, subgoals, and the strategies or HLAs that can be used to achieve goals.
- Metacognitive skills, which are higher-level processes that initiate and guide cognitive activities, to manage not only the diagnosis and selection of appropriate actions, but also to manage the response of distributed personnel.

A literature review on training cognitive skills was conducted. This report describes 19 general approaches to training cognitive skills or facilitating the training of cognitive skills, applying both to individuals and teams of individuals. These 19 approaches were grouped under the following seven headings to create links back to the elements of cognitive skill:

1. Training to teach knowledge
2. Training to teach knowledge representation
3. Training to teach rules applied to decision-making
4. Training to teach strategies, goals, and subgoals
5. Training for management of mental resources
6. Training a decision-making process
7. Training team skills

The following paragraphs provide brief summaries of the training approaches identified in each of these groups.

1. Training to Teach Knowledge

Knowledge is a critical component of cognitive skills. The complex cognitive skills required for nuclear power plant decision-making are built on knowledge of thermodynamic theory, plant systems and operation, specific phenomena, plant system interconnections, the logic underlying procedures, plant-specific facts and relationships, etc. Somehow, this extensive knowledge must be available--in someone's head, in a procedure, in a schematic, on a CRT, etc.--to support decision-making. Teaching knowledge is typically perceived as straightforward and uncomplicated. However, while trainees can often learn knowledge quickly, two types of knowledge failures can occur: knowledge is not tied to its use in task performance (i.e., it is inert), and knowledge is forgotten when it is needed. The following techniques can be used to prevent these knowledge failures.

Present knowledge in a job or functional context. There is ample evidence that a functional context aids a learner in making new knowledge fit more meaningfully into existing knowledge structures. That is, the job context or functional context provides a structure on which to hang new knowledge, which also aids retention. The functional context aids the trainee by furnishing cues to help retrieval and by facilitating, through the use of a conceptual framework, the regeneration of information that may have been forgotten.

Overlearning to enhance knowledge retention. Another technique to enhance long-term retention of knowledge is called "overlearning." Overlearning refers to practice that extends beyond the achievement of some level of mastery. For example, a training objective might (somewhat arbitrarily) define mastery of a task as the ability to complete a procedure without performance aids (e.g., a procedure) in less than 2 minutes within some level of tolerance. Practice on this task during initial training may be terminated as soon as this criterion has been achieved. Overlearning would specify additional practice beyond this level. Numerous empirical studies have demonstrated that retention is better for overlearned tasks, and in general, more overlearning leads to more enhanced retention.

Distributed practice to enhance knowledge retention. While the number of practice trials or training time is strongly related to the level of learning, retention also depends on the distribution of practice trials across time. For a fixed amount of practice, long-term retention can be enhanced by spacing practice instead of massing all practice into a single session. For example, four hours of practice can be given in a single day (massed practice) or split into four sessions, each of which is one hour and separated by several days from other practice sessions (distributed or spaced practice).

Contextual variety to enhance knowledge retention. Another approach to enhancing long-term retention of knowledge and simple skills is to vary the training setting. This approach, which introduces variety to the training context, is sometimes called contextual variety or contextual interference. The goal of this set of techniques is to force trainees to develop a more elaborated or richer mental representation that can be accessed more easily and used more flexibly. Generally, the training objective is to have trainees encode knowledge in multiple contexts so that its retrieval does not rely on replicating the exact conditions present at the time of learning.

Cooperative learning and peer teaching to enhance learning. Another means for getting trainees actively involved with the material is to hand the role of instructor to trainees. Cooperative learning and peer teaching are techniques that force learners to take on multiple roles in approaching the material, and they couch learning in a more comfortable social setting. In cooperative learning, the material to be learned is divided, and each member of the group becomes responsible for instruction.

"Accelerated Learning" programs. There are currently several commercially available programs that make strong claims about enhancing learning. Examples of these "accelerated learning" programs are Suggestive Accelerative Learning and Teaching Techniques (SALTT), Suggestopedia, and Superlearning. Some of these programs make extraordinary claims about their effects on learning--e.g., "increase learning 5 to 50 times...requires no effort on the part of students...awakens creative abilities." The review of cognitive skill training approaches also analyzes the support for the claims behind these commercially available products.

2. Training to Teach Knowledge Representation

An important aspect of knowledge is its organization in long-term memory. Simply having access to knowledge is insufficient for skilled performance; the information must be organized within the job context. Skilled practitioners develop methods for extracting information from the world based on the meaningful patterns that occur and based on their understanding of the functional relationships between events and objects. Thus, training in this area should focus both on teaching trainees to identify important patterns and on teaching mental models that support decision-making. The following are approaches for this aspect of cognitive skill training:

Training critical perceptual patterns. Skilled performance often relies on extracting the relevant information from the world and ignoring or bypassing information that does not currently have relevance. The ability to identify meaningful organizations of information supports two aspects of performance. First, the initial task representation that is developed is strongly influenced by an understanding of meaningful patterns. Experts see the world through a filter that breaks up, or parses, the world into meaningful objects and events. Thus, trainees need to learn the functional groups that help them represent the task. Second, certain patterns of information (e.g., visual patterns, auditory patterns, combinations) indicate that a specific response is required. Simple cues to respond are auditory alarms. However, experts can become sensitive to more complex

cues that guide behavior. Skilled practitioners acquire these patterns, and it is important to make them available to trainees.

Train mental models. Mental models provide a deeper description of the knowledge required by performers. Mental models are complex representations that allow one to simulate mentally a system or process in order to reason about cause and effect, consequences of actions, feasibility of control actions, effects of malfunctions or failed components, etc. A primary reason to train mental models is to guide trainees in developing useful and effective representations of the system. Unaided, trainees will develop a system representation, but that representation may contain misconceptions about the system, inaccuracies, or gaps. Several computer-based approaches have been developed to guide the development of mental models for reasoning and problem solving.

3. Training to Teach Rules Applied to Decision-making

An early phase in the development of cognitive skills is the construction of domain-specific rules. Many researchers have focused on the development of condition-action pairs, called production rules, that proceduralize knowledge for the performance of specific tasks. There have been a number of analyses of simple cognitive tasks that have successfully derived a set of rules for task performance. These rules can form the basis of an expert system that can solve problems or make decisions. The analysis of rules has led to two approaches to training. One approach emphasizes identifying and eliminating incorrect rules, called buggy rules, that are formed in the course of learning. The second approach uses the rules underlying the model of skilled performance to guide trainee performance as a task is learned.

Identify and eliminate buggy rules. By carefully studying performance of tasks that are highly procedural, one can document systematic errors in trainees' procedures. It has been determined that errors are often not simply random occurrences, but reflect the presence of incorrect rules that had been acquired in the process of learning. These rules are called buggy rules (as a reference to the "bugs" found in computer code). Programs have been developed in the area of mathematics and computer programming to identify, diagnose, and correct these buggy rules.

Train production rules. The rule-training approach has been extended to create a number of intelligent tutoring systems (ITSs) that address LISP programming and several areas of math education. The primary role of each tutor is to diagnose errors and intervene when the trainee commits an error or is stuck. For example, when the trainee types an inappropriate bit of code, the tutor intervenes immediately to provide an explanation of why it is incorrect. The trainee is then given the opportunity to try again. If the trainee continues to input incorrect code, he will be supplied with the appropriate response. If the trainee proceeds through the exercise without error, the tutor's role is minimal.

4. Training to Teach Strategies, Goals, and Subgoals

An important subset of cognitive skills are those associated with simple task performance. Beyond applying general cognitive processes to knowledge to develop task-specific rules (or cognitive procedures) is the need to apply those rules to solving problems or making decisions. Specifically, a task can be analyzed into an organized collection of goals and subgoals that must be effected in order to achieve the task. After the set of goals is established, the performer must then identify the specific rules that can be applied to accomplish each goal. A strategy was defined as the sequence of rules used to achieve a subgoal or goal. More generally, these elements are central to the broader activity of planning. A number of training techniques have

been developed and refined over the last 15 years that focus on these elements of cognitive skill. These techniques can be grouped into three categories: cognitive apprenticeship, coached practice environments, and planning-support environments.

Cognitive apprenticeship. At the highest level of description, cognitive apprenticeship presents a model of skilled performance, supports practice of the task, and encourages comparisons of the trainee's performance to the model. Cognitive apprenticeship techniques often employ groups of trainees with the intent of developing the roles of both producer and critic.

Coached practice environments. A second approach, which has been employed in several intelligent tutoring system (ITS) projects, is referred to as a learning environment or a coached practice environment. The intent of this approach is to immerse trainees in the problem-solving activity and to coach them opportunistically. The model of skilled performance is not presented in its entirety up-front as it is in the cognitive apprenticeship approach, but is revealed via coaching that occurs throughout instruction.

Planning-support environments. Like other learning environments, planning-support environments provide a task environment and a coaching capability. What is different about this approach is the greater structure imposed on the planning element of a task. What sets them apart is their focus on supporting explicitly the planning activities via a graphical support environment in which tasks (such as programming) are initially conducted at a higher level. The details of performance are neglected until the construction of effective plans is complete. Moreover, hints and advice are initially directed at the level of strategies and subgoals.

5. Training for Management of Mental Resources

Because of limitations in human memory and attention, a training program must aid trainees by ensuring that sufficient mental resources are available--initially to increase training effectiveness, later to enhance job performance. There are two general approaches to manage mental resources during training: providing support in task performance (e.g., scaffolding techniques) and reducing task performance requirements. The following two techniques have been used to enhance the efficiency of attentional resources in performing complex tasks:

Reduce the need for mental resources with automaticity training. There have been a number of demonstrations of the ability to train skills to the point where their execution requires virtually no mental resources--they become "automatic." Those skilled in reading, driving, or typing are prime examples of the benefits of automating low-level skills. When these low-level skills are automated, more important activities--e.g., sentence and paragraph comprehension in reading, route finding in driving, or text editing in typing--can be performed simultaneously and still receive the level of attention they require. The development of automated skills, called automaticity training, has been refined over the last 10 years.

Eliminate inefficient strategies. Early in training, the development of automated individual skills can aid in reducing mental resources and preventing trainees from becoming overwhelmed. However, at some point task components must be integrated, and studies have shown that automated skills may not be integrated into a dual- or multiple-task setting without a decrement in performance. Thus, there needs to be a transition to dual-task practice after the early phases of automaticity training are complete. Only by practicing a skill when there are additional requirements for mental resource (i.e., a second task) can the trainee learn the most efficient strategies for sharing attention and memory. Several techniques are available for promoting the most efficient use of mental resources in complex tasks.

6. Training a Decision-Making Process

One approach for training decision-making skills is to train personnel to apply a formal decision-making process. Ideally, this training could improve decision-making efficiency and skill and reduce the effects of bias in human decision-making. However, a recent review of training studies that have taken this approach shows a general failure of this approach for realistic, complex decision-making tasks.

Train a formal procedure for decision-making. A set of training studies exist that trained decision-theory-based procedures, such as multi-attribute utility (MAU) models. However, MAU and related techniques that focus on formalizing the selection of the best alternative are not useful for many of the important decision-making tasks people face. Thus, there is a need to develop a better understanding of real-world decision-making tasks and train the process underlying those tasks.

Reduce decision-making biases. Training approaches also exist for reducing or eliminating decision biases. Instead of training a set of procedures or a method, these programs attempt to eliminate the biases that occur naturally in human decision-making. Even in cases where training reduced biases, no generalization or transfer of training to other decision-making situations was achieved. Thus, it seems that any training to reduce or eliminate decision-making biases will have to focus on the biases specific to a decision-making task. Training that attempts to provide a general sensitivity to decision-making bias is not likely to be effective.

7. Training Team Skills

In the analysis and training of cognitive skills, there is a substantial literature on skills defined at the individual level but relatively little on skills defined at the team or crew level. One concern is the lack of description of expertise defined at the team level. However, one systematic approach has been developed in the commercial and military aviation context: aircrew coordination training (ACT) or cockpit resource management (CRM).

Employ a behavior-based ACT approach. The general ACT approach can have multiple phases: awareness, practice and feedback, and reinforcement. In the awareness phase, seminars and group exercises are used to present the basic concepts of team performance. In many cases, these activities have been borrowed from management courses, and the topics covered include communication, decision-making, workload management, management styles, and leader and subordinate responsibilities. This phase rarely provides skill practice in an operational environment. The practice and feedback phase is best exemplified by the line-oriented flight training program (LOFT). A behavior-based program seeks to identify particular behaviors within team skill dimensions that result in effective team performance. LOFT uses realistic scenarios to involve the crew in a complex or difficult situation in which team skills are important. Crew performance is videotaped and reviewed in a debriefing session that includes the instructor and the crew. The reinforcement phase, or recurrent training phase, is a means to provide LOFT-type exercises on a recurring basis.

Develop "shared mental models". In order to function effectively, teams may share mental models of the task environment, of the equipment or interface, and of the team and its interactions. These various types of mental models allow crew members to share an understanding of the current state of the task, of the needs or expectations of other crew members, of the control actions that are needed, etc. This shared understanding supports

coordination and communication. One of the few training approaches that have been offered to support the development of shared mental models is cross-training--that is, allowing crew members to serve in a different role in order to understand the needs and demands of that role.

Summary of Training Approaches

In terms of drawing conclusions about general characteristics that are critical to effective training of cognitive skills, at least five important characteristics have emerged from the review of approaches. However, note that not every one of the 19 approaches reviewed reflects all five characteristics, which are the following:

1. Develop a model of skilled or expert performance to be used as a model and as a diagnostic aid.
2. Require the trainee to become involved in evaluating his/her performance (or the performance of others) using as a standard the model of skilled performance.
3. Have the trainee actively engaged in the task as a setting for instruction.
4. Allow the trainee to be involved (eventually) in performance of the complete task.
5. Aid the trainee in managing mental workload throughout training.

First, it is clear that developing a model of skilled performance through some form of cognitive task analysis is a critical input to cognitive skill training. It is important to emphasize that this analysis addresses both the knowledge required and the processes that support the application of that knowledge. Simply teaching knowledge is insufficient. The cognitive skills that are required for skilled performance serve two roles in instruction: as a model and as a diagnostic aid. In some cases, a model of skilled performance is presented up-front for trainees or used to structure the instructional environment. In other cases, the model is used to generate explanations or to provide hints as learning progresses. In all cases, the tutor or instructor understands how the task should be performed and why. Moreover, this model serves as a means for assessing and remediating trainee performance. Much of the work in intelligent tutoring systems has focused on techniques for describing the trainee in terms of the expert model. The instructor or tutorial system requires this diagnosis to determine the instructional focus and feedback provided to trainees as learning progresses.

A second important characteristic of training, and another use of the model of skilled performance, is having a standard for the trainee's self-monitoring and self-diagnosis. There is a clear value in training trainees to be both performers and critics. While this may begin with the practice of critiquing others, eventually trainees learn to apply the same analysis to their own performance.

The third characteristic of nearly all of the effective training techniques is to involve the trainee in the actual task or a simulation of the task. A simulation is preferred because of the capabilities it offers for controlling the learning environment. In the training techniques reviewed, trainees were engaged in a number of activities, including actual problem solving or decision-making, system design, exploration, prediction making, watching example problems solved by an expert, and evaluating or critiquing the performance of others. In several cases, trainees were thrust into a simulated task environment where they could do no damage and were required to complete tasks that were well beyond their current capabilities.

A fourth characteristic of many of the training techniques described above was an emphasis on allowing the trainee to be involved in the performance of the complete task. Trainees are supported initially through scaffolding or other techniques that allow them to work on single

elements, but also allow them to integrate these elements into a complete whole. An important aspect of this technique is that trainees are given the opportunity to observe the metacognitive skills required for task performance. The instructor or tutor who is supporting the trainee provides a control structure for accessing and executing task elements. As trainees master the lower-level elements, they can take on larger roles and eventually perform the entire task. The importance of involvement with the complete task does not reduce the value of part-task training. Part-task training can have a role in managing mental resources. However, eventually this form of training must be integrated back into the context of the whole task.

Finally, many of the effective techniques reviewed incorporate mechanisms for reducing the mental resource requirements of the training setting. Because cognitive skills need to be learned at various levels--execution of rules, goal achievement, and metacognitive control--it is difficult for trainees to keep track of all aspects of task performance simultaneously. Instructional effectiveness is facilitated when some of these elements can be removed in the short-term or the problem representation provides some of the structure of the expert solution. Previous sections have identified more specific methods for controlling this aspect of cognitive skill training.

Training to Reduce the Effects of Stress

There are documented effects of stress on cognitive task performance, and training may be useful to address these effects. The project report considered three approaches in the identification of potential sources of stress. The first approach considered environmental factors that contribute to stress. The primary sources identified were high heat, poor lighting, encumbrance of protective clothing, noise, and fatigue caused by prolonged work, sudden changes in work shift, or loss of sleep. The second approach addressed the role of novelty and uncertainty in producing stress; primary sources here were the occurrence of a novel event, a violation of expectations, loss of critical information, and a failed implementation of a plan or control action. Finally, the report considered task-related factors that contribute to stress. Additional sources identified from this approach were high workload, time pressure, and performance anxiety.

The stress literature identifies the effects of stress primarily from a physiological response: either generally described as increased arousal or more specifically identified in terms of changes in the endocrine system. A state of heightened arousal is believed to have consequences tied to physical health, emotions, and performance. The project report specifically addressed only impairments of performance of cognitive skills. A review of the literature indicated the stress can lead to the following types of impairments:

- A narrowing and shift in attentional focus.
- A reduced working memory capacity.
- Speed-accuracy trade-offs in some decision-making tasks.
- Communication patterns of crew members and crew leader.

Many of the cognitive skills identified above are likely to be affected by these impairments. However, there are several training techniques for eliminating or mitigating the effects of stress on the performance of cognitive skills. The primary techniques that have the potential to be effective are the following:

1. Expose the crew to realistic emergency and severe accident events through simulation - Realistic simulation can aid personnel in developing expectations about the event, skills for controlling the event, and skills for obtaining feedback concerning the success of control

actions. This approach primarily removes novelty and uncertainty, which are likely to be major contributors to stress.

2. Reduce the need for mental resources and make processing more efficient - A number of training techniques exist that can make personnel more efficient processors and reduce the demands on attention and working memory.
3. Enhance crew communication and coordination skills - Crew training techniques have been successfully used for enhancing crew skills, especially skills for communication. These skills directly target the types of communication failures that are likely to occur under stress.

In general, the approach to training offered here attempts to develop more highly skilled personnel. When the necessary cognitive skills become mastered at a high level of performance, personnel are less susceptible to the likely effects of stress. There are a number of positive outcomes:

- Novelty and uncertainty are removed or greatly reduced.
- Operators and technical staff better understand what effect their control actions will have.
- Operators and technical staff can better cope with (and maybe stay ahead of) task demands.
- The crew shares and uses critical information better.

Summary and Conclusions

Throughout the broadly defined SAM decision-making process, complexity and the potential for human error present themselves in diverse ways. Although the development of SAM guidance may reduce the influence of certain factors, there will remain a major role for cognitive skills. Investigations of performance with EOPs indicates that even when detailed procedures exist operators still rely on cognitive skills to enhance efficient and safe operation. One approach for enhancing human performance is to provide training to address the important cognitive skills. The project described in this paper addressed training approaches in the following ways:

- Reviewed 19 general training approaches for addressing cognitive skills and indicated how these approaches are tied to the cognitive skills identified.
- Analyzed the likely effects of stress on cognitive task performance to identify other training needs.
- Proposed training approaches to address the effects of stress.

References

Hoecker, D.G., Pople, H.E., & Benhardt, H.C. (1991). *Initiating cognitive environment simulation at Savannah River.* (STC Technical Report 91-SJ4-SACES-R1). Pittsburgh, PA: Westinghouse Science and Technology Center.

Kauffman, J.V., Lanik, G.F., Spence, R.A., & Trager, E.A. (1992). *Operating experience feedback report - Human performance in operating events.* (NUREG-1275, Vol. 8). Washington, DC: U.S. Nuclear Regulatory Commission.

Rasmussen, J. (1986). *Information processing and human-machine interaction: An approach to cognitive engineering.* New York: North-Holland.

Roth, E.M., Woods, D.D., & Pople, H.E. (1992) Cognitive simulation as a tool for cognitive task analysis. *Ergonomics, 35,* 1163-1198.

U.S. Nuclear Regulatory Commission (in press). Cognitive skill training for nuclear power plant operational decision-making. (NUREG/CR-6126). Washington, DC: USNRC.

Organization and Management Activities in the Nuclear Power Industry

Robert C. Evans

Robert N. Whitesel

Nuclear Management and Resources Council

The purpose of organization and management development activities in the commercial nuclear power industry is to foster high levels of power plant performance and safety through improved human performance. The NRC has been working to develop assessment tools to assay the effects of organizational factors on plant safety. The utility industry has been working on initiatives targeting individual accountability, the improvement of plant performance and the elimination of the items identified through the NRC assessment process.

Organization and management activities do not focus on industry organizational charts, but on the personnel processes and dimensions (factors) that affect safety and economic performance. As individual terms these activities are often combined and referred to as organizational factors. As an area of study, organizational factors has become more prominent as the industry emphasis has switched in recent years from hardware issues related to safety and economics, to personnel-related issues.

Beyond the obvious safety objectives affected by improved human performance, plant performance improvements, in areas such as capacity factors, can be achieved through improved human performance. For example, it is estimated that as many as half of the unplanned reactor scrams are caused by personnel errors. The integrated effect of

these scram-initiating errors is conservatively estimated to be 100 lost capacity days per year. The financial impact of these events is estimated to be $100M per year.

There is general agreement within the NRC research community on 20 organizational factors that, taken individually or in combination, affect nuclear power plant safety performance. A sample of these factors include:

- Personnel selection
- Resource allocation (personnel and hardware)
- Technical knowledge (at all levels)
- Training
- Goal prioritization (company and facility wide)
- Communication (verbal and written)
  - External
  - Interdepartmental
  - Intradepartmental
- Coordination of work (central coordination)

While these factors are listed as 20 discrete terms, in some cases these terms may interact, or overlap.

For the NRC, plant safety is the target of organizational factors research. Researchers agree that safety culture is at the apex of the organizational factors pyramid. Safety culture is defined as the integration of the value systems of an organization (Nuclear Power Plant) and its demographic features, such as age, gender, income, learning history and ethnic-social distribution. With this definition, one can see that there

are variables which can be manipulated, particularly in the multifaceted area of value systems, to affect safety culture.

The NRC researchers continue to verify and validate the factors that affect plant safety. However, the nuclear utility industry has had the foresight and initiative to implement programs which systematically address those organizational factors shown to significantly impact the safe and economical operation of other process industries.

Activity to improve human performance is carried out by the Institute of Nuclear Power Operations (INPO) and individual companies. The INPO activities in the form of programs include the Human Performance Enhancement System (HPES), the development of good practices (which amounts to the sharing of techniques), operating experience sharing, and the Organizational and Administration (O&A) assessments that are carried out as part of INPO's periodic evaluations of individual site performance.

The INPO Human Performance Enhancement System is built on six premises:

- Human performance problems can be reduced and minimized.

- The management policies and practices related to human performance are essential to establishing an atmosphere that encourages problem identification and resolution as well as accountability for correct task performance.

- People want to perform well and accept responsibility for their performance.

- Accurate identification and correction of causes can prevent repeat events.

- The causes of non consequential events are the same as those of consequential events.

- Utility sharing of lessons learned promotes better plant and industrywide understanding, identification and correction of causes of human performance problems.

Individual utility activities which target organizational factors to enhance human performance, include the following:

- Bench Marking - Utilities bench mark their processes and performance against other utilities and industries with proven successful operations. Several utilities have entered into a formal contract to share beneficial practices and exchange information related to improving productivity.

- Process Mapping - Many utilities are heavily involved in process mapping efforts as a step toward re engineering selected processes to improve human performance.

- Monitoring human error rate - Some utilities refer to this activity as trending human performance problems. The process, under both names, characterizes deficiencies that occur as a result of personnel error, human action, human inaction, or man-machine interface as human performance/human error problems. The data are compiled and trend

reports are generated with corrective actions being requested of the cognizant groups, as appropriate.

- Root Cause Analysis - Many utilities extend their trend analyses from monitored human errors to the identification of root causes. Root cause analysis is fundamental to eliminating recurring human performance problems.

- Corporate Performance Indicators - In an effort to trend human performance at the corporate level, many utilities have developed a manifold of human performance factors which taken collectively measure overall organizational success. Several of the factors routinely tracked include:

  - unplanned absenteeism rate
  - attrition rate
  - accident statistics
  - number of grievances
  - number of disciplinary actions taken
  - number and nature of FFD cases
  - number and nature of NRC reportables involving human performance factors

- Organizational Development - Many utilities subscribe to organizational development activities with internal/external consultants and/or as participants in a national leadership development center. Organizational

development is a system-wide process of data collection, diagnosis, action planning, intervention and evaluation aimed at:

- re-aligning organizational components
- developing new solutions for old problems
- developing the organizations ability to renew itself

- Quality Management - Nuclear utilities have followed the lead of large successful corporations in pursuing quality management activities. The activities include Total Quality Management (TQM), teamwork and leadership, professionalism, empowerment, selection, assessment, training and development, performance evaluation and succession planning.

Analysis of the TMI-2 accident showed the nuclear industry the need to develop highly effective organizations. Industry programs in support of effective organizations began in earnest in the mid-1980's. The increase in programs which affect the quality of organizational performance in the nuclear industry over the past seven years indicates that this process is a rapidly developing, evolutionary activity.

The nuclear utility industry in the U.S., like the manufacturing industry internationally, recognizes that product or performance quality cannot be inspected in. Quality in personnel performance or product development is achieved most effectively, and in a more timely and productive manner, when it is built into day-to-day operations. The challenge for each nuclear organization has been to establish and cultivate principles that integrate quality objectives into daily work activities at the organization and individual levels. Line organization components are viewed as the key to quality performance. This accounts for the increase in industry programs geared toward

enhancing work group effectiveness. Strong industrywide support for these quality-enhancing programs is essential to ensure the nuclear utility industry maintains its viability in the nations' energy mix as it produces electricity safety and cost effectively.

Potential Human Factors Research Relating to Modern Technology in Nuclear Power Plants

James Ketchel,

Electric Power Research Institute
3412 Hillview Ave
P. O. Box 10412
Palo Alto, CA 94303

Robert Fink,
MPR Associates,
320 King Street
Alexandria, VA 22314

Lewis Hanes, Robert Williges, & Beverly Williges
Consultants

Abstract

This paper discusses proposed human factors research to address advanced human-machine interface technology in nuclear power plants. It relates to a current EPRI project to identify a prioritized list of specific research issues that could be assessed to improve control room and other user interface areas. The project seeks to bridge the gap between the functional requirements of advanced design initiatives and the human factors research needed to support them. It seeks to identify potential benefits to be expected, as well as potential problems that might be introduced by advanced technology. It provides an organized approach to identifying human factors research needs, information already available, and measures of performance and effectiveness that might be used to assess the value of potential improvements. Those parts of the proposed plan that are subsequently approved by EPRI management and by the utility advisory committee will provide a basis for recommending research priorities.

Overview

Obsolescence has struck at nuclear power plants, many of which were constructed forty years ago. Some of the instrumentation and control equipment has become difficult and costly to maintain for want of replacement parts, and control room designs are based on obsolete technology. The new technology of the ' 70s and ' 80s away from analog systems toward digital instrumentation, computing, and display offers a design challenge to effectively transfer to the new. Both existing plants and new plants can be made more reliable, economical, usable, and effective in terms of equipment and the human-machine interface (HMI). If we effectively pursue the opportunity that this provides, we should be able to give control room

and workstation operators, supervisors, maintainers, engineers, planners, and schedulers all of the information needed in the appropriate form to effectively manage their workloads and direct plant activities. There can be greater awareness of the state of plant processes; and all users can be better supported in decision-making and problem-solving tasks.

There is a clear opportunity to improve crew and system performance. The hardware/software technologies are available. The need is to understand how best to use them. This includes gaining a clear understanding of the specific benefits we hope to obtain and problems we expect to resolve by applying them. It also includes avoiding new problems that may be introduced, and determining the means by which we can assess system performance and effectiveness.

EPRI has provided a wealth of human factors guidelines on HMI topics ranging from control room and display system design to current work on annunciator system specifications, and alarm minimization and diagnostics. Requirements have been developed for designing new systems in the Advanced Light Water Reactor (ALWR) program and for updating existing systems in the Integrated Instrumentation and Control Upgrade Initiative, both of which rely heavily on modern technology. In the human factors area, the next step is to determine additional research needed to support the advanced system designs and to establish a rational, prioritized plan for so doing. This is the objective of the subject HMI research plan.

EPRI's contractor, MPR Associates, and its subcontractors are developing the first iteration of a prioritized HMI research plan that will indicate research and development needs, risks, benefits, and where feasible, performance criteria and potential performance measures. An important part of this work is to avoid unnecessary duplication by determining lessons learned from completed research and from implementations of advanced technology and design concepts.

The following are examples of general areas of high priority research needs that have been identified and are addressed in more detail later. Final prioritization of these and other topics must await internal EPRI review and review by the utility Task Force Human Factors Subcommittee . As general topics, most of these have a familiar ring. Virtually all have been mentioned in a variety of forums as genuine research issues.

- Improved support for knowledge-based behavior
- Information access and display navigation
- Organization and structure of information to support users and tasks
- Intelligent display - control coupling
- Integration of information displays with procedures
- Integration of automation with procedures
- Operator aiding

The differences between past recommendations for research and present opportunities are at least twofold. The first obviously centers on the above developments in technology which provides a clear opportunity, if not demand for change. Secondly, and more subtly, it involves depth, scope, and readiness considerations. This includes recognizing alternatives for improvements in performance and cost savings that are based on years of related research that has not reached full fruition, or is not yet fully used. For example, EPRI's continuing work on annunciator systems has offered many solutions to identified problems that have provided utilities with alternative design concepts. These have been used in a number of cases to enhance existing plant designs, as well as to provide alternatives to be considered for new designs.

The culmination of the annunciator line of research will be to integrate displayed procedures and operator aiding with alarm conditions for each mode of plant operation. Once the components and information needs are defined, an integrated display system can provide operators and others with situation awareness, and can provide automatic or semiautomatic techniques to aid in task and workload demands.

Each of the above general topics subsumes many difficult research questions and issues, some of which are basic, if not altogether new. For example - How can large data bases be organized to support the cognitive styles and information processing needs of users? How many displays are needed and of what types? How do we avoid overburdening operators in accessing large quantities of information? What is the best use of automation and means of keeping operators in the loop? What should be done with the control room environment to facilitate both CRT usage and operator alertness? And which alternatives are most cost effective?

EPRI intends to review the first iteration of the proposed plan internally and with the research community in order to better identify high priority issues needing immediate attention and to identify appropriate lessons learned.

Research Needs

In a paper recently presented at the NRC's Digital Technology Workshop, Lew Hanes, an EPRI consultant on the research reported herein, touched on many of the research areas of interest. He advises that since we have limited experience with the effects of digital technology on human performance, and since guidance documents are incomplete, it is important to transfer knowledge from related applications and to perform high priority applications research. This suggests that in addition to the detailed requirements documents that EPRI has been developing, supporting research is clearly needed in a number of areas. A good deal of this is either underway at EPRI or elsewhere, or is being planned. The following table lists twenty topical areas of interest, each of which subsumes a number of specific research issues.

Table 1. Overview: Examples of Advanced HMI Research Issues Being Considered

HMI Topical Area	Research Issues
1. Operating Philosophy	Improve cognitive or knowledge-based behavior and support: • assess crew structures and needs • support integration of information for decision making
2. Workstation Arrangement and Integration	Assess control and information access. Integrate controls, displays, procedures, alarms, and operator aids at the workstation.
3. Display System	Organize and structure information presentation to support various types of user tasks (e.g., ops, maint., eng, planning and scheduling). To access information assess: • navigation • keyhole effects • display thrashing • overviews Deal with different user needs and proficiencies.
4. Controls	Soft vs dedicated (hard) controls. Integrate with procedures. Intelligence: • built-in checks • predictors, warnings, etc. • intelligent and explanatory interlocks Couple displays with soft controls. Soft controls guidelines.

Table 1 Continued

5. Alarms	Alarm reduction, diagnostics, and prioritization. Integrated alarm information and advisory system. Display techniques, coding, etc. integrated with other process information, e.g., mimic display.
6. Procedures	Formatting and use of electronic procedures. Dealng with multiple procedures, conflicts, interrupts, and priorities. Integration of information display with procedures. Operator aids, e.g., context-sensitive display call-up and tracking. Integration with alarms.
7. Automation and Workload	Function allocation and rationale. Information needs. Automatic display selection/advising. Automatic and electronic procedures. Automation vs operator workload, alertness, awareness, and proficiency. System monitoring, checking and tracking.
8. Crew Awareness and Alertness	Elements of situation awareness and their measurement. Overview display(s) / mimics for group viewing. Alerting functions and automatic means for verifying alertness, awareness.
9. Operator Aids	Determine needs for: • decisions • diagnostics • data/ display/ control / navigation aids • procedure/response tracking • predictors Effects of reliance on operator aids. Verification and validation

Table 1 Continued

10. Data System	Define information needs of operators, maintainers, engineers, planners, schedulers, etc. Determine practical and efficient methods to acquire, process, transport, control, and display information. Assess cost saving opportunities.
11. Control Room Facilities and Environment	Lighting systems that enhance alertness and maintain display usability Control of noise levels of alarms and usability of voice output devices. Crew communications.
12. Technical Support Center (TSC) and Emergency Operations Facility (EOF)	Capabilities and data/information needed in TSC and EOF matched to available technology. Coordination and communication between main control room and TSC, EOF, and others.
13. Crew Coordination and Communications	Effective use of crew resources including information aids, communications, and interaction, within and outside the control room.
14. Operation with Degraded HMI	Information requirements for maintenance staff when system errors/failures occur. Information priority relative to other information demands. Guidelines for design of backup and use of alternate HMIs, including auxiliary stations.
15. Maintenance Technician Interface	Information needs for maintenance workstation and guidelines for design and implementation: • document and information management and techniques to reduce workload and errors • data protection and safeguards: authorization and security measures without cumbersome access to needed data

Table 1 Completed

16. Training	Review of experience with embedded training and lessons learned. Clean, clear separation of training from real operations.
17. Design, Implementation, Verification & Validation	Appropriate measures of operator/system performance. Generalization of results from samples to full regime of operational situations. Guidelines for V&V
18. Transition Between Old and New Technologies and Mix of the Two	Methods for combining and integrating technologies during transition, and phasing in the implementation of new features and equipment. Guidelines for transition.
19. Experience/Lessons	Industry-wide review of experience with HMI and human performance needs and experiences in existing applications. • cost-effectiveness • lessons learned • needs
20. Advanced Technologies	Research emerging technologies that can replace traditional menuing and windowing interfaces, with that more closely tied to how operators think, e.g., moving a handle on a graphic representation of valve to open it instead of a pull-down menu. • determine needs, costs, and utility

These examples of research issues imply a considerable investment of funds and effort by EPRI, the utilities, vendors, and others, but we are not starting from zero. For instance, much of EPRI's recent work on microprocessor-based annunciator specifications, alarm diagnostics and minimization ; its current research on compact workstation design; and its continuing work on procedures can be directly applied. Moreover, there are lessons to be learned from offshore research and applications, including that done at Halden's facilities in Norway.

In setting priorities, one of our tasks will be to determine the most pronounced needs and payoff opportunities. It is not sufficient to call for an improvement simply because it would be a little better to do it that way, if it means widely disproportionate costs in terms of system complexity and expense. Since our resources are limited, we should think about what needs to be done first to correct known problems, to enhance system safety, efficiency, and effectiveness, and to minimize waste. For instance, planning an information processing system that provides for multiple user inputs and outputs can be of substantial benefit if it avoids duplication of effort, adds needed standardization, and improves system speed, capacity, and reliability. An on-going EPRI project in bar coding follows this orientation. It focuses on baseline system capabilities and application modules that can be readily adopted rather than on limited customized improvements.

A closing thought is that although the costs of advanced HMI system research are high, the benefits can also be substantial. Preliminary findings from the above bar coding study reveal both increased accuracy and some instances of savings in labor and time in the 40% to 80% range. Savings from modern HMI systems need to be estimated and verified.

An Assessment of Human Factors Research Facilities and Capabilities for the U.S. NRC

Valerie Barnes, Compa Industries, Inc.
Stuart O. Parsons, Parsons and Associates, Inc.
K. Ronald Laughery, MicroAnalysis and Design, Inc.
Jerry Wachtel, U.S. Nuclear Regulatory Commission
J.J. Persensky, U.S. Nuclear Regulatory Commission

The Human Factors Branch of the Nuclear Regulatory Commission's (NRC) Office of Nuclear Regulatory Research is sponsoring a study to identify the need for and availability of additional facilities for supporting human factors regulatory research. The objectives of the study are to: (1) determine the availability and capabilities of existing research facilities to support the current and expected human factors regulatory research needs of the NRC; (2) determine the need, if any, for an enhancement of, or supplement to the present human factors research facilities by detailing those regulatory research needs, current and expected, that cannot be met with existing facilities, or that cannot be performed at these facilities; (3) specify the characteristics of facilities that would be required to support these needs; and (4) perform a cost-benefit study of possible alternatives. The methods and preliminary findings of this on-going effort are described here.

Background

The Human Factors Branch of the Nuclear Regulatory Commission's (NRC) Office of Nuclear Regulatory Research is sponsoring a study to identify the need for and availability of additional facilities for supporting human factors regulatory research. Human factors research has been performed to support the NRC's regulatory mission for more than ten years at various facilities, such as private research institutions, universities, Department of Energy national laboratories and international cooperatives. However, researchers have experienced limitations in their access to appropriate research facilities and to other resources required to resolve important regulatory research needs. These limitations include:

- Lack of available licensed nuclear power plant operators or other representative personnel to serve as test subjects for research involving control room design, operations, maintenance practices, etc.
- Limited access to realistic simulator environments
- Lack of sufficient laboratory time to support experiments that require longitudinal study (such as vigilance, shift work, slowly evolving events)
- Lack of industry cooperation because of regulatory exposure or impact (real or perceived).

The purpose of this study, then, is to identify and evaluate alternative methods for addressing these limitations. The objectives of the study are to: (1) determine the availability and capabilities of existing research facilities to support the current and expected human factors regulatory research needs of the NRC; (2) determine the need, if any, for an enhancement of, or supplement to the present human factors research facilities by detailing those regulatory research needs, current and expected, that cannot be met with existing facilities, or that cannot be performed at these facilities; (3) specify the characteristics of facilities that would be required to support these needs; and (4) perform a cost-benefit study of possible alternatives. The methods and preliminary findings of this on-going effort are described here.

Methods

Four primary sources of information are being used to address the objectives of the project: representatives of facilities with human factors research capabilities, NRC staff, researchers who have conducted human factors research for the NRC, and a panel of subject matter experts (SMEs).

In order to identify the availability and capabilities of existing research facilities, project staff developed a list of facilities at which human factors research is performed based on their own knowledge as well as input from NRC staff members and the SMEs. To-date, representatives of 45 facilities have been contacted and asked to provide the following types of information:

- the number, availability and areas of expertise of the human factors research staff
- the number, availability and areas of expertise of technical support staff (e.g., nuclear engineers, programmers)
- existing research facilities, such as full-scope or part-task nuclear simulation capabilities
- access to appropriate test subjects, such as licensed nuclear power plant operators.

Facility representatives also were asked to discuss their availability for NRC contracting. The types of facilities contacted included Department of Energy (DOE) national laboratories, Department of Defense human factors laboratories, NASA labs, other government facilities, universities, non-profit corporations and corporations in the private sector.

In order to identify present and anticipated human factors regulatory research needs that cannot be met with existing facilities, 21 NRC staff members have been interviewed to-date. These interviews address the basis for current regulatory research needs in the human factors area and the staff's perceptions of emerging issues, derived from their inspection support activities and reviews of operational data. In addition, memoranda detailing regulatory research needs formally transmitted to RES from other NRC offices were reviewed.

Researchers who have conducted human factors regulatory research for the NRC over the

past ten years also were contacted. These individuals were asked to characterize the research projects in which they have been involved and to discuss any effects on the projects that they might have experienced resulting from a lack of access to research facilities or limitations in the available facilities.

Finally, a panel of SMEs was formed and the first of three anticipated meetings was held to obtain their guidance regarding the conduct of this project. The SMEs selected vary in their expertise. Several of them have directed human factors research programs as managers in other government agencies, such as the National Aeronautics and Space Administration and the Department of Transportation. Others on the panel are recognized experts in the areas of conducting human factors research in a variety of domains or specifically in the nuclear power industry. In addition to the SMEs, the meetings also have included a number of invited participants representing various stakeholders in the nuclear power community, such as a representative of the Professional Reactor Operators Society, a representative of the the Nuclear Utilities Management and Resources Council, and representatives of the DOE national laboratories with human factors research capabilities.

The first SME meeting was held early in the project in Chattanooga, TN at the NRC's Technical Training Center (TTC). The project objectives and methods were presented, those present toured the TTC facilities, and three working groups met to discuss the following topics: (1) appropriate research methods and characteristics of facilities required to meet the NRC's regulatory research needs in the human factors area; (2) improvements to the processes of conducting NRC regulatory research that could enhance the NRC's access to facilities and capabilities; and (3) the need for project staff to contact additional facilities.

Preliminary Findings

Although the project is not yet complete, the results of the information-gathering activities to-date have suggested several preliminary conclusions. Perhaps the most important of these is that extensive facilities and capabilities exist to support NRC human factors regulatory research in every domain of current and potential concern to the NRC. For example, the staff sizes of the facilities contacted ranged from three professionals and technicians to 291, with 13 facilities staffed with more than 40 human factors professionals. All but one of the facility representatives contacted indicated that their organizations would be interested in supporting NRC research. Five of the facilities claimed to have full-scope nuclear power plant simulators and three claimed part-task nuclear power plant simulators. Of the five facilities with full-scope simulators, all claimed access to trained nuclear power plant operators for test subjects. Representatives of all of the DOE national laboratories contacted, six of the universities, and four of the private-sector organizations indicated that they have experience in performing human factors research in the nuclear power industry.

However, no single organization was found that combines all of the desirable characteristics for performing some types of NRC human factors regulatory research identified in the interviews with NRC staff. For example, regulatory research to address questions associated

with automated control rooms may require access to nuclear power plant simulator models and computer-based interfaces with licensed operators as subjects for test and evaluation of different system concepts and configurations. Obviously, the vendors who developed automated control rooms have, in some cases, extensive and sophisticated research facilities, experienced research staff and access to appropriate subjects. However, the availability of the facilities for use by the NRC may be limited by conflict of interest concerns.

The researchers who have performed human factors regulatory research or technical assistance for the NRC confirmed that a lack of access to facilities and appropriate subjects have impacted previous studies. For example, completion of several projects has been significantly delayed because of difficulties in obtaining access to facilities and one project was cancelled because no licensees contacted were willing to participate in the research. The researchers also pointed out, however, that the majority of the projects in which they have been involved have not required access to research facilities, but rather depended upon literature reviews, event data base analyses, the gathering of expert opinion, and other methods that are not facility-dependent.

Several recommendations were made to the project staff by the SMEs and working group participants at the first SME meeting. The primary recommendation from the SMEs was that individual regulatory research needs, as they are presently formulated at the NRC, not be the sole basis for determining the NRC's research agenda, and subsequently, the types of facilities to which researchers might require access. Rather, the SMEs recommended that the basis for evaluating facilities and capabilities be a strategic, long-term human factors research plan that recognizes the need to respond to short-term, "fire-fighting" research questions from the field. Working group recommendations included guidance to the project staff (1) to abandon efforts to identify required facility characteristics in terms of research methods; (2) to consider alternative contracting mechanisms, such as Centers of Excellence in various human factors research areas, that could bring together the facilities and capabilities required to support research in those areas; and (3) to contact a broader range of research facilities than originally planned.

Next Steps

Once the information-gathering activities have been completed for this project, the next step will be to identify feasible alternatives for enhancing access to existing research facilities and capabilities. The costs and benefits of those alternatives will then be evaluated and a final set of recommendations made.

Implications of an HRA Framework for Quantifying Human Acts of Commission and Dependency: Development of a Methodology for Conducting an Integrated HRA/PRA*

M.T. Barriere,[1] W.J. Luckas,[1] S.E. Cooper,[2] J.Wreathall,[3] D.C. Bley,[4] and W.S. Brown[1]

[1]Brookhaven National Laboratory
Upton, NY
[2]Science Applications International Corporation
Reston, VA
[3]John Wreathall & Co.
Dublin, OH
[4]PLG, Inc.
Newport Beach, CA

ABSTRACT

To support the development of a refined human reliability analysis (HRA) framework, to address identified HRA user needs and improve HRA modeling, unique aspects of human performance have been identified from an analysis of actual plant-specific events. Through the use of the refined framework, relationships between the following HRA, human factors and probabilistic risk assessment (PRA) elements were described: the PRA model, plant states, plant conditions, PRA basic events, unsafe human actions, error mechanisms, and performance shaping factors (PSFs). The event analyses performed in the context of the refined HRA framework, identified the need for new HRA methods that are capable of: evaluating a range of different error mechanisms (e.g., slips as well as mistakes); addressing errors of commission (EOCs) and dependencies between human actions; and incorporating the influence of plant conditions and multiple PSFs on human actions. This report discusses the results of the assessment of user needs, the refinement of the existing HRA framework, as well as, the current status on EOCs, and human dependencies.

1.0 INTRODUCTION

As part of an NRC sponsored program evolving from an assessment of human reliability issues in Low Power and Shutdown (LP&S) operations in nuclear power plants (NPPs), an improved approach to human reliability analysis (HRA) is currently being developed. This approach will be consistent with and reflect human behavior based on detailed analysis of actual events that have been encoded into the Human Action Classification Scheme (HACS). It is intended to be fully integrated with probabilistic risk assessment (PRA) methodology and to enable a better assessment of the human contribution to plant risk, both during LP&S and at-power operations.

Weaknesses in existing HRA methods and specific areas for concentrated development were identified based on the insights gained from the study of human reliability issues in actual events and from experience in applying existing HRA methods. A detailed program plan outline for producing an integrated HRA/PRA methodology that addresses these weaknesses has been developed. NUREG/CR-6093 provides details on the human reliability issues and the associated program plan outline.

*Work performed under the auspices of the U.S. Nuclear Regulatory Commission.

This report details progress to date beyond that presented at the 20th Water Reactor Safety Meeting (October 1992) with respect to each program plan task. Specifically, this report discusses an assessment of user needs, the refinement of an existing HRA framework, the characterization and representation of errors of commission (EOCs), and the development of an approach to deal with dependency between human actions. This report also identifies anticipated follow-on efforts including the development of a quantification process and implementation guidelines as well as, a demonstration of the guidelines and methodology.

2.0 ASSESSMENT OF USER NEEDS

Through the assessment of user needs, several findings that the integrated HRA/PRA methodology should address were identified. These findings included the need for:

- Developing a more realistic representation of the dynamic nature of the human-system interaction, especially during response to accidents;
- Facilitating realistic evaluation of multiple factors influencing human performance; and
- Providing consistent and repeatable results that minimize resource requirements.

3.0 APPROACH FOR DEVELOPING AN HRA FRAMEWORK

In support of developing a new HRA framework to address the user needs described above and improve HRA modeling, it was recognized that the unique aspects of human performance must be identified. Review and analyses of actual LP&S and at-power events provided the best vehicle for obtaining a general understanding of the dynamic nature of the human-system interaction.

The strategy of using actual plant-specific events as a basis for the development of the new HRA framework and improved HRA methods, was to provide a realism which has been missing in the treatment of human performance in PRA models. In addition, these analyses also provided the basis for identifying more specific requirements of HRA methods such as which classes of human actions (e.g., initiators, pre-accident errors, recoveries) and performance shaping factors (PSFs) are important. Significant differences between human performance during LP&S and that during at-power operations also were identified.

3.1 Data Analysis Strategy

The following steps were implemented for analyzing actual plant-specific events: (1) selection of data sources, (2) development of an analysis tool, (3) event analyses, and (4) review and verification of analysis results. The data sources used for the analysis of LP&S events were full-text LERs identified as significant in NUREG-1449, NRC Augmented Inspection Team (AIT) and Incident Investigation Team (IIT) reports, and AEOD Human Performance reports. NRC event-based reports (i.e., AITs and IITs) and AEOD reports were the source of data for at-power events. The analysis tool developed is called the Human Action Classification Scheme (HACS) which is described in detail in NUREG/CR-6093.

HACS is based, in part, upon a variety of previously defined schemes and was developed in conjunction with the review of full-text licensee event reports (LERs). The resultant scheme is capable of documenting the relevant, available plant-specific information, such as that provided in full-text LERs. For example, HACS documents the following: the number of human actions involved in a particular event and, for each human action, the action class (e.g., initiator, recovery), error mode (i.e., errors of

omission or commission), error mechanisms (e.g., slip, mistake), location (i.e., in-control room or ex-control room), activity being performed (e.g., maintenance, operation, testing), and the effect of the action (i.e, active or latent). For recovery actions, the location and time for performing recovery actions is also recorded.

Additional HACS fields which contribute to the concise but descriptive record of each event include: unit status, event time, noteworthy plant conditions (e.g., unusual plant configurations, important equipment out-of-service), system and component involved, automatic equipment response to event, the uniqueness to LP&S or at-power, an assessment of event significance, and the corrective actions taken. Table 1 provides a listing of all the HACS database fields.

Table 1. HACS Database Fields

Field 1-Event or Document Identification	Field 15-Human Action Descriptor
Field 2-Event Description Summary	Field 16-Error Mode
Field 3-Event Date and Time	Field 17-Error Type
Field 4-Plant Type/Vendor	Field 18-Active/Latent Effect
Field 5-Unit Status	Field 19-Performance Shaping Factors
Field 6-Noteworthy Plant Conditions	Field 20-Recovery Time
Field 7-Other Unit(s) Status	Field 21-Recovery Locus
Field 8-Human Action Number & Description	Field 22-Recovery Origin
Field 9-Responsible Personnel Type	Field 23-Related Automatic Equipment Response
Field 10-Event Activity	Field 24-Fission Products Barrier Breached/ Threatened
Field 11-Human Action Location	Field 25-Other Effects
Field 12-System Identification	Field 26-Event Initiator
Field 13-Component Identification	Field 27-Unique to Operating State
Field 14-Displays/Controls/Instruments Identification	Field 28-Corrective Action Taken

Using the HACS information fields, three data bases have been created for recording the analysis results of the analyses for LP&S PWR, LP&S BWR, and at-power events, respectively. Although relatively few events (i.e., 32 PWR LP&S events, 32 BWR LP&S events, 14 at-power events) have been analyzed so far, the data sources selected, especially event-based NRC reports, have been chosen for the unique depth and breadth of detail that they provide. In addition, work is continuing to add events and associated human performance information to the data bases.

Because of the number and variety of information fields contained in the HACS, analysis results encoded in the three data bases can be "sliced" or combined in numerous ways. The results and accompanying discussion given below specifically identify the insights that can be derived by viewing the data analyses in the context of the new HRA framework.

4.0 HRA FRAMEWORK

In PRAs for NPP, HRAs require consideration of a variety of factors, including the plant state (as represented in the PRA), the equipment being operated or maintained, human system interface aspects associated with the task(s) being performed as well as situation specific PSFs. While these factors have been implicitly incorporated in HRA studies performed to date, they have never been formally specified in any of the existing HRA methods. In order to address these HRA limitations and accommodate previously identified concerns associated with modeling EOCs and human dependencies (NUREG/CR-6093), it was necessary to develop an explicit framework of how HRA and PRA modeling are related.

The purpose of the HRA framework is to provide a logical and explicit basis for the development of rules for incorporating human failure events into PRAs that are consistent with knowledge about the consequences and rates of occurrence of different types of human errors. In order for the framework to best describe the relationships between human errors as considered in the behavioral sciences and human failure events as considered in the PRA systems-analysis tasks, an existing framework was selected and refined. The refinement is based on, and has been initiated by, the review of significant operational events as described above and the desire to make any new developments in HRA more representative of real-world events.

Once refined, this framework provided a basis for incorporating different kinds of human errors into the evaluation of various human failure events. It further provided an indication of the kinds of data relationships that will be required to produce a working HRA/PRA methodology. This framework, therefore, is essential for tasks involving the representation of EOCs and dependency as well as the quantification process which are discussed in Sections 5.0, 6.0, and 7.0 respectively. The following discusses the existing HRA framework and its development into the refined HRA framework.

4.1 Existing Framework

Figure 1 presents a description of the relationships between HRA and PRA activities as typically performed today. The building blocks of the PRA model are the basic events. These basic events include different failure modes of components and subcomponents that, in combination, lead to failures of systems. The basic events are combined in the fault trees according to the definitions of system and functional failures. Combinations of fault trees are represented in the PRA event trees according to the plant state being analyzed (such as a LOCA or other accident scenario) to describe combinations that lead to unacceptable accident conditions such as core damage.

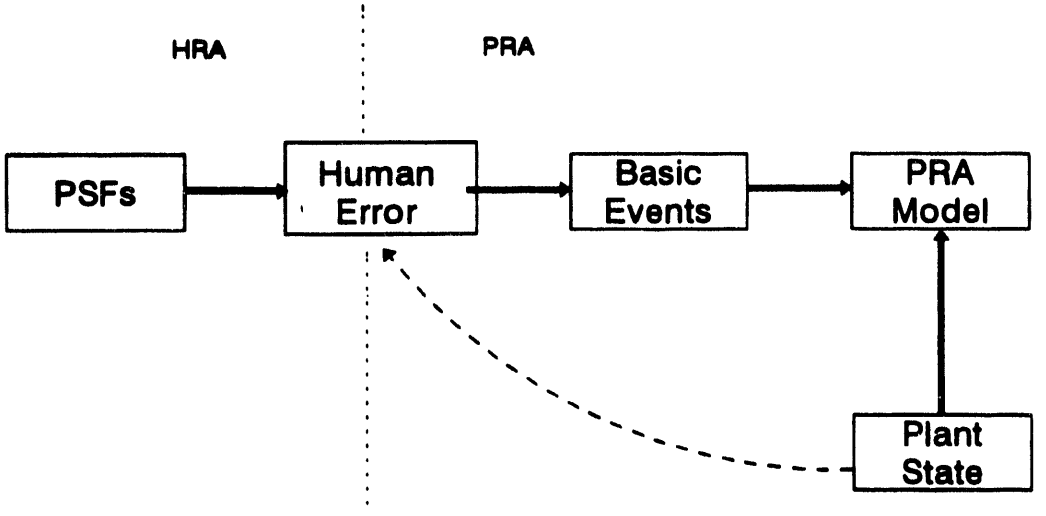


Figure 1. Existing HRA framework

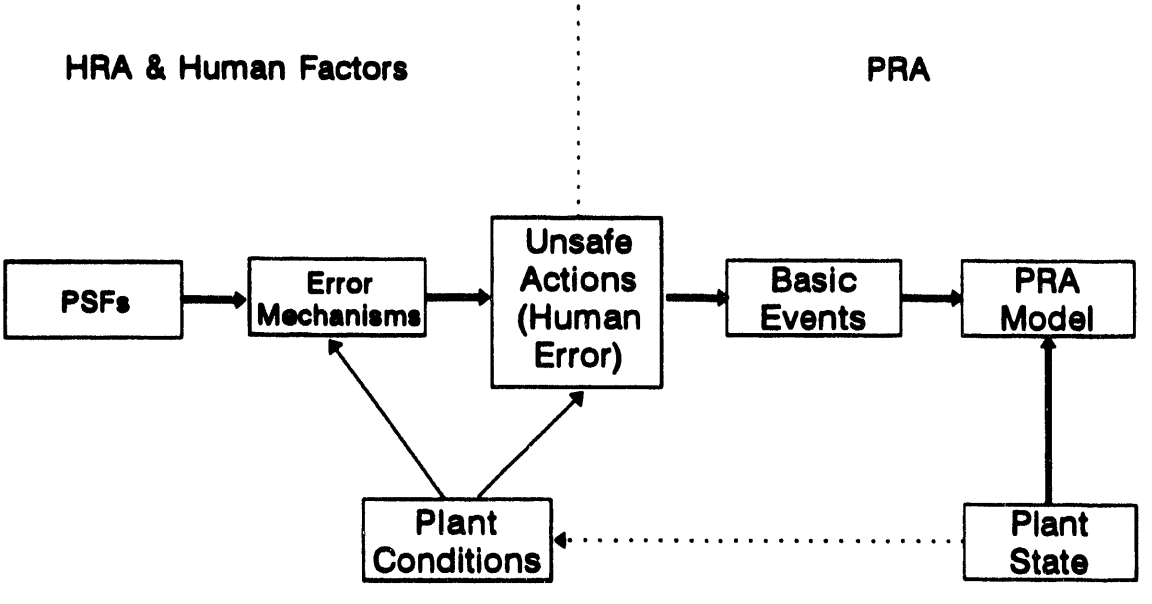


Figure 2. Refined HRA framework

In this framework, human errors are one of the constituents of basic events that lead to system or functional failures, as in "Operator fails to open recirculation suction valve" leading to failure of recirculation flow in a small-break LOCA.

These human errors, comprising basic events, are broadly undifferentiated; that is, no major differences between various errors are considered. They are, for the most part, identified simply with descriptions such as "Operator fails to _" or "Maintenance technician fails to restore _". In many PRAs they are evaluated on the basis of a small set of common PSFs. These PSFs, for example, have included the timescale for actions, the effectiveness of annunciators, and the ability of a second person checking the first. While some PRA studies have incorporated other PSFs, they have been primarily subjectively developed. In addition, these PSFs have been applied frequently to large groupings of human error events with little consideration as to the specific kinds of errors they cause or influence.

The human performance issues are addressed in the context of the accident scenario defined by the plant state in the PRA. For example, the final HRA quantification is performed on a "cutset-by-cutset" basis, especially where the quantification for post-accident responses is based on a timescale available for action. Cutsets are the boolean logic statements resulting from the event-tree models that define a unique combination of basic failure events that would cause the accident. One cutset may represent a combination of failures associated with a pump in one train and a valve in another train, and failure of the operators to restore operation. The timescale available for operators to recover the valve close to the control room in time to prevent core damage in that cutset (and hence the probability of recovery) may be quite different from a cutset that involved accessing some remote area of the plant. Although current PRAs do attempt to incorporate situation-specific factors that may influence human performance, improvements are necessary to more realistically accommodate the influence of plant state on human performance.

4.2 Refined HRA Framework

Figure 2 presents the elements of the refined framework as presently conceived. The refined HRA framework revises the relationships between human errors, their causes, and the basic events modeled in PRAs. The most important changes lie in the addition of explicit identification of multiple error mechanisms as causes of human errors, and the role that plant conditions play in forcing the occurrence of human errors.

Specifically, the revised framework describes relationships between the following elements: the PRA model (i.e., fault trees, event trees), plant states (i.e., those definitions or constraints on operational modes modeled, model assumptions, initiating events, etc.), plant conditions (e.g., LP&S-specific plant configurations, system unavailabilities), PRA basic events, unsafe acts, human error mechanisms, and PSFs.

The following discusses those framework elements that have been added or revised. These elements will be discussed in terms of: the change in terminology of "human errors" to "unsafe actions," the addition of error mechanisms, the refinement of PSFs and PRA basic event, and the addition of plant conditions, respectively.

4.2.1 Unsafe Actions

The term "human error" has been used interchangeably with "human failure event" by PRA analysts for nearly two decades. The term refers to a basic event involving a lack of action, or an inappropriate action, taken by operations, maintenance, or other staff member, that leads the plant to a

less-safe state. However, the term "human error", when used by behavioral scientists, can refer to quite different aspects in human behavior. These aspects can be in conflict with those intended by the PRA analyst. In particular, the PRA concern is only that an unsafe condition results; the reasons why that occurred are of generally limited concern to the PRA. In contrast, from the behavioral perspective, the consequence of the error is generally of limited interest when compared to the underlying causes of such error.

For the purposes of making explicitly clear the concern to the PRA, the refined framework does not refer to human errors, it refers instead to "unsafe actions." Unsafe actions are those actions taken by people that lead the plant into a less-safe state. Unsafe actions also include actions not taken (the so-called errors of omission). Unsafe actions imply nothing about whether the action taken (or not taken) was a "human error", to avoid the inference of blame or that the human was the root cause of the problem. As will be described later, people are often "set up" by circumstances and conditions to take the actions that were unsafe. In those circumstances, the human did not commit an error in the every-day sense of the term; they were doing what was the "correct" thing as it seemed at the time.

4.2.2 Error Mechanisms

The unsafe acts that are contributors to important PRA basic events can be considered the results of specific error mechanisms. The different error mechanisms defined in the refined HRA framework are: slips/lapses, mistakes, and circumventions. These different error mechanisms provide reasons for failing to perform an action, or performing some other unsafe act. Consequently, there are important differences between these error mechanisms, both as to the conditions under which they can occur and their potential impact on risk. The following provides a summary of the distinctions between the classes of error mechanisms, based on work by Reason (1990).

Slips and lapses lead to unsafe actions where the outcome of the action was not what was intended. Skipping a step in a procedure or reversing the numbers in an identification label are examples of lapses and slips, respectively. Both are errors associated with what has been termed skill-based level of performance. This level of performance is associated with the predominantly automatic control of routine and highly-practiced actions. The significance to risk of these error mechanisms seems to be quite small for the simple fact that these actions, not being as intended, are easily recognized by the person involved and (in most circumstances) easily corrected. HRA methods like the Technique for Human Error Rate Prediction (THERP) (NUREG/CR-1278) address slips and lapses as their primary focus.

For unsafe actions where the action was as intended, there are two broad classes of error mechanisms. The first is where, while the action was as intended, the intention was wrong. For example, the operator may have misdiagnosed the plant condition and is following the procedure for the wrong condition. The consequential actions are mistakes. The second is where a person decides to break some rule (even though the rule is known to them) for what seems to be a good (or at least benign) reason, such as reversing the steps in a procedure to simplify the task. Unsafe actions in this last category are circumventions. It should be noted that acts of sabotage are distinct from circumventions in terms of the intended consequence.

Mistakes can be considered rule-based or knowledge-based depending on whether the task is demanding rule-based or knowledge-based performance; that is, whether documented or trained instructions are being followed (as in almost all NPP activities important to safety) or whether the person involved is relying on technical and specialist knowledge (as in generalized troubleshooting). Rule-based mistakes are further subdivided as to whether the wrong rules are being followed (e.g., following misdiagnosis), or the rules are the "correct" ones but contain omissions or errors.

Mistakes are perhaps the most significant to risk because they are being followed purposefully by the user, who has limited cues that there is a problem. Indications contradicting the erroneous diagnosis are often dismissed as for instance, "instrument errors." Often it takes an outsider to the situation to identify the nature of the problem as happened at Three Mile Island. Existing HRA methods address slips/lapses and, to a lesser extent, mistakes. However, mistakes are the dominant error mechanism for LP&S conditions, as documented in both the PWR and the BWR LP&S HACS data bases.

Circumventions are potentially significant contributors to risk in that unanalyzed conditions can result from unexpected combinations of errors and circumventions. However, two conditions seem to mitigate this potential. First, the person committing the circumvention is (usually) aware that the action has occurred and can bring any significant consequence to the attention of other staff (attitudes to punishment can heavily influence this self-reporting, however). Second, in the current environment in the nuclear industry, circumventions seem to be a relatively rare occurrence.

4.2.3 Performance Shaping Factors

As previously stated, existing HRA methods recognize, usually implicitly, a relatively small set of influences on human performance, i.e., PSFs. In addition, current HRA quantification methods are typically driven by a single, dominant PSF (e.g., time available for response).

Given the differences between the possible error mechanisms that could be the cause of one unsafe action, the use of a single set of PSFs for all mechanisms is inappropriate. Each error mechanism has its primary set of PSFs. A salient feature in the refined HRA framework is the recognition that different PSFs may apply to different error mechanisms. For example, based on the analysis of actual events, important PSFs for slips and lapses, included workload and fatigue, the format of job aids, the availability of appropriate memory helpers (checklists, mnemonics, etc.) and calculators. For rule-based mistakes involving inadequate procedures, PSFs associated with the technical validity and completeness of procedures or work orders, and coordination of multiple work groups, were found to be important. The rate and location of circumventions was found to be strongly influenced by the task design, the occurrence of incompatible goals or requirements, and the rewards/penalties system for compliance.

The important point from the event analyses is that no single set of PSFs apply to all error mechanisms, and that using a single set of PSFs would only be appropriate if that error mechanism was the most risk-significant. The refined framework provides for an expanded list of PSFs and the explicit consideration of multiple PSFs. As observed in the LP&S PWR event analyses, the majority of EOCs, both slips and mistakes, were found to be influenced by multiple PSFs.

4.2.4 PRA Basic Events

Traditionally, there are three types of basic events included in PRA models, which represent human errors: pre-accident (or latent) and post-accident human failure events and non-recovery actions. Although human-induced initiators are recognized as possible initiating event causes, the frequency of human initiators for at-power events has typically been small compared to hardware-caused initiators. Consequently, it has been considered sufficient to capture both human and hardware failures in the initiating event frequency data for at-power PRAs. This review and analysis of actual plant-specific event has indicated that human actions are the dominant contributor to LP&S initiators. Thus basic events should accommodate the unique aspects of human action initiators.

4.2.5 Plant Conditions

Starting with the PRA basic event (involving some unsafe action), events occur with the combinations of an unsafe act ("operator fails to ...", "technician inadvertently ...") and a plant condition in which that unsafe act has risk-significant consequences. For example, operators terminating operation of a heat-removal system in the condition of significant decay-heat levels is an event of importance in a PRA, but under other conditions, or involving other systems, the same unsafe act may not be a PRA basic event. Therefore, unsafe acts must be considered in combination with the plant conditions in which they are risk-significant.

Plant conditions are the specific features of the plant and its operating state that can influence human actions performed and can create opportunities for unsafe actions. For example, draindown operations in a PWR LP&S refueling outage requires many manual actions by operators under conditions of limited instrumentation alarms etc. Conversely, maintaining a reactor at-power requires only a few manual actions (such as performing surveillance tests). To some degree these conditions are implicit in the plant state defined in the PRA. However, the specific human interactions with the plant are not defined traditionally in the PRA, especially for actions that could lead to initiating events or other errors of commission.

A detailed description of plant conditions is necessary to identify the possible situations where people are almost forced into failure. The influence of plant conditions can be seen from the frequent and continuous human interventions with the plant during LP&S operations. For example, combinations of workload, ambiguous task requirements/instructions, and a lack of supervision led a situation where operators overdrained the reactor water level beyond midloop within 8 hours of shutting down the reactor (Prairie Island, Unit 2, in February 1992). This example indicates the level of specification for plant conditions necessary to be identified in order to potentially define the conditions under which humans are more likely to fail. It is this level of plant condition description that enables the important identification of, for instance, EOCs, which primarily result from errors during periods of intervention with the plant (such as changing power levels, performing surveillance testing, or maintaining LP&S conditions).

5.0 ERRORS OF COMMISSION

For purposes of this research project an error of commission is operationally defined as ***an overt unsafe human action that leads to a change in plant configuration with the consequence of a worsened plant state.*** EOCs are identified as a critical area for HRA development. The principal reason for this identification is that the state-of-the-art in HRA does not address EOC modeling. Consequently, EOCs are not currently captured in PRAs. However, the data analyses have shown EOCs to be dominant contributors to risk especially in analysis of actual LP&S events. The fundamental characteristics of EOCs are being examined, in an on-going task in order to develop EOC modeling methods.

Specific examples of EOCs identified in the plant specific event analyses include:

- RCS overdraining resulting in loss of shutdown cooling;
- Erroneous termination of safety injection;
- Other actions performed under conditions not well covered by procedures, training, instrumentation.

The event data represented in the LP&S HACS databases indicated that EOCs are the dominant unsafe action mode. Furthermore, EOC human initiators were found to be more prevalent than EOO human initiators. On the other hand, the majority of EOCs committed during at-power events are non-initiators (i.e., either pre-accident or post-accident). EOCs, in general, and EOC initiators, in particular, should be considered in new HRA methods.

In addition, mistakes have been found to be the predominant error mechanism of EOCs while slips have been found to be the predominant mechanism for EOOs. Since slips are more commonly modeled in at-power PRAs, new HRA methods, which address LP&S, must also include consideration of EOCs that result from mistakes.

6.0 HUMAN DEPENDENCY

Human dependency can be characterized by two or more PRA Basic Events (a,b) involving human actions whose failure probabilities are not independent and therefore causes the probabilistic relationship $P(a,b) \neq P(a) \times P(b)$ to be true. Some examples of human dependencies being examined include:

- direct dependence on some common external process (e.g., procedure-writing or planning);
- multiple tasks dependent on common PSFs such as supervision, training, and procedures;
- multiple actions dependent on a single rule-based mistake (e.g., misdiagnosis);
- task-sequential dependencies where errors in performing task A influences reliability of subsequent task B; and
- direct task interactions, such as failure in Task A causing failure in Task B (e.g., error in calibrating level sensors causing incorrect level measurement, which fails operation of mitigating systems).

There are several different kinds of dependence mechanisms that can cause these relationships. For this project the dependence mechanisms being investigated in an on-going task, are those that influence multiple human actions. These include common processes, common PSFs, and other local task dependencies. Each of these dependence mechanisms is discussed below.

Common processes are those that, by their nature, are common-mode influences to whole groups of human actions. These include: management decisions; work organization, planning and scheduling; and other programmatic functions (e.g., procedure development) within the plant. Deficiencies in these processes can lead to poor or erroneous performance simultaneously in many plant departments (e.g., operations, maintenance), and between work teams within departments. One simple example is the case where a lack of work planning led to the simultaneous performance of maintenance of two redundant trains of diesel generators during a refueling outage. A second example is the development of technically inaccurate procedures within the procedure-writing function, that led to errors in performance by both operations and maintenance.

The category of common PSFs relates to the potential effects of such influences as common procedures, common human-systems interfaces (e.g., work environment), and common training programs. Common PSFs can also include poor morale or behavioral norms which, for example, can be important

for circumventions. These common PSFs have the potential, if less than adequate, of causing a significant increase in the failures probabilities for those human actions affected by them.

An example of such a common PSF was during the event at Oconee Unit 3, in March of 1991. In that event, a sequence of errors occurred that were largely (though not exclusively) the result of several operators separately being misled by an erroneous label (i.e., poor human-systems interface). That label was not the formal plant label (which was very difficult to observe), but nonetheless misled both the operators installing the blind flange and different operators later checking the installation.

In addition to common processes and common PSFs are the local task dependencies. These are aspects of the job and the task that result in the probabilities of failure no longer being independent. Examples could include the influence of a common supervisor, the work being performed in a common area, or the consequences of timing or interdependencies from one action or failure on another. For example in the Oconee event, the occurrence of the failure to properly check the blind flange installation, led to the opportunity for the subsequent testing crew to fail. If the first task had been performed correctly, the later failure would have become moot. This dependence is common with many redundant tasks.

7.0 CONCLUSIONS

The following subsections discuss the status of this research project with respect to results to date, implications of the refined framework, and follow on efforts.

7.1 Results To-Date

Key findings from the actual plant-specific event analyses include:

- Human actions are significant contributors to risk during LP&S operations;
- Human-induced initiators comprise a significant portion of the observed unsafe actions;
- Mistakes (versus slips) and errors of commission (versus omission) predominate the error mechanisms and modes of unsafe human actions which occur during LP&S (when compared to at-power operations);
- There are frequently dependencies between human actions, which should be addressed in addition to hardware dependencies;
- The most frequently cited PSFs are procedures and human engineering;
- Human actions influenced by multiple PSFs were found to be present in most events of significance;
- PSFs and unsafe actions appear to be very sensitive to the context of the plant conditions; and
- Recovery is frequently aided by situation-appropriate PSFs such as procedures, training, and the technical knowledge of the operations and management personnel.

These results provide the focus for HRA methods development to address the associated deficiencies in current HRA methods which were previously developed and used in PRAs for at-power conditions.

7.2 Implications of Framework for HRA Methods

The insights obtained from the plant-specific event analyses, and in the context of the refined HRA framework, have several implications with respect to the development of new HRA methods. These include:

- HRA methods must be capable of evaluating a range of different error mechanisms, not just those for which data are readily available. For example, many HRA methods provide data for slips and lapses. None provide ways of quantifying rule-based mistakes involving technically deficient procedure, which is perhaps one of the most risk significant mechanisms;

- Both error modes, commission and omission, must be addressed by new HRA methods, especially in order to realistically model LP&S conditions;

- Dependencies between human actions, should be addressed by new HRA methods;

- Plant conditions must be considered in HRA methods: in the determination of what basic events are appropriate to model, in the identification of opportunities for unsafe acts (e.g., EOCs), and in the determination of likely error mechanisms and their associated PSFs;

- New HRA methods must recognize that unsafe acts frequently are influenced by multiple PSFs and that different PSFs may be important to different error mechanisms.

7.3 Follow On Efforts

Once the examination of EOCs and Dependency is completed, the effort for quantification process development will commence followed by the development of implementation guidelines. Finally, a demonstration of the methodology using the guidelines will be conducted by PRA/HRA analysts on appropriately selected events for a BWR and PWR. This demonstration will be used to assess the usefulness and understandability of the guidelines including, their ease of implementation and consistency with expectations and other PRA/HRA results.

Some potential applications also being considered for the refined HRA framework and event analysis approach/results include:

- General improvements in the understanding of human contributions to safety (ultimately addressing both PWRs and BWRs, for both LP&S and at-power operations);

- Identification and analysis of trends of events with respect to human performance and its contribution to risk;

- Identification of potential improvements that can be made in outage planning and management;

- Identification of potential human reliability improvements that can be made through changes to for instance, procedures, training, human engineering, and organizational processes;

- Increased understanding of influences on human performance outside the control room which may be applicable to maintenance activities for both LP&S and at-power conditions.

In addition, since the data analyses of "real" events performed for this project have identified gaps between current PRA methods and the "real world," the development of analytical methods to fill these gaps may be critical to the transition to regulation on the basis of operating experience, i.e., performance-based regulation.

REFERENCES

NUREG-1449, "Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States," Draft Report for Comment, U.S. Nuclear Regulatory Commission, February 1992.

NUREG/CR-6093, "An Analysis of Operational Experience During Low Power and Shutdown and A Plan for Addressing Human Reliability Assessment Issues," to be published.

Reason, James T., Human Error, Cambridge University Press, 1990.

RESULTS AND INSIGHTS OF A LEVEL-1 INTERNAL EVENT PRA OF A PWR DURING MID-LOOP OPERATIONS*

T.L. Chu,[1] Z. Musicki,[1] P. Kohut,[1] J. Yang,[1] B. Holmes,[2] G. Bozoki,[1] C.J. Hsu,[1] D.J. Diamond,[1] S.M. Wong,[1] R.F. Su,[3] V. Dang,[3] N. Siu,[3] D. Bley,[4] D. Johnson,[4] and J. Lin[4]

[1]Department of Advanced Technology
Brookhaven National Laboratory
Upton, N. Y. 11973

ABSTRACT

Traditionally, probabilistic risk assessments (PRA) of severe accidents in nuclear power plants have considered initiating events potentially occurring only during full power operation. Some previous screening analysis that were performed for other modes of operation suggested that risks during those modes were small relative to full power operation. However, more recent studies and operational experience have implied that accidents during low power and shutdown could be significant contributors to risk.

During 1989, the Nuclear Regulatory Commission (NRC) initiated an extensive program to carefully examine the potential risks during low power and shutdown operations. The program includes two parallel projects being performed by Brookhaven National Laboratory(BNL) and Sandia National Laboratories(SNL). Two plants, Surry (pressurized water reactor) and Grand Gulf (boiling water reactor), were selected as the plants to be studied.

The objectives of the program are to assess the risks of severe accidents initiated during plant operational states other than full power operation and to compare the estimated core damage frequencies, important accident sequences and other qualitative and quantitative results with those accidents initiated during full power operation as assessed in NUREG-1150. The scope of the program includes that of a level-3 PRA.

The objective of this paper is to present the approach utilized in the level-1 PRA for the Surry plant, and discuss the results obtained. A comparison of the results with those of other shutdown studies is provided. Relevant safety issues such as plant and hardware configurations, operator training, and instrumentation and control is discussed.

[2] AEA Technology
[3] M.I.T. (N. Siu currently at INEL)
[4] Pickard, Lowe and Garrick

---

* This work was done under the auspices of the U.S. Nuclear Regulatory Commission.

INTRODUCTION

Traditionally, probabilistic risk assessments (PRA) of severe accidents in nuclear power plants have considered initiating events occurring only during full power operation. Some previous screening analyses that were performed for other modes of operation suggested that risks during those modes were small relative to full power operation. However, more recent studies and operational experience have implied that accidents during low power and shutdown could be significant contributors to risk.

During 1989, the Nuclear Regulatory Commission (NRC) initiated an extensive program to carefully examine the risks during low power and shutdown operations. The program includes two parallel projects being performed by Brookhaven National Laboratory (BNL) and Sandia National Laboratories (SNL). Two plants, Surry (pressurized water reactor) and Grand Gulf (boiling water reactor), were selected as the plants to be studied.

The objectives of the program are to assess the risks of severe accidents initiated during plant operational states other than full power operation and to compare the estimated core damage frequencies, important accident sequences and other qualitative and quantitative results with those accidents initiated during full power operation as assessed in NUREG-1150[1]. The scope of the program includes a level-3 analysis.

A phased approach was used in the level-1 program. In phase 1 which was completed in Fall 1991, a coarse screening analysis including internal fire and flood was performed[2]. The objective of the phase 1 study was to identify potential vulnerable plant configurations, to characterize (on a high, medium, or low basis) the potential core damage accident scenarios, and to provide a foundation for a detailed phase 2 analysis.

Mid-loop operation was selected as the plant configuration to be analyzed in phase 2, based on the results of the phase 1 study. The objective of the phase 2 study is to perform a detailed analysis of the potential accident scenarios that may occur during mid-loop operation, and compare the results with those of NUREG-1150. The scope of the level-1 study includes plant damage state analysis, uncertainty and sensitivity analysis. Internal fire and internal flood analyses are also included. A separate study on seismic analysis is being performed for the NRC by Future Resources Associated, Inc. and PRD Consulting.

The objective of this paper is to present the approach utilized in the level-1 internal events PRA for the Surry plant, and discuss the results obtained. The work on internal fire, internal flood, and seismic analysis will be published separately.

METHODOLOGY

Due to the changing plant configuration during low power and shutdown operation, it was necessary to define different outage types and different plant operational states (POSs) within each outage type. Within each POS, the plant configuration continues to change with time, and the decay heat continues to

decrease. These factors significantly affect scenario frequencies. Therefore, a "time window" approach was developed. In this approach, different time windows representing different decay heat levels and success criteria within each time window, were defined.

Within each time window, the approach used in performing the PRA for a particular POS in a particular outage type is similar to that used in the NUREG-1150 study. The approach includes typical tasks such as identification of initiating events, development of fault trees and event trees, and quantification. The following is a summary of the approach used in those tasks that are characteristic of this shutdown study.

Outage Types, Plant Operational States, and Time Windows - Outages were grouped into four different types: refueling, drained maintenance, non-drained maintenance with use of the residual heat removal(RHR) system, and non-drained maintenance without the use of the RHR system. Due to the continuously changing plant configuration in any outage, plant operational states (POSs) were defined and characterized within each outage type. Each POS represents a unique set of operating conditions (e.g. temperature, pressure, and configuration). For example, in a refueling outage, up to 15 POSs were used. They represent the evolution of the plant throughout a refueling from low power down to cold shutdown and refueling, and backup to low power. An extensive effort was made to collect Surry-specific data needed to characterize each POS. This included review of operating and abnormal procedures for shutdown operations, review of shift supervisor's log books, review of monthly operating reports, and performing thermal-hydraulic calculations. Three mid-loop POSs, in which the reactor coolant system (RCS) level is lowered to the mid-plane of the hot leg, were selected for detailed analysis. Two of them occur in a refueling outage, (POSs R6 and R10), and one in a drained maintenance outage, (POS D6). They are characterized by different decay heat level, and different plant configurations, such as the number of RCS loops that are isolated, and whether or not the RCS has a large vent. R6 represents a mid-loop operation that takes place early in a refueling outage. This mid-loop operation allows fast draining of the RCS loops to permit eddy current testing of the steam generator tubes. R10 takes place after the refueling operation is completed to allow additional maintenance of equipment in the RCS loops. D6 represents a mid-loop operation in which maintenance activities require the plant to go to mid-loop, and is characterized by the highest decay heat level among the three mid-loop POSs.

In order to more accurately define the decay heat level when an accident is initiated, a time window approach was developed. Table 1 is a summary of the success criteria for the time windows. A total of 4 time windows after shutdown were defined, each with its own unique set of success criteria reflecting the decay heat level. For POSs R6 and D6, all 4 windows were needed. For POS R10, only time windows 3 and 4 were applicable. A statistical analysis on the time to mid-loop and the duration of mid-loop was performed to determine the probability that a given accident occurs in a particular time window, conditional on the accident occurring. In this approach, an event tree was developed for each accident initiating event, POS, and time window. For 16 initiating events, a total of 160 event trees were developed.

Definition of Time Windows Based on Supporting Thermal-Hydraulic-Analysis - The main purpose of the thermal-hydraulic analysis was to support the event tree development and accident sequence quantification. Thermal-hydraulic considerations are the basis of the time window approach. The time windows were defined based on the times when the success criteria of important mitigating functions change. Detailed calculations were done to determine the timing of a feed and bleed operation during mid-loop operation. The calculation also provided information on the amount of refueling water storage tank (RWST) water needed to sustain the feed and bleed operation, as well as the timing of core uncovery for different initial conditions. The MELCOR[3] code was also used to assess whether or not gravity feed from the RWST could be used to provide long term cooling (i.e. 24 hours, decay heat removal). For the case of reflux cooling, the results of studies at the Idaho National Engineering Laboratory (INEL), Westinghouse, and Virginia Power were reviewed and used to determine the success criteria. The results of the analysis of feed and spill, gravity feed and reflux cooling were used to determine the boundary of the time windows. For example, the time boundary between windows 2 and 3 was chosen to be the time when recirculation is not necessary for the first 24 hours after the accident started. It was estimated to be 10 days based on the inventory available in the RWST and the flow needed in the feed-and-spill operation.

Initiating Event Analysis - The approached used to identify potential initiating events, was to review existing studies, search licensee event reports, (LERs), review published NRC documents, and review current Surry operating procedures. This approach should ensure that any incident that has occurred or any scenario that has been studied will be considered in the present study. However, a systematic approach, such as a failure mode and effect analysis (FMEA) or a hazard and operability study (HAZOP), was not used to provide further assurance that all possible initiating events in all possible operating states have been identified.

Event Tree Analysis - In phase 1 of this study, accident scenarios were developed for all Low Power and Shutdown POSs. For those POSs that are similar to power operations, (e,g, low power operations), the relevant NUREG-1150 event trees were reviewed and modified (if necessary) to reflect the current plant design and operation. For other POSs, event trees were developed in the course of group discussions, involving typically four or more BNL staff members with expertise in PWR operations, PRA, human reliability analysis (HRA) and thermal-hydraulic molding. Communications with staff at Virginia Power were established to clarify questions on the plant design and operations.

In phase 2, the event trees developed for the mid-loop POSs were reviewed and modified to incorporate additional information obtained in the system analysis and to reflect the current understanding of the expected operator responses to the accidents. A two-day meeting with Virginia Power operations personnel was held to discuss the potential accident scenarios, and the expected plant and operator responses.

System Analysis - The fault tree models developed as part of NUREG-1150 study were reviewed and modified, when necessary, to develop fault tree models for the

plant at shutdown as well as during low power operation. Typically, two fault trees were developed for each system. One tree is applicable to power operations, and the other is applicable to shutdown conditions. The system configuration during shutdown was identified by reviewing the operating procedures used during shutdown, shift supervisor's log books, and the system training manual. Typically, the following changes were made to NUREG-1150 fault trees to derive the fault trees applicable to shutdown conditions.

1) Valve failure modes were changed. The position of valves during shutdown may be different from that during power operation. Therefore, the applicable failure modes of the valves will be different from those of power operations.

2) Human error events associated with backup of automatic actuated systems or components which failed were modified to manual actuation with no automatic backup.

3) Maintenance unavailabilities relevant to the specific POS were estimated. For mid-loop POSs, the reduced inventory check list was used to determine whether certain maintenance events are permitted. Those maintenance events prohibited by the check list, e. g. diesel generator maintenance, during mid-loop were deleted from the model.

4) System success criteria were changed if necessary.

Human Reliability Analysis - Two types of human error events were identified and modeled in this study: pre-accident errors and post-accident errors. For pre-accident errors, those identified in the NUREG/CR-4550 study for Surry were adopted. Additional pre-accident errors were identified in the system analysis task and were added to the system fault trees.

The approach to evaluating human actions and recovery actions that follow an initiator is first to qualitatively define the event scenario, required action, important factors affecting operator performance, and the consequences of the action not being successful.

The qualitative evaluation of the actions and the important parameters that affect operator performance were used to derive the human error probabilities (HEPs) using an adaptation of the success likelihood index methodology. This methodology is based on the assumption that the likelihood of operator error in a particular situation depends on the combined effects of a small set of performance-shaping factors (PSFs) that influence the operator's ability to accomplish the action.

Data Base Analysis - An extensive effort was devoted to collecting data for characterizing the plant during shutdown. The effort involved compiling a of a data base of initiating events, and reviews of the shift supervisor's log books, outage schedules, minimum equipment list, and monthly operating report to collect the data needed to estimate the frequency of shutdown, duration of plant operational states, and maintenance unavailabilities.

RESULTS AND INSIGHTS

Table 2 is a comparison of the results of this study with those of NUREG-1150 and the individual plant examination (IPE) performed by the utility for Surry. The table displays the results in two ways. The core damage frequency is the frequency that core damage occurs when the plant is at mid-loop, and the instantaneous core damage frequency is the core damage frequency divided by the fraction of time the plant is at mid-loop. The former accounts for the fact that the plant is at mid-loop only a small fraction of the time, while the latter is the frequency at which core damage occurs given that the plant is at mid-loop. It can be seen that the core damage frequency of mid-loop operations is approximately one eighth of that of power operation as estimated in NUREG-1150, while the plant is in mid-loop operation less than 7% of a year. Table 3 shows the frequency that core damage occurs for each combination of time windows and POSs. It can be seen that the frequency decreases with time window/decay heat, due to relaxing success criteria and increasing the frequency for R6 is higher than that of D6 due to the fact that the RCS loops may be isolated in R6 making reflux cooling impossible. The difference between the results of R6 and R10 is due to the difference in maintenance unavailability.

The following are insights derived from this study:

Changing plant practices and information - The plant is aware of the potential safety concerns of reduced inventory operations and is constantly improving its practice regarding such operation. This is reflected in the improvement in the operating procedures and abnormal procedures used during shutdown as well as changes in the plant practice. The most significant change in plant practice started in the refueling outage of unit one in 1992, during which mid-loop operation was totally avoided. This appears to be the new plant policy. Another way of reducing the risk due to reduced inventory operation is to perform it while the fuel in the core is removed during the refueling operation.

In order to limit the changes in the model developed for this study to account for the changes in plant practice and information, it was decided that the study will use the procedures and other plant information available as of April 30, 1993. Regarding the plant's policy of avoiding mid-loop operation, it was decided that this study would use the data collected from past outages prior to the unit 1 refueling outage of 1992. As a result, the estimated core damage frequency reported for this study is expected to be an over estimation. It is emphasized, however, that the core damage frequency quoted in Table 2 has been reduced significantly as a result of changes made before April 1, 1993.

Operator Response - The dominant cause of core damage was found to be operator failure to mitigate the accident. It should be mentioned that there is very large uncertainty in the human error probabilities currently used in this study. In general, it would be beneficial to have good training, procedures, and instrumentation to ensure that the utility staff are able to respond to shutdown accidents.

Procedures for Shutdown Accidents - Very few procedures are currently available for accidents during shutdown. The loss of decay heat removal procedure, (AP 27), is the only procedure that was written specifically for shutdown conditions. It was found that the procedure is conservative with regard to the equipment needed to establish reflux cooling and feed-and-bleed. In this study, the use of less than the number of steam generators specified in the procedure for reflux cooling was treated as a recovery action, and a more realistic success criteria was used for feed-and-bleed when the decay heat is high. In most cases, the information in the procedures for power operation was helpful, if used for shutdown accidents. However, some procedures written with power operation in mind would mislead the operator if followed during shutdown.

Instrumentation - It was recognized that the level instrumentation used during mid-loop operation, i.e., standpipe level instrumentation and ultra-sonic level instrumentation, have limited applicability during a shutdown accident. The standpipe system provides correct level indication only when there is no pressure build-up in the system. The ultra-sonic level instrumentation only provides level indication when the level is within the reactor coolant loops. This level instrumentation may not therefore be useful during a feed and bleed operation.

Supporting Thermal Hydraulic Analysis - It was found that the thermal hydraulic behavior of the reactor coolant system is rather complex. This is mainly because the pressurizer is usually the relief path for coolant or steam, and the vessel head does not have a large vent. When performing thermal hydraulic analysis in support of the PRA effort, consideration has to be given to longer term system behavior, at least 24 hours into the accident. In this study, such calculations were done for feed-and-bleed operation using a charging pump, and with gravity feed from the RWST. It is believed that additional supporting calculations would be helpful for a better understanding of the effectiveness of reflux cooling, and feed and bleed using a low pressure injection pump.

Maintenance Unavailability - Based on a review of shift supervisor's log books and minimum equipment lists for three refueling outages, the maintenance unavailabilities of equipment that can be used to mitigate an accident were found to be very high. As a result of the requirement of generic letter 88-17, the plant is required to have one high head pump and one low head pump available. In the quantification of this study, it was assumed that charging pump A, charging pump cooling water pump A, and low head injection pump A are available. Based on the check list used for reduced inventory conditions, it was also assumed that maintenance of diesel generators, 4 kv emergency buses, and stub buses is not allowed.

It was found in this study that maintenance unavailability is the dominant cause of equipment unavailability. In combination with human errors, maintenance of the charging pump cooling water pump, the charging pump, and the low head injection pump appear in the dominant cutsets for some of the core damage sequences.

Isolation of Reactor Coolant Loops - In this study, it was found that isolation of the RCS loops is an important contributor to the core damage frequency.

Review of the plant shutdown experience indicated that the reactor coolant loops are isolated for extended periods of time during a refueling outage. This practice makes the steam generators unavailable for decay heat removal upon loss of RHR. During mid-loop operation, the availability of the SGs makes reflux cooling a possible method of mitigating a loss of RHR. This might be the only mitigation function available in a station blackout.

Single Failures of the RHR System - The RHR system at Surry is not a safety related system (i.e., it does not perform the safety injection function in scenarios initiated at full power). As a result, many single component failures can cause loss of RHR.

Valve Arrangement of Auxiliary Feedwater System and Main Steam System During Shutdown - The auxiliary feedwater system has six MOVs (151A, B, C, D, E, and F) inside the containment in the flow path to the steam generators, that are normally closed during shutdown. They would become difficult to locate during a station blackout. Similarly, the main steam non-return valves are normally closed during shutdown, and have to be opened in order to use steam dump to the condenser. They depend on offsite power as their motive power and would be very difficult to open without it.

Potential for Plugging the Containment Sump When Recirculation Is Needed - Due to activities inside the containment, transient material and equipment are brought into containment during shutdown. For example, large plastic Herculite sheets are often used to separate work areas from the rest of the containment. When an accident requiring recirculation from the containment sump occurs, as is the case in time windows 1 and 2, the transient material would increase the potential for plugging the containment sump.

CONCLUSION

The results of this study show that the core damage frequency during mid-loop operation is comparable to that of power operation. It is recognized that very large uncertainty exists in the human error probabilities currently used in this study.

A comparison of the results for the three mid-loop POSs shows that it is preferable to enter mid-loop when the decay heat is relatively low. This study identified that only a few procedures are available for mitigating accidents that may occur during shutdown.

This study assumed that the reduced inventory check list was followed, and found that the maintenance unavailability of equipment not on the list were dominant contributors to system unavailability. However, it is believed that the check list is sufficient for ensuring the availability of essential equipment.

Table 1. Definition and Characterization of Time Windows

	WINDOW 1	WINDOW 2	WINDOW 3	WINDOW 4
Definition	<= 75 hours	> 75 hours and <= 240 hours	> 240 hours and <= 32 days	> 32days
Representative Decay Heat	13.23 MW(2days)*	10 MW(5 days)	7 MW(12 days)	5 MW(32 days)
Success Criteria				
Reflux Cooling	3 SGs	2 SG	2 SG	1 SG
Feed and Bleed				
LHSI	1LHSI*(SV removed + 2 PORV)	1LHSI*(SV removed + 2 PORV)	1LHSI *(SV removed + 1PORV)	1LHSI *(SV removed + 1PORV)
HHSI	1HHSI*(SV removed + 1 PORV)	1HHSI*(SV removed + 1 PORV)	1HHSI*(SV removed + 1 PORV)	1HHSI*(SV removed + 1 PORV)
Gravity Feed	1 SV removed * LHSI flow path provides 4.3 hours for operator actions (with less than 2 hours of subcooling)	1 SV removed * LHSI flow path provides 6.5 hours for operator actions (with 2 hours of subcooling)	1 SV removed * LHSI flow path provides 12 hours for operator actions (with 2 hours of subcooling)	1 SV removed * LHSI flow path provides sufficient cooling for 24 hours (with more than 3 hours of subcooling)
Recirculation	needed(HPR + LPF&Steam + LPF&Spill)	1 RWST,needed	not needed	not needed
		2 RWST, not needed		
Recirculation Spray	needed	1 RWST,needed	not needed	not needed
		2 RWST,not needed		
Probability that IE Occurs in the Window				
D6	0.117 (0.31)*	0.436 (0.454)	0.375 (0.21)	7.20E-02 (2.6E-02)
R6	1.7E-02 (5.82E-02)	0.543 (0.7)	0.41 (0.24)	3.4E-02 (1.48E-03)
R10	0.0	0.0	0.016 (2.2E-02)	9.84E-01 (0.98)
* applicable to over-draining initiating event only, based on time to mid-loop				

Table 2

Comparison of Total Core Damage Frequency with NUREG-1150 and IPE

Study	Results				
PWR Low Power and Shutdown Study (Mid-Loop POSs, Internal Event Only)		R6	R10	D6	TOTAL
	CDF* (per year)	1.45E-06	3.12E-07	3.12E-06	4.88E-06
	Fraction of a year the plant is in mid-loop	1.63E-02	1.52E-02	3.49E-02	6.64E-02
	Instantaneous CDF** (per year)	8.88E-05	2.05E-05	8.94E-05	7.35E-05
NUREG-1150 (Internal Events Only)	4.01E-05				
IPE (Internal Events Only)	7.40E-05				

* CDF reflects the fraction of time the plant is at mid-loop
** Frequency of core damage given that the plant is at mid-loop

Table 3

Frequency that Core Damage Occurs Given in the POS and Window (per year)

Frequency that Core Damage Occurs Given in the POS and Window (per year)			
	R6	R10	D6
Window 1	8.59E-04	-	3.28E-04
Window 2	8.16E-05	-	6.06E-05
Window 3	6.17E-05	6.62E-05	5.32E-05
Window 4	1.81E-05	1.97E-05	1.01E-05
NUREG-1150	4.01E-05		

REFERENCES:

1. U. S. Nuclear Regulatory Commission, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, Vols. 1-3, December 1990.
2. T. Chu, et., al., "PWR Low Power and Shutdown Accident Frequencies Program, Phase 1A-Coarse Screening Analysis," Rough Draft Letter Report, November 13, 1991.
3. Summers, R.M., et. al., "MELCOR 1.8.0: A computer code for Nuclear Reactor Severe Accident Source Term and Risk Assessment Analysis." NUREG/CR-5531, Sandia National Laboratories, Albuquerque, NM, January 1991.
4. Naff, S.A., et. al., "Thermal-Hydraulic Processes During Reduced Inventory Operation with Low Residual Heat Removal," NUREG/CR-5855, Idaho National Engineering Laboratory, April 1992.
5. Fletcher, C.D., et. al., "Thermal-Hydraulic Processes involved in Loss of Residual Heat Removal During Mid-Loop Operation, EGG-East-9337," Idaho National Engineering Laboratory, October 1991.
6. Wald, L.W. and W.C. Arcieri, "Consequence of the Loss of Residual Heat Removal System Pressurized Water Reactors," NUREG/CR-5820, Idaho National Engineering Laboratory, May 1992.
7. T.S. Audreycheck, et. al., "Loss of RHR Cooling while the RCS is Partially Filled," WCAP-11916, Westinghouse Electric Corporation, July 1988.
8. "Background and Guidance For Ensuring Adequate Decay Heat Removal when RCS Loops are closed, Surry and North Anna Power Stations," NE Technical Report No. 865, Virginia Power, December 1991.
9. "Analysis of Core Damage Frequency: Surry Unit 1, Internal Events," NUREG/CR-4550, Vol. 3, April, 1990.

IPE DATA BASE STRUCTURE AND INSIGHTS*

J. Lehner and R. Youngblood
Department of Advanced Technology
Brookhaven National Laboratory
Upton, NY 11973

ABSTRACT

A data base (the "IPE Insights Data Base"), has been developed that stores data obtained from the Individual Plant Examinations (IPEs) which licensees of nuclear power plants are conducting in response to the Nuclear Regulatory Commission's (NRC) Generic Letter GL88-20. The data base, which is a collection of linked dBase files, stores information about individual plant designs, core damage frequency, and containment performance in a uniform, structured way. This data base can be queried and used as a computational tool to derive insights regarding the plants for which data is stored. This paper sets out the objectives of the IPE Insights Data Base, describes its structure and contents, illustrates sample queries, and discusses possible future uses.

INTRODUCTION

A data base, called the IPE Insights Data Base, has been developed that stores data obtained from the Individual Plant Examinations (IPEs) that licensees of nuclear power plants are conducting in response to the Nuclear Regulatory Commission's (NRC) Generic Letter GL88-20. In this paper, the IPE Insights Data Base will be referred to as the "data base." The data base is a collection of linked dBase files, storing information about plant designs, core damage frequency (CDF), and containment performance in a uniform, structured way. The data base was designed to accommodate information in accord with expectations based on the requirements of GL88-20, NUREG-1335, and some early IPE submittals. In the most general terms, the key results called for in NUREG-1335 are the plant-specific dependence table, the dominant accident sequences, and release category information. However, licensees have been given substantial freedom in the presentation of this information, and the level of detail designed into the data base corresponds to the level of detail expected in individual IPE submittals.

Information is extracted from the submittals and entered into the data base in such a way that queries regarding individual plants or classes of plants can be answered using the data base. The kind of query supported by the data base is discussed below.

*Work performed under the auspices of the U.S. Nuclear Regulatory Commission.

OBJECTIVE

The data base is designed to answer general questions such as: What features does each submittal take credit for? How does this factor into the core damage frequency (CDF) and/or containment performance of the plant? If two plants in basically the same class have markedly different CDF and/or containment performance, what is responsible for this? If a class of plants seems to share a particular contributor to risk, what design features are responsible for this?

If a particular difference between two plants is driven by one of them having more redundancy in safety systems, or more success paths for core cooling, this connection should manifest itself in the database. If one plant is an outlier by virtue of lacking a design feature common to other plants, or by virtue of an adverse functional system interaction, this should likewise show up. Not all such significant factors lend themselves to this treatment; details of intra-system topology are beyond the scope, as are plant-specific failure probabilities for all components. However, functional dependencies, success paths, redundancy, diversity, and so on can be addressed. Accordingly, the goal of the present development is to record the presence or absence of hardware in each design, characterize its functional dependencies, and relate these features to the CDF and containment performance.

STRUCTURE OF THE DATA BASE

In order to implement the present design within dBase IV, a number of different data base files have been constructed, each storing a different type of information. There are two sections of the IPE data base, corresponding to the Level 1 analysis in the IPE submittals and the Level 2 analysis. The Level 1 information is further subdivided into BWR and PWR dBase files.

The backbone of the IPE Insights Data Base is a basic list of BWR and PWR systems, in terms of which: (1) the design of any BWR or PWR can be described with reasonable fidelity, (2) plant-specific dominant accident sequences can be described accurately, and (3) the success paths assumed in the IPE (its mission success criteria) can be described.

The relationships between major elements of the IPE Insights Data Base is shown in Figure 1. Several of these elements contain field names corresponding to elements of the basic system list (i.e., system names: A,B,C...etc). This is the essential linkage that relates functional dependencies to accident sequences as well as success strategies. This is why the system list was referred to above as the "backbone" of the data base.

For purposes of illustration, consider the particular PWR system corresponding to the emergency feedwater system (the safety-grade system supplying makeup to the secondary side). For each PWR plant, the dependence table data base file shows what other systems support this system (SS1, SS2, etc. in Figure 1); the mission success data base file shows what role this system plays in each of the success paths; the dominant accident sequence data base file shows whether a failure of this system is essential in any given dominant accident sequence. The data base file containing information on the dependence of BWR systems is analogous to the PWR file. Finally, a Frontline Systems data base file shows how many trains of this system each plant has and what this system is called at any given plant. The intent is to store similar information about every important BWR and PWR system.

The relationship between accident sequences and release categories is established through the Plant Damage State field, which is common to the accident sequence data base file and the containment matrix (C-matrix) data base file. No scheme for plant damage state definitions was prescribed in NUREG-1335, nor has one been presupposed here. If a submittal defines plant damage states, its scheme is used. The presumption is that the IPE submittal will contain a partitioning of the frequency of each accident sequence over a set of release categories. If this is true, then the present scheme can accommodate the variety expected in the submittals. An assumption which is made here is that the submittal's definitions of release categories can be put into reasonable correspondence with the release categories used in the data base. This scheme allows linkage of (for example) the frequency of "Early Failure" (one of the data base parameters related to release categories) to particular combinations of system failures, dependencies, mission success criteria, etc. It should be noted here that later experience with IPE submittals has shown that a significant fraction of them do not report the plant damage state to which each dominant accident sequence is assigned. In these cases the link between the Level 2 information and the Level 1 data is lost.

MAJOR ELEMENTS OF THE LEVEL 1 IPE INSIGHTS DATA BASE

The Level 1 dBase files are General Plant Information, Front-Line Systems, Support Systems, Dependency Table, Core Damage Prevention Strategies, Mission Success Paths, and the Accident Sequence Table. A brief description of each file follows.

General Plant Information

The General Plant Information data base file contains the following information: plant name, plant type, NSSS vendor, number of loops (PWRs only), plant output, containment type, number of units, total core damage frequency, and, if a multi-unit site, are support systems shared, does crosstie capability exist, and is there a common control room. This information enables the user to sort or query across a subset of the entire data base, i.e., by plant type, by containment type, by NSSS vendor.

Front-Line and Support Systems

Development of a key systems list for both BWRs and PWRs was a crucial first step in the construction of the data base files. The files relate the generic key systems list (Frontline and Support) to plant specific nomenclature and information on the number of trains and any credit taken for cross-tie from another unit. The files, therefore, contain the following fields: plant name, key systems list, plant-specific nomenclature, number of trains and notes. These aspects of the files are described in the following paragraphs.

The first field is the name of the plant. The second field contains the key systems list. In the previous section, the key systems list was described as the backbone of the IPE Insights Data Base, because defining this list goes a long way towards defining the structure of the entire data base. Dependencies, mission success criteria, and accident sequence descriptions are all keyed to this list. However, its formulation is not unique. As experience was gained, it was necessary to modify the definition of this list in order to improve the usefulness of the data base. Accordingly, compromises had to be made, as summarized below.

Consider the simple problem of comparing two BWR (or two PWR) designs at the system level. The approach taken in the data base is to develop the system list in such a way that a very simplified design comparison between two plants could be formulated as a statement of (a) which systems on this list are present in both designs, (b) which systems are present in one design and not the other, and (c) which systems are present in neither. Unfortunately, even this simple task is not straightforward when all methods of injecting water into the reactor coolant system (RCS) are considered. The capabilities of individual BWR and PWR systems in the U.S. vary somewhat, even for systems which have the same name and perform similar functions. Proceeding formally, one could have assumed that every BWR and PWR system is completely unique. This would have led to a very long list of systems which could not be used to compare plants in any meaningful way, since no two plant designs would appear to have anything at all in common. Approaching from the opposite extreme, one could have combined all systems which perform a low pressure injection function (for example) into a single entity. This would also thwart the objective of plant design comparison, because on this basis, plants would differ only in the number of trains of this entity, and aggregating several frontline systems into one masks any differences in their support requirements.

After some experimentation, the following basic set of BWR functions has been used to organize the frontline systems list: Reactivity Control, Pressure Boundary Integrity, High Pressure Injection, Low Pressure Injection, and Containment Systems. Under each function a group of plant systems are considered, each of which could carry out the function.

In a similar manner, a basic set of PWR functions were defined and used to organize the frontline systems list: Reactivity Control, Primary Integrity, Primary Inventory-injection, Primary Inventory-recirculation, Secondary Integrity, Secondary Inventory, Containment. This set has been used in the data base in the formulation of the systems list.

These schemes work for the BWRs and PWRs to which they have been applied. Extra places ("alternate systems") on the list have been defined under some functions, in the expectation that some plants will take credit for systems which cannot be placed in reasonable correspondence with a shorter list.

It has been necessary to develop conventions regarding how the correspondence is to be established between this list and any particular BWR or PWR design. For example, if a plant has several auxiliary cooling systems, one could ask how to place these into correspondence with the several auxiliary cooling systems which have been allowed for in the systems list.

No single BWR or PWR may have all of the systems which appear on the respective BWR or PWR lists, but essentially any system playing a significant role should correspond to some entry, even if it is necessary to resort to one of the "alternate" system designations. (If a violation of this is encountered, the list is modified.) Thus, the list itself is a vehicle for comparing design features of two plants.

The third field stores the nomenclature used in the submittal corresponding to the equivalent system in the key systems list.

In order to make meaningful comparsions of systems between plants, more detail is needed on such questions as redundancy of systems. Accordingly, the number of trains of each system at each plant is stored in a separate field. This permits comparison of what different plants require in order to deal with a given initiator, what alternative means can be brought into play if the first success path fails, and so on.

The data base stores how many trains each sy tem has, whether the pumps are identified with more than one system, and whether a given system can be supplemented by cross-tying to another unit. For example, for low pressure injection and suppression pool cooling in a BWR, the same pumps may be involved in both functions, but the flowpaths are different, and the consequences of failing the two functions are different. The data base approach is to reflect the number of pumps under both low pressure injection and suppression pool cooling. In order to indicate that the pumps in the low pressure injection field are also part of a different system, two fields adjacent are provided: one to signal that this hardware is multi-purpose, and another to give the name of the system's other identity.

Dependence Table

This file shows the direct functional dependences of each frontline and support system; that is, what other systems any given system depends on. There are separate files for BWRs and PWRs. The dependence table can be drawn as a matrix: headings across the top are systems from the key systems list; the labels going down (labelling records in this data base file) are support systems. If a system performs a frontline function and also supports another frontline system, it shows up on the left-hand side of the matrix as if it were a support as well as in the systems list across the top. Each element of this matrix then tells about the direct functional dependence of the column system on the row system. A blank entry means that there is no direct dependence.

Core Damage Prevention Strategies

For each challenge i.e. initiator category (i.e. transients as well as LOCAs) for which success criteria are provided in the IPE submittal, this data base file provides a list of strategies to prevent core damage. Each strategy is described in terms of a combination of safety functions which have to succeed in order to prevent core damage, given the initiator in question. A special set of safety functions has been defined for this purpose.

Mission Success Paths

The mission success data base file tells what success paths the IPE assumed in its reported results. Each record in this data base file relates a specific complement of equipment to a particular type of initiator and a particular type of safety function. If a safety analysis takes credit for more than one way to remove heat, its results cannot be understood without an unambiguous statement of exactly how decay heat can be removed.

Each distinct way of performing a given function receives its own record. For example, following a transient with failure of high pressure systems, depressurization and low pressure injection are called for. There may be several low pressure systems which are capable of injecting enough water to cool the core. This situation is represented by several records.

IPEs of plants whose core damage frequency from transients is especially low should be expected to explain this result in terms of credit for numerous and diverse ways of cooling the core. By showing all success paths explicitly, the data base shows why the frequency is low. If the low frequency cannot be understood on this basis, then perhaps the failure expression has been quantified with low frequencies, and this may warrant scrutiny.

Accident Sequences

The accident sequences file stores dominant accident sequences from each submittal. Every dominant accident sequence appears as a record in this file. The goal is to record which systems failed in the sequence, what sort of phenomenology goes along with these failures, and the frequency of the sequence.

Licensees have considerable freedom in how they report this information. The data base structure is a compromise between simplicity and searchability. The fields in this data base file are as follows: plant name, the submittal's name for the sequence, plant damage state, core damage frequency, the initiator, lost supports, failed functions, causes, a field called "attributes," the key systems list, and a comment field. In the following paragraphs some of these field are elaborated on in the context of this data base file.

The Plant Damage State field stores the submittal's plant damage state designator. The purpose of this field is to link accident sequences with phenomenology, as represented in the containment performance data base file.

The Initiator field stores the accident sequence initiator. This information may be implicit in the submittal's sequence designator, but this is not standard across plants since submittals do not be use a universal scheme for designating initiators or sequences. In this field, the initiators are designated within a universal scheme. Support system initiators receive special designation.

If the accident sequence involved total loss of one or more support systems, such as emergency ac, service water, and so on, then the field name(s) of the lost support function(s) are given in the Lost Supports field.

Every accident sequence involves failure of at least one safety function. In the Failed Functions field, the name(s) of the lost function(s) are indicated.

The purpose of the Causes field is to record whether a particular physical cause enters into the particular accident sequence. The causes allowed as entries are fire, internal flood, or common cause failure.

For a number of ad hoc characteristics of sequences, such as station blackout or ATWS, the catchall field "Attributes" has been defined. This field contains a list of key attributes separated by commas, based on a dictionary of allowed entries.

The Key Systems List fields store which systems fail in each sequence. As discussed above in previous sections, the same systems list is used to discuss dependencies, mission success criteria, and sequences. The convention is to show which frontline systems failed in order to bring about

core damage and only those systems. If the sequence involved a human failure, this is also recorded. By definition, every sequence must fail all success paths in some functional area discussed above under Mission Success.

The Notes field is used to record any additional information not captured in the previous fields, which is considered important for understanding the sequence.

MAJOR ELEMENTS OF THE LEVEL 2 IPE DATA BASE

As noted previously, the Level 1 portion of the data base is connected to the Level 2 portion through the Plant Damage States (PDS). In the Level 2 analysis, the plant damage states are divided into several possible fission product release paths and/or containment failure modes via the C-matrix. Each failure mode is associated with a quantity of fission products released to the environment (Source Terms or Release Classes). The Data Base is structured to capture the various elements of the Level 2 portion of an IPE. Each element of the Level 2 IPE is allocated a separate dBase file as follows: Plant Damage State Definitions, C-matrix (containment performance), Source Terms, and Level 2 Analysis Parameters (source term characteristics).

Plant Damage State Definitions

The Plant Damage States file is structured to capture information which the IPE analyst used to define the various plant damage states. The assumption is that the IPE submittal specific PDSs can be characterized in terms of the following parameters allowed in the data base file: level of RCS pressure (high, medium or low); containment integrity (intact, pre-existing leak, or bypassed); RWST/CST inventory (injected or not); availability of containment sprays and heat removal; and, for PWRs, whether the steam generators are available for cooling.

Containment Performance

Information on containment performance is captured in a file in the form of a matrix, which relates the plant damage states to various failure modes. The PDS designation scheme is flexible but some structure had to be imposed on the various failure modes to be included in the containment matrix. Currently, six failure modes are included.

Each record in this file contains a plant name, a plant damage state designator, frequency, and split fractions which allocate the indicated plant damage state over the following possibilities: bypass, early failure, late failure, basemat melt-through, vessel breach without containment failure, and no vessel breach. Because the entries are split fractions, they should sum to unity within a given plant damage state. In addition, each split fraction is allocated to one or more release category designators. These designators connect the containment performance file to the source term file.

Source Terms

Information on Source Terms is entered into a file which relates the release category designators identified in the containment performance file (C-matrix) to the quantity of fission products released to the environment.

Each record in the file contains the release class designator and the fractional release (to the environment) of up to nine different fission product groups.

Level 2 Analysis Parameters

Information on containment failure modes and other analysis parameters related to the source term characteristics is contained in a file which is connected to the rest of the data base through the release category designators. This file, therefore, provides information on how the source terms were calculated for each release category.

Each record in the file contains a Release Class, Containment Failure Mode, Containment Failure Cause, Failure Location (BWRs only), Containment Failure Size, Zr Oxidation (in-vessel), Amount of Core in Core/Concrete Interactions (CCI), CCI Disposition, Vessel Failure Mode, Suppression Pool Bypass (BWRs only), Sprays Available, Credit Taken for Decontamination in Reactor Building (BWRs) or Auxiliary Building (PWRs), and notes. The various fields are described in terms of a dictionary of allowable entries categorizing each field. For instance Containment Failure Cause records the cause of containment failure (steam and gas pressurization, H_2 combustion, DCH, or Basement melt-through). Loss of containment isolation or bypass events can also be entered into the field.

EXAMPLES OF QUERIES

Dbase 4 allows the user to find particular fields or entire records satisfying certain conditions as well as to perform calculations such as summing or counting. The following examples illustrate the types of questions that can be asked of the data base and the types of results that can be extracted.

One may want to know how "important" is RCP seal LOCA to total core damage frequency. This could be asked for a particular plant or across all PWR plants, or for a subset of PWR plants, i.e., Combustion Engineering (CE) PWRs. First, consider the case of a particular plant. Using the data base, the sequences involving RCP seal failure, as indicated in the sequence equipment failure list, would be sorted out and their CDF would be summed. The result would be divided by the total CDF of all sequences for the particular plant. The resulting fraction would give an indication of the "importance" of seal failure to CDF in the plant in question. This same fraction could be obtained for any number of plants in the data base with a particular characteristic, for instance CE PWRs, and averaged over the group to obtain the "importance" of RCP seal LOCA for the group.

One could carry the above exercise one step further by asking for a list of plants for which RCP seal sequences constitute more than 10% of the core damage frequency contained in the described sequences. A series of commands can be applied to the data base whereby iteratively for each plant the accident sequences are searched, summed and divided by total CDF as above and then the plant is listed if the result is greater than 0.1.

Another question of interest for an analyst trying to gain insights might be: For core damage sequences, how often does loss of offsite power (LOSP) result in station blackout? To obtain the answer one could search the accident sequence part of the data base for sequences where the initiator was designated with "LOSP" and add up the CDF of these sequences. From this group of

sequences, those with "SBO" (station blackout), in the attribute column can be selected and their CDFs summed. Dividing this latter sum by the total CDF for the LOSP sequences will provide a fraction indicating how often LOSP results in SBO.

As a final illustration of a data base query consider the following. One may wish to compute the percentage of CDF due to LOCA for all plants which require human action at switchover to recirculation, and compare this with the percentage of CDF due to LOCA for plants which do not require human action at switchover. This could be accomplished with these steps: The percentage of CDF due to LOCA for each plant could be calculated in a similar manner as percentages were calculated for the previous examples. (LOCA sequences are identified from the initiator or, if it is a transient induced LOCA, from the "TIL" designation in the attributes field of the sequence). One could then determine what class a given plant is in according to whether HPR (high pressure recirculation) or LPR (low pressure recirculation) has an "H" designation in the mission success paths for LOCAs. The H designation means human action is required. The CDF for each group, i.e. with and without H, can than be summed, normalized and compared.

This last example also illustrates a caveat for data base users. Suppose a significant difference were found in the CDF for the two classes of plants. An analyst then would have to ensure that the difference really is due to the presence or absence of human action at switchover and not for other, not immediately apparent, reasons.

POSSIBLE FUTURE USES OF THE IPE INSIGHTS DATA BASE

As the above examples have illustrated, the data base has a number of unique features which make it a useful tool to carry out meaningful comparisons of plant features and gain insights about their strength and weaknesses.

First of all, the data base captures information about all PWRs in a unified structure and information about all BWRs in a unified structure.

Besides capturing the essential characteristics of each of the significant accident sequences, the data base also captures the success strategies that the IPEs take credit for.

Since the information in the IPEs, and therefore in the data base, is essentially at the system and function level, the data base can be used as a tool to determine the importance of plant features at this level. In other words, the data base can indicate how particular design features are related to core damage frequency in positive and negative ways. Certain features may represent vulnerabilities which will show up under the accident sequence part of the data base. Others may show up as assets in the core damage prevention strategies that the data base captures.

Because the data base can work with classes of plants, the potential significance of certain generic issues can be obtained with the data base.

SUMMARY

As described in the previous sections, the IPE data base stores information about plant design and aspects of the plant risk profile in a structured way. This uniform characterization in the

data base is made difficult by the inhomogeneity of content among the IPE submittals. The greatest challenge in setting up the database and capturing data from the IPEs is to achieve uniformity while accurately preserving the salient points of the analysis contained in each individual IPE. It is the uniformity of the information which makes the data base amenable to high-level but complex queries dealing with classes of plants.

Currently, no checking of licensee-provided information is performed prior to data entry. The facts provided in the IPE submittals are taken at face value and translated into the data base structure without further review.

The level of detail recorded in the database is at the systems level. Therefore, the database can be used to efficiently gain insights for many safety issues of interest at the systems level or at the function level. More detailed information was not required in the submittals, and has not in general been made available.

As of October 1993, data from approximately half of the expected IPE submittals has been entered in the data base, with all entries expected to be completed by mid-1995. Data entries undergo a comprehensive quality assurance process. In addition a thorough trouble-shooting and shakedown of the data base is also needed; this is expected to start in early 1994.

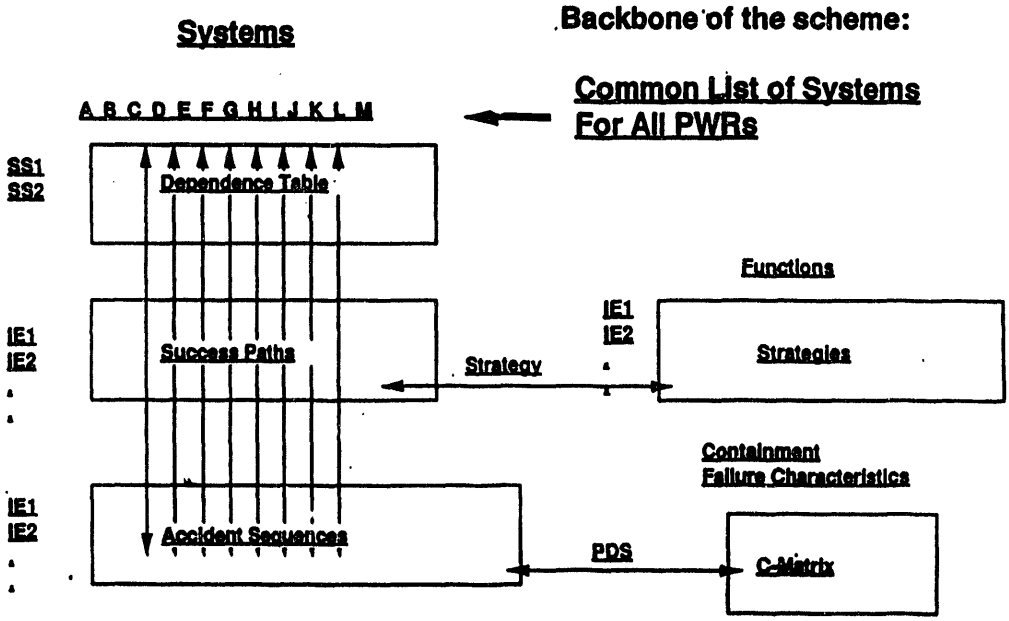


Figure 1. Structure of IPE Data Base

INDIVIDUAL PLANT EXAMINATION PROGRAM ASPIRATIONS AND ACHIEVEMENTS

John H. Flack
U.S. Nuclear Regulatory Commission

ABSTRACT

An Individual Plant Examination (IPE) is a systematic examination of a nuclear power plant for vulnerabilities, or risk significant contributors. By mid 1994, all licensees of commercial nuclear power plants will have performed an IPE on their units. To date, the NRC staff has received sixty-three (80%) of the seventy-eight expected IPE submittals. Twelve IPE reviews are now complete, with twenty-two in various stages of review. This paper provides a preliminary overview and comparison of licensees IPEs to Commission objectives. Insights and findings stemming from the review program are also presented.

BACKGROUND

In 1985 the Commission put forth the Severe Accident Policy Statement (Reference 1), with the conclusion that existing plants posed no undue risk to public health and safety. In formulating this position, the Commission recognized the benefit of Probabilistic Risk Assessments (PRAs) in identifying previously unrecognized severe accident vulnerabilities, and safety enhancement opportunities. Based on this observation, the NRC developed an integration plan for closure of severe accident concerns (Reference 2), with the Individual Plant Examinations IPEs as a key element.

In 1988, the NRC specified the purpose and objectives of the IPE program in Generic Letter 88-20 (Reference 3), and a year later initiated the process through issuance of Supplement 1 to Generic Letter 88-20 (Reference 4). An associated submittal guidance document NUREG-1335 (Reference 5), issued with the generic letter supplement, identified the information that licensees need to submit in response to the generic letter request. To date, sixty-three (80%) of the seventy-eight IPE submittals have been submitted to the NRC for review. Twelve reviews have been completed, with twenty-two in various stages of review. All IPEs are expected to be submitted by mid 1994 (Figure 1).

Unlike previous PRA reviews which tend to requantify and compare results, the IPE reviews primarily focus on the process used by licensees in meeting their IPE program objectives. Process reviews focus on items such as completeness, scope, analytic techniques, and assumptions. The reviews do not requantify or validate licensee numerical estimates (although significant

deviation from generally accepted generic estimates are questioned and probed further). Although the process does not confirm the so called "bottom-line" estimate, it does assess those areas in the analysis which could significantly impact the estimate and associated conclusions.

IPE reviews are performed by teams, with members having expertise in reactor systems, containment performance, and human reliability. The reviews involve a two step process, with the second step determined on a case-by-case basis. The first step (or Step 1) review consists of a series of tasks: an initial check of the IPE submittal for completeness and consistency with past PSA practices, generation of questions, and interactions with licensees on various technical aspect of the analysis. A more detailed audit, or Step 2 review, may be performed if a licensee's IPE approach (or plant) appears unique, or submittal findings are not consistent with conventional PRA experience. The second step utilizes contractors with compatible technical expertise, involves a site visit and audit of supporting documentation. Audited information generally includes fault trees, calculations, data, notebooks and other information not contained in the IPE submittal.

Upon completion of the IPE, findings and rationale for acceptance are documented in a Staff Evaluation Report (SER) and issued back to the licensee. The SER focuses on key areas essential to understanding the IPE findings, important insights, and any recommendations for follow-on activities. As discussed below, acceptability of an IPE is based on the extent to which the process met the program objectives.

COMPARISON OF IPEs TO COMMISSION OBJECTIVES

The objective of IPE program as put forth in Generic Letter 88-20, is to have licensees: (1) develop an appreciation of severe accident behavior, (2) understand the most likely severe accident sequences that could occur at their facilities, (3) gain a quantitative understanding of the overall probabilities of core damage and fission product release, (4) reduce the overall probabilities of core damage and fission product releases, by modifying, where appropriate, hardware and procedures. Licensees meeting these objectives will have substantially progressed in resolving severe accident concerns, and be on firm ground when implementing their accident management program (a follow-on activity needed for closure of severe accidents). These objectives also form the framework of the NRC review process and basis for acceptability.

- **To develop an appreciation of severe accident behavior,**

Essentially all licensees have chosen to do at least a Level 1

probabilistic risk assessment (PRA) and a containment performance analysis consistent with the Generic Letter 88-20 Appendix 1 guidance. (Some 42% of the IPEs actually go beyond the Generic Letter requirement by including either a full scope Level 2 or Level 3 PRA.) Probabilistic studies provide an enhanced understanding of plant safety from a broader perspective, one which looks beyond system success, to failure and progression of accidents which go beyond the plant's design basis. In general, performance of an IPE/PRA consistent with "conventional wisdom" would naturally lead to an appreciation and understanding of severe accidents. However, in order to ensure technology transfer and an integrated appreciation of severe accidents at the operations level, licensee involvement in the analytic process is critical. In fact, transfer of insights to plant personnel is perceived to be one of the major benefits of the program.

The reviews to date indicate that licensees have been involved in the process primarily to ensure that analytic models represent the as-built, as-operated plant, and that operational characteristics are properly reflected in the analysis. Involvement generally includes plant walkdowns, documentation reviews, operator interviews, simulator exercises, and peer reviews. Although consultants still provide significant support, discussions with licensees indicate that 50% or more of the technical work is being performed by "in-house" utility staff.

In addition to licensee involvement, licensees are planning to keep their IPE/PRA updated, or "living," an activity not required by Generic Letter 88-20. By maintaining "living" programs and a dedicated staff, IPEs can provide additional assurance that their PRA results and conclusions are valid, and allow a better perspective from which to address safety issues as they surface. Areas identified in submittals where licensees plan to apply their IPE/PRA insights through their "living" programs include:

- development of an accident management program,
- support of licensing action, including changes to allowed outage times of equipment and/or tech specs changes,
- evaluating the significance of various safety issues,
- evaluating the impact of design changes,
- prioritization of proposed improvements,
- reviewing new plant projects,
- briefing and providing senior management with risk insights,
- supplementing reliability centered maintenance programs,

training operators, and

- license renewal

The use of IPEs in some of these areas, however, will likely require additional staff review as they extend beyond the scope of the IPE program. Nevertheless, future use and application of IPEs via "living" programs indicate that benefits are going to be long lasting.

o To understand the most likely severe accident sequences that could occur at their plant

One of the most highly regarded insights gleaned from the IPE is the identification of dominant sequences and associated contributors. Each sequence contains an accident initiator and subsequent equipment or human failures that describe the course of events leading to core damage, or release of radioactive material. Dominant sequences are plant-specific, and depend on plant design (redundancy and diversity of systems), analytic assumptions, applied techniques, and data.

Based on information submitted to date (Table 1), loss of offsite power (LOSP) events still remain one of the most important contributors of core damage. Other important initiators include loss of coolant accidents (LOCAs) for PWRs, and anticipated transient without scram (ATWS) for BWRs. Flooding can be an important accident contributor to any plant design (switchgear being most vulnerable). For PWRs, steam generator tube ruptures can be significant because of containment bypass.

Another important source of contributors to core damage are contained in the transient, or "other" category. These initiators result from dependencies between the front-line systems, support systems, and initiating events. Since system failures can both cause an initiating event and impact the mitigation capability, this class of events can become the dominant contributor to the overall risk at any plants. Transient types of events include, for example, loss of AC or DC bus, loss of component cooling water or service water, loss of HVAC.

Table 2 depicts the range of these contributors, and demonstrates their plant-specific nature. Although differences in plant design (such as the number of trains or diversity of function) can impact the risk estimates, underlying modeling assumptions can also substantially effect IPE findings and insights. Some of the more subtle but critical assumptions are associated with treatment of:

- human reliability and credit taken for operator recovery action,

- common cause failure,

- environmental effects including loss of HVAC, or internal flooding involving plant equipment,

- data and application of data to situations involving substantial loading, or accidents conditions beyond the design basis,

- success criteria, and

- degradation of equipment under adverse plant conditions, e.g., reactor cooling pump seals.

Sensitivity studies, and uncertainty analyses provide valuable insight into understanding the impact and meaning of various assumptions in the analysis. Importance measures (a type of sensitivity analysis), for example, are frequently being used to gain additional insight. Three of the more common measures include risk achievement worth, risk reduction worth, and Fussel-Vesely.

Licensee peer reviews by knowledgeable analysts can also check and provide feedback on various assumptions, adding credibility to the analysis. Meeting the intent of Generic Letter 88-20 requires peer reviews as an intrinsic part of the IPE process, a key area of focus during the staff review.

o **To gain a more quantitative understanding of the overall probabilities of core damage and fission product release**

The development and application of probabilistic techniques in conjunction with deterministic reasoning, provides licensees with a complete picture of their plant's safety capacity. Using an integrated analysis, licensee's are in a better position to understand, for example, what it means to have a certain piece of equipment out of service, or the effect of human error in response to severe accidents.

Because of variations in modeling assumptions, data, and level of effort, the "bottom-line" estimate (for example, the overall core damage frequency estimate) is generally considered to be one of the weakest aspects of the IPE/PRA. In fact, placing emphasis on the "bottom-line" can have an adverse effect on the analysis as it tends to narrow the focus. The "bottom-line" is, therefore, perceived as a byproduct of the analysis, the important insights stemming from the analysis itself.

With proper characterization, however, the IPE bottom-line results can provide some relative insight into the safety capacity of a specific classification of plants. For example, the overall average CDF of all the reported PWRs and BWRs IPEs

are reported to be:

7.8 x 10-5/yr for PWRs
2.0 x 10-5/yr for BWRs

From a design perspective, the lower value for BWRs is not unexpected as BWRs have more redundancy and diversity in decay heat removal than PWRs. Figure 2 depicts the spread in core damage frequency (averaged over intervals of 2.5) reported to date. The one to two orders of magnitude variation demonstrates the difficulty in using the "bottom-line" without supplementary information to place estimates in their proper perspective. Variations in plant design (redundancy and diversity), operations, underlying assumptions, and data can all have a major impact on the overall results.

- **Reduce the overall probabilities of core damage and fission product releases, by modifying, where appropriate, hardware and procedures**

The IPE process requires licensees to report the criteria used to define a vulnerability, and the fundamental causes of each vulnerability identified. In response to the reporting guidelines, definitions of vulnerabilities tend to fall into one of the following categories:

Global - this definition simply defines vulnerabilities as the top (or all) sequences leading to core damage, (which implies that all plants have vulnerabilities).

Specific - application of numerical criteria based on sequence frequency or percent contribution to CDF, e.g., a 50% or more contribution to the core damage frequency and/or a sequence greater than 10 E-4/yr.

Process - involves review and evaluation from a number of different perspectives. Most licensees approach vulnerabilities this way, using cost, perceived benefit, and engineering judgement to determine if improvements are warranted.

In general, implementation of safety enhancements in response to potential vulnerabilities requires a thought process that takes into consideration all of the above, e.g., significance of contributors to core damage or early containment failure, cost verses benefit, and engineering/management judgement. From an NRC perspective, the reviews focus on the process used in identifying and evaluating contributors to core damage or containment failure within the analytic framework, rather than specifically on the definition of vulnerability. For example, numerical criteria which might be used to explicitly define vulnerability, is generally dependent on implicit modeling

assumptions and other aspects of the analysis. The ability of the IPE to support the definition of vulnerability (or threshold for plant improvements) has become the reviewer's focal point.

Significant contributors to core damage (or vulnerabilities by most analyst's standards) generally stem from support system failures or environmental effects such as flooding. Listed below are a number of areas where improvements to equipment, or procedures have enhanced plant safety:

- use of the fire water system as an accident mitigating system, e.g., as backup cooling to plant equipment (PWR charging pump oil coolers, emergency diesel generators heat exchanger), as a makeup source for auxiliary feedwater system in PWRs, and as a source of water for either flooding the reactor cavity through the drywell sprays, or for coolant injection through the RHR system in BWRs,

- implementation of system or unit cross-ties to enhance redundancy and provide a degree of diversity to system performance,

- enhancing internal flood protection by providing water tight doors and procedures to protect against switchgear room flood,

- upgrading alternate power supply, e.g., adding additional emergency power in the form of emergency diesels, blackstart diesels, or gas turbines to reduce the probability of station blackout scenarios,

- increasing the likelihood of AC power recovery by extending station blackout coping times, e.g., upgrading batteries or adding battery charging capability,

- enhancing core cooling for sequences involving containment bypass and failure of recirculation, e.g., refilling water storage tanks,

- reducing the likelihood of RCP seal failure by installing improved RCP pump seals and procedures to reduce the probability of seal failure,

- increasing room cooling capability, e.g., upgrading HVAC systems and adding procedures and temperature alarms that would help mitigate loss of room cooling,

- reducing system asymmetries by balancing bus loads or adding redundancy to existing systems in order to reduce the significance of single failures, and

- utilizing diversity in DHR, e.g., by implementing procedures

and training for feed and bleed and/or secondary side depressurization, or by using the fire water system and other available systems as alternate core injection in BWRs.

SUMMARY AND GENERAL OBSERVATION

In many cases, IPE reviews indicate that licensees are more than meeting the intent of Generic Letter 88-20. This is apparent in the number of identified safety enhancements and number of licensees planning to maintain their IPE/PRA as "living" documents (not a requirement of the IPE program). The IPEs are complex and require expenditures averaging 2-3 million dollars, with an equivalent amount of licensee staff resources. This reflects licensees' recognition of the potential usefulness of these evaluations. In many cases, insights identify simple improvements, leading to plant modification and procedural changes are of low cost.

The IPE reviews indicate that results, findings, and conclusions can be sensitive to implicit assumptions. For example, assumptions regarding RCP pump seals can determine whether transients or LOCAs dominate the risk at a PWR. Techniques used to treat human reliability, common cause failure, and data can also have a major impact on the overall risk estimates. For proper application of IPE insights, consideration of underlying assumptions and their sensitivity to the overall estimate cannot be ignored. Continued use of the IPE as a "living" document should help to validate some of these assumptions.

REFERENCES

1. "Policy Statement on Severe Accidents," U.S. Nuclear Regulatory Commission, Federal Register, Vol. 50, 32138, August 8, 1985.

2. USNRC, "Integration Plan for Closure of Severe Accident Issues," SECY-88-147, May 25, 1988.

3. NRC letter to All Licensees Holding Operating Licenses and Construction Permits for Nuclear Power Reactor Facilities, "Individual Plant Examination for Severe Accident Vulnerabilities - 10 CFR 50.54(f)," Generic Letter No. 88-20, dated Nov. 23, 1988.

4. NRC letter to All Licensees Holding Operating Licenses and Construction Permits for Nuclear Power Reactor Facilities, "Initiation of the Individual Plant Examination for Severe Accident Vulnerabilities - 10 CFR 50.54(f)," Generic Letter No. 88-20, Supplement 1, dated August 29, 1989.

5. USNRC NUREG-1335, "Individual Plant Examination: Submittal Guidance," Final Report, August 1989.

IPE SUBMITTAL SCHEDULE
(Current Status)

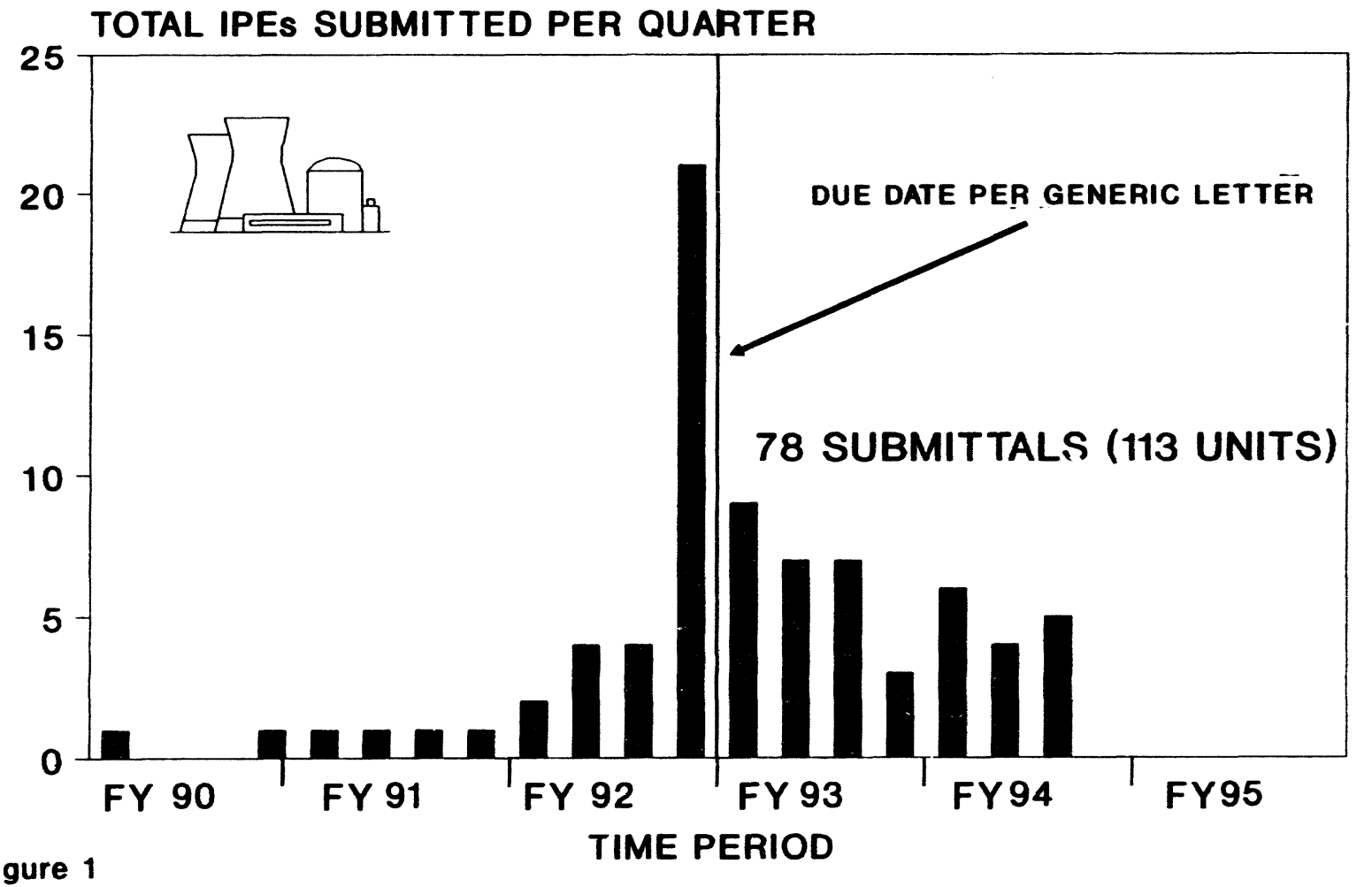


Figure 1

CORE DAMAGE FREQUENCY

Internal Events

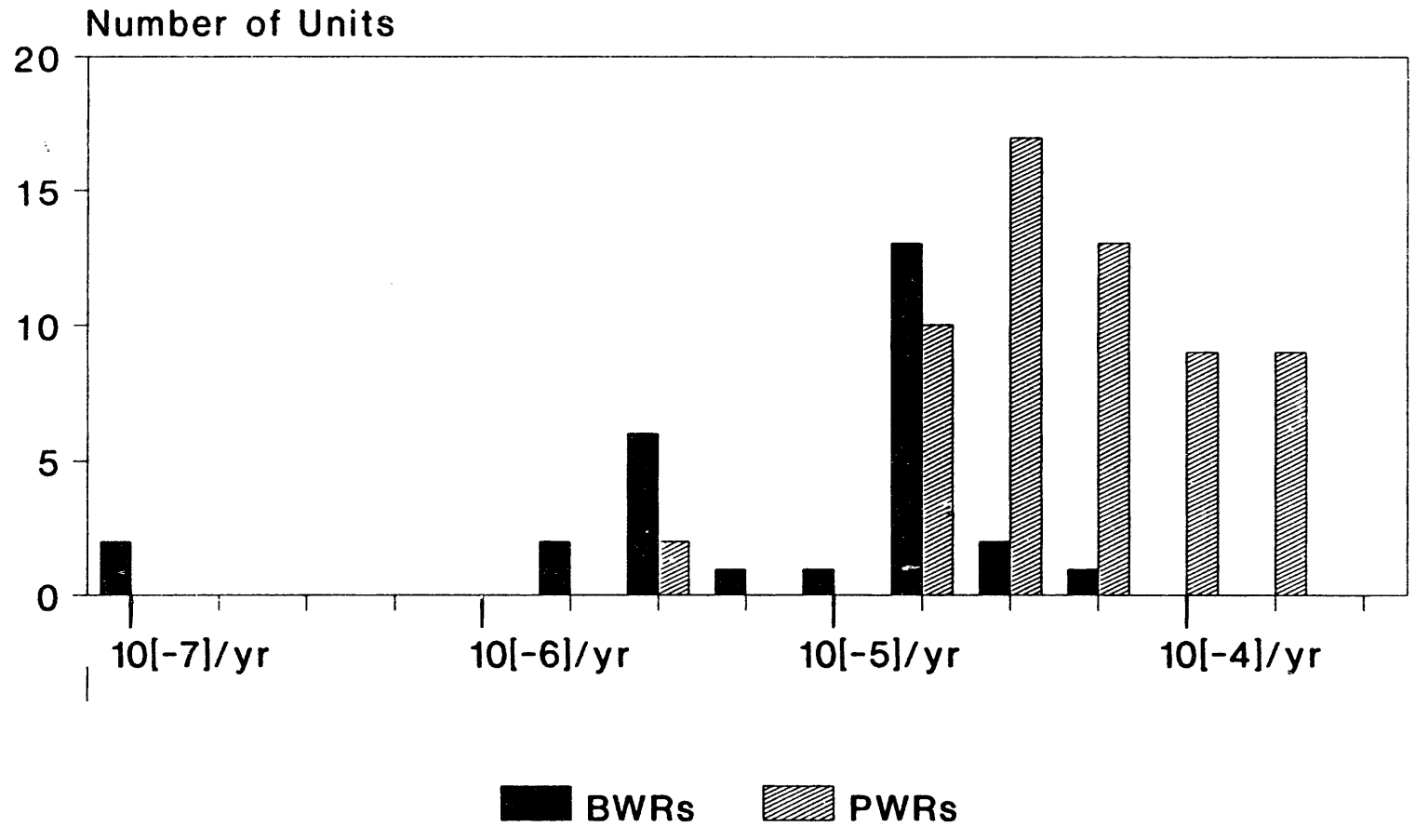


Figure 2

TABLE 1

PRELIMINARY FINDINGS
(AVERAGE %)

	PWRs	BWRs
LOSP	26%	38%
LOCA	24%	5%
ATWS	3%	20%
FLOOD	*10%	9%
ISLOCA	1%	1%
SGTR	5%	N/A
TRANSIENTS (OTHER)	31%	27%

* EXCLUDES SURRY FLOOD

TABLE 2

RANGE

	PWRs	BWRs
LOSP	40% - 6%	91% - 2%
LOCA	64% - 8%	16% - 1%
ATWS	5% - 1%	79% - 1%
FLOOD	*23% - 0%	25% - 0%
ISLOCA	3% - 0%	4% - 0%
SGTR	29% - 1%	N/A

* EXCLUDES SURRY FLOOD

Handbook of Methods for Risk-Based Analysis of Technical Specification Requirements

P.K. Samanta and W.E. Vesely
Department of Advanced Technology
Brookhaven National Laboratory
Upton, New York 11973

*Science Applications International Corporation
655 Metro Place South
Dublin, Ohio 43017

Abstract

Technical Specifications (TS) requirements for nuclear power plants define the Limiting Conditions for Operation (LCOs) and Surveillance Requirements (SRs) to assure safety during operation. In general, these requirements were based on deterministic analysis and engineering judgments. Experiences with plant operation indicate that some elements of the requirements are unnecessarily restrictive, while others may not be conducive to safety. Improvements in these requirements are facilitated by the availability of plant specific Probabilistic Safety Assessments (PSAs).

The use of risk and reliability-based methods to improve TS requirements has gained wide interest because these methods can:

- quantitatively evaluate the risk impact and justify changes based on objective risk arguments.
- provide a defensible basis for these requirements for regulatory applications.

The United States Nuclear Regulatory Commission (USNRC) Office of Research is sponsoring research to develop systematic risk-based methods to improve various aspects of TS requirements. The handbook of methods, which is being prepared, summarizes such risk-based methods.

The scope of the handbook includes reliability and risk-based methods for evaluating allowed outage times (AOTs), action statements requiring shutdown where shutdown risk may be substantial, surveillance test intervals (STIs), defenses against common-cause failures, managing plant configurations, and scheduling maintenances. For each topic, the handbook summarizes methods of analysis and data needs, outlines the insights to be gained, lists additional references, and presents examples of evaluations.

INTRODUCTION

The TS requirements for nuclear power plants define the LCOs and SRs to assure safety during operation. These requirements, originally based on deterministic analyses and engineering judgments, have been applied and reviewed over the years. However, experiences with plant operation indicate that

some elements of the requirements are unnecessarily restrictive, whereas others may not be conducive to safety.[1] For various reasons, improvements or changes in these requirements become necessary, and USNRC receives submittals from licensees to modify many aspects of the requirements.[2,3,4]

With the availability of plant-specific PSA methodologies, there is a significant interest in analyzing and justifying changes in the TS requirements using the PSA models.[5-8] There are many reasons for this interest in using risk analysis or PSA-based methods:

a) a PSA-based analysis gives a quantitative assessment of the impact of the change on the plant's risk, and so the justification for the change can be based on objective arguments,

b) changes to many requirements can be assessed consistently (using risk measures) and assurance can be obtained that the basic intent of the TS to maintaining a margin of safety during normal and accident conditions is not compromised, and

c) a defensible basis is presented for regulatory review and application.

Many changes to TSs were analyzed by PSA-based analysis and approved by USNRC. Also, USNRC has sponsored research to develop systematic risk-based methods to address various aspects of TS requirements. The handbook of methods, which is being prepared and is discussed here, will summarize methods showing illustrative examples of how to apply such methods to improve TS requirements.

In this paper, we briefly discuss the objectives and scope of the handbook, and give examples of the types of analysis that will be covered.

OBJECTIVE, SCOPE, AND USES OF THE HANDBOOK

The basic objective of the handbook is to summarize risk-based methods for analyzing various aspects of the TSs. The primary focus is to enable USNRC reviewers to assess whether proper evaluations are made in using risk-based analysis to change the TS requirements. Therefore, for each aspect of the TS, the handbook will summarize:

- the issues to be addressed,
- the methods and steps to be followed in a PSA-based application, and
- with illustrative examples and insights for seeking changes to the TS requirements.

The scope of the handbook covers aspects relating to LCOs and SRs in Technical Specifications. The handbook will address risk and reliability-based methods for evaluating:

- Allowed outage times (AOTs): This includes methods for evaluating AOT requirements both during power operation and periods of shutdown. The risk impacts of changes to single or multiple AOT requirements also will be discussed.
- Action statements requiring shutdown: This aspect particularly addresses those systems which are needed for shutting the plant down. The risk of shutting the plant down in failure(s) in these systems is usually substantial, and the action requirements should compare the risk of continued operation versus shutdown.

- Surveillance requirements: This includes both the surveillance test frequency (or the surveillance test interval) and any requirement for test strategy (e.g., staggered testing, sequential testing). Surveillance requirements during power operation and shutdown will be included.

- Treatment of common-cause failures: In deciding AOTs and SRs, the treatment of common-cause failure is important. Specific analysis and requirements for addressing common-cause failures will be discussed, and also, the enhancement of defenses against these failures through TS requirements.

- Management of outage configurations: The risk from simultaneous outages of multiple components can be much larger than single component outages. TSs forbid outages of redundant trains within a safety system, but many other combinations of components, if simultaneously unavailable, can pose significant risk. In seeking TS changes and in controlling operational risk, these configurations will be analyzed.

- Scheduling preventive maintenance: TS LCOs are specified so that, following detection of failure, the equipment can be repaired. However, these LCOs also are used to perform planned preventive maintenance during power operation. Risk-based analysis of preventive maintenance and scheduling of such maintenance will be considered in the handbook.

The handbook is expected to have several uses:

a) It can be used for USNRC review of risk-based analysis of TS requirements submitted by the licensee.

b) The licensee can use the handbook in preparing the submittals to USNRC,

c) Individual Plant Evaluation (IPEs) being completed can be applied to analyze TS requirements, and

d) The handbook will ensure consistency in the analysis and in the review process.

EXAMPLES OF APPLICATION AREAS IN THE HANDBOOK

We next give three example applications representative of those to be presented in the handbook. The example applications presented here are:

1. LCO action statements requiring plant shutdown.

2. Surveillance test intervals addressing adverse effects.

3. Scheduling maintenance during power operation versus shutdown.

In the handbook, the following aspects will be discussed for each application area.

- summary of current TS requirements and issues,

- methods for analysis of the requirements and the treatments of the issues,

- steps in the analysis,
- data needs,
- sensitivity and uncertainty analysis,
- insights on changing the requirements based on the results of the analysis.

LCO ACTION STATEMENTS REQUIRING PLANT SHUTDOWN[9]

When the ability to remove decay heat is reduced during the operation of a nuclear power plant, for example, when failures are detected in the residual heat-removal systems or standby service water systems of a BWR, the question arises as to whether it is better to continue power generation while repairing the failed equipment, or to go to shutdown, even though the ability to remove decay heat is impaired. These situations are unique in the sense that the risk of shutting down, with the consequential need to start up and operate the affected decay-heat removal systems, may be more significant than the risk of continued operation over a usual repair time.

Technical Specifications usually limit the time available for repairs to within an allowed outage time. If repairs cannot be made within this period, or if no time is allowed, the plant must be shut down for the repairs.

PSA methods can be used to consistently evaluate and compare the risks of these alternative operational strategies in failure situations, including the risk of entering plant shutdown modes.

The LCOs were primarily directed towards minimizing risk during power generation, assuming that the shutdown states are relatively safe, i.e., the risk of a plant shutdown was assumed to be negligible. Although this may be a reasonable assumption in many safety systems, it is not necessarily reasonable for the decay-heat removal systems which are especially needed in the plant shutdown states.

The risk comparison approach evaluates the two principal alternatives:

- CO - Continued operation, where repairs are undertaken at a temporarily increased risk level, while operating at full power.
- SD - Shutting down, where a controlled shutdown is made to undertake repairs.

Comparison of risks between these two alternatives is central to the approach, and is made using several risk measures. If both incur a small risk, then a flexible allowed outage time for repairs while operating at full power can be applied without further analysis.

Figure 1 shows an example analysis for a three-train standby service water (SSW) system in a boiling water reactor (BWR). The figure compares the core-damage frequency (CDF) associated with continued operation (CO), and that for plant shutdown (SD) for failures in one, two, and three SSW trains. As shown, under the existing requirements, the risk of shutting down in these three situations is larger than that for continued operation. These results are used, along with an analysis of available alternatives, to suggest modifications to current action statements.

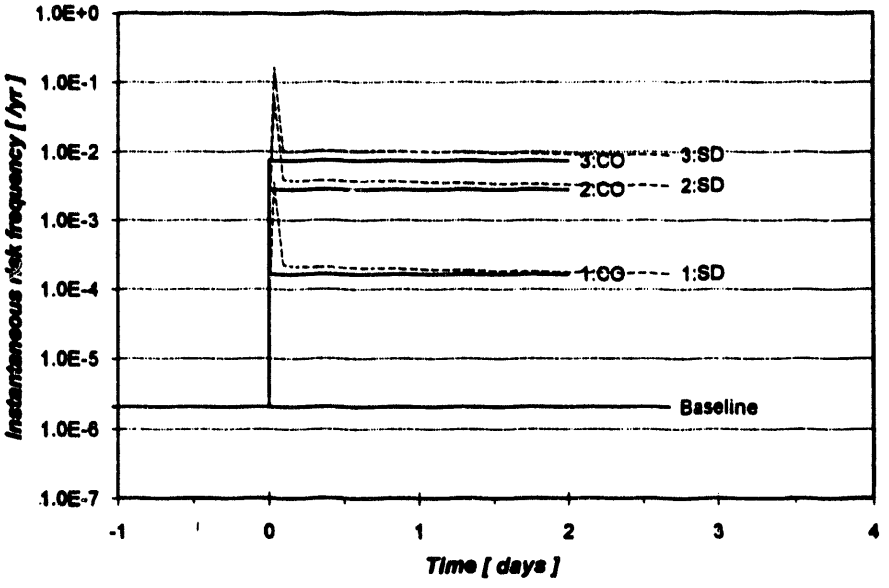


Figure 1: Instantaneous risk frequency for continued operation (CO) and shutdown (SD) alternatives in failure situations of the SSW system. (For example, 2:CO denotes the CO alternative for the situation where two SSW trains are inoperable.)

AOT for multiple failures:

The results show that the increase in risk is significant for multiple failures of standby service water trains. The risk in shutting down is comparable to that for continued operation over a predicted repair time of about 1 to 7 days, depending on the type of failure; it tends to increase for higher failure multiplicities. This result contrasts with current allowed outage times, which allow shorter or no repair time for multiple failures. Thus, our results suggested having a reasonable allowable outage time for multiple train failures. However, it should be equal to or shorter than that for single train failures, to avoid the temptation to declare additional trains inoperable to avoid plant shutdown, given that the repairs already needed will exceed the predefined allowed outage time.

Testing redundant trains to detect latent failures in the remaining trains or to assure availability of alternative operation paths:

Often, there is no clear requirement in the current action statements to check the status of remaining operation paths. If the initial failure is severe and requires a long repair time, then additional tests are recommended to check for common cause failures. Such tests are recommended during the first part of the allowed outage time, and should be preceded by diagnostic checking to avoid unnecessary damage to components (e.g., as would be caused by a sudden start-up of pumps). Testing also can assure the availability of an alternative success path justifying allowed outage time to repair the failed component.

Splitting the allowed outage time and assessing the repair and shutdown needs:

The allowed outage times for the critical failure situations can be split into two parts, priority being given to repair during the first phase. In most cases, the decrease in risk achieved from repairing the initially detected failure is large, so this is the most risk-effective way to reduce the situation-specific

risk level. If the repair cannot be completed in a short time, the time needed should be assessed and the redundant operation paths checked before the end of the first phase of the allowed outage time. If the operability of the redundant paths is successfully assured, which is the most likely outcome, the second part of the allowed outage time may safely be used to complete the repair. Alternatively, if more failures are identified or no repairs are considered possible during the remaining allowed outage time, the proper action can be decided, knowing the status of the plant systems. Usually, initiating shutdown without incurring more risk in the power generating state will be desirable.

Timing and target state for shutdown:

In high-risk failure situations, it may not be wise to delay the shutdown or stay in the intermediate states, when the need for shutdown becomes evident. The safest option will be to proceed quickly to the target state, if alternative back-up systems can be made available for shutdown cooling.

SURVEILLANCE TEST INTERVALS ADDRESSING ADVERSE EFFECTS[10]

Surveillance tests are required in nuclear power plants to detect failures in standby equipment to assure their availability in an accident. However, operating experience of the plants suggests that, in addition to the beneficial effects of detecting latent faults, the tests also may have adverse effects on plant operation or equipment. Examples of the adverse effects of testing are: (1) plant transient caused by the test, and (2) wear-out of safety system equipment due to repeated testing. Risk-based methodology can quantitatively evaluate both the beneficial and adverse effects of testing to decide on an acceptable test interval.

Figure 2 shows a typical result of the risk-effectiveness evaluation with respect to transients that may be caused by testing the main steam isolation valve (MSIV) of BWR plants. The figure shows the sensitivity of three kinds of test-related risks to the variation of test interval, T: (1) the test-caused CDF contribution due to transients, R_{trip}; the adverse effect of testing, (2) the test-detected CDF contribution, R_D, and (3) the total CDF impact of the test, R_T, which is the sum of R_{trip} and R_D. In this example, only the adverse effect of transients is considered, and other adverse effects are considered negligible.

To assure the risk-effectiveness of the testing, the test interval should be chosen such that R_D, the beneficial effect of testing, is equal to or greater than the adverse effect of testing, R_{trip}. As shown in the figure, when T is greater than 54 days, R_D is larger than R_{trip}, and the test is risk-effective; where $T <$ 54 days, the test is risk-ineffective.

The results of this type of quantitative risk evaluation can be used to define surveillance requirements. In many cases, additional qualitative considerations, e.g., radiation exposure to personnel from the tests, burden of work on the operator conducting the test, should be addressed in arriving at the requirement for test frequency.

SCHEDULING MAINTENANCE DURING POWER OPERATION VERSUS SHUTDOWN[11]

The original concept for separating maintenance between shutdown and power operation was to perform as much maintenance as possible during plant shutdown to reduce the risk from component downtimes during power operation. The need to carry out more maintenance during power operation is based on two factors: a) longer fuel cycles and the desire to shorten plant outages, and b) the effect of maintenance on improving the reliability of equipment.

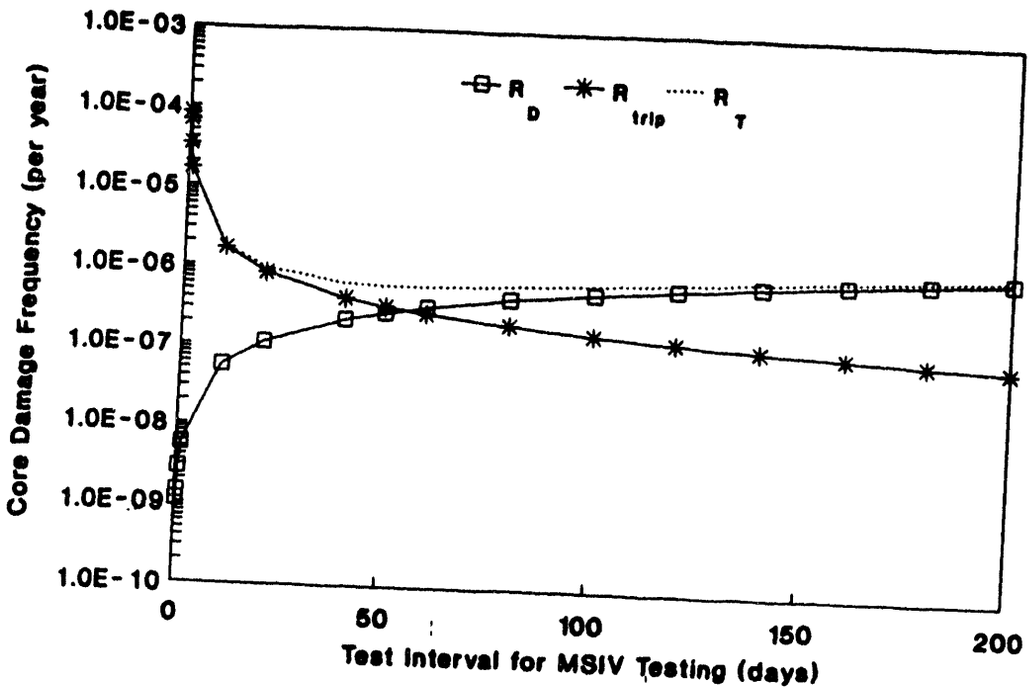


Figure 2: Sensitivity of the core-damage frequency impact to the interval for testing the main steam isolation valve (R_D = test-detected risk impact; R_{trip} = test-caused risk impact due to transients; R_T = total risk impact of the test).

The desire to shift certain portions of maintenance activities to power operation is based on the following considerations:

- Many maintenance activities require a relatively short duration, e.g., changing oil, and can significantly contribute to the reliability of the equipment.
- The level of plant risk can be maintained the same or even slightly decline when a portion of preventive maintenance (PM) is transferred from shutdown periods to during power operation.
- The risk during shutdown period also can be significant, and maintenance of multiple equipment during that period can pose a high risk.
- The distribution of maintenance between power operation and shutdown periods provides operational flexibility; scheduling of maintenance and management of maintenance personnel become easier.

The concerns with such shifting of maintenances result from the following:

- The primary motivation for carrying out maintenance during power is to reduce the plant's outage period.
- Many maintenance tasks could be scheduled just prior to entering a plant outage, thereby significantly increasing the risk then.

It is clear that optimization of maintenance during power operation versus shutdown can improve the safety of the plant. Such practices are expected to be more prevalent as the amount of maintenance increases, and also as the number of redundancies increase, giving in a larger number of components requiring more maintenance.

In an application, the relative advantages and disadvantages of maintenance the emergency diesel generator (EDG) during power operation and shutdown periods are studied to determine how its maintenance needs can be balanced.

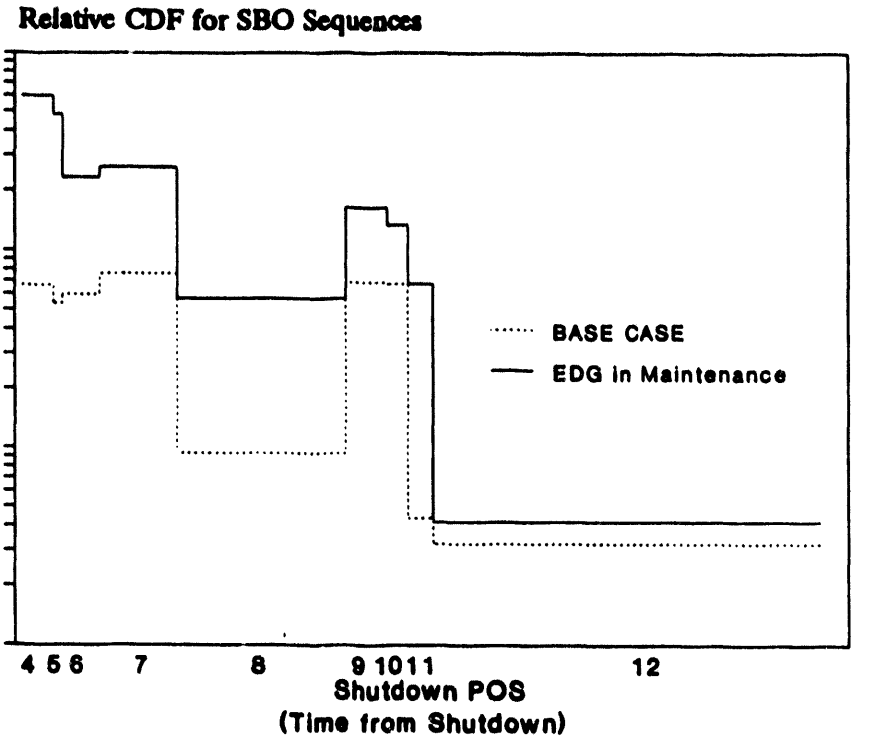
To assure the reliability of EDGs, preventive maintenances are scheduled regularly. For the US plants, on the average an EDG is unavailable for maintenance approximately 2% during power operation and 12% of shutdown periods, i.e., considering a plant with 80 percent capacity factor, an EDG is unavailable for maintenance about 15 days per year. An important factor in the decision is the relative risk impact of EDG maintenance during power operation versus plant shutdown. If possible, the burden of EDG maintenance should be on those periods when its impact on plant risk is minimal.

PSA-based calculations assess the risk impact of taking the EDG out-of-service for maintenance. The risk impact is assessed in terms of the CDF. The conditional CDF, given that EDG is unavailable for maintenance, is calculated to identify the risk impact during different plant operation periods (shutdown vs. full power). For full-power operation, a single conditional CDF, given an EDG is in maintenance, is calculated using the corresponding full-power PSA. The shutdown periods are divided into a number of plant operational states (POSs), each represented by the respective PSA model which is used to calculate the CDF. The low power and shutdown PSA for a pressurized water reactor has 15 defined POSs, whereas there are 7 for a boiling water reactor. The impact of EDG maintenance differs from one POS to another. Accordingly, the effect of EDG maintenance on CDF is calculated for each POS using the respective CDF model.

The conditional CDF, given EDG is in maintenance, between power operation and shutdown periods, and among the shutdown POSs are compared to identify the periods when the risk-impact of EDG maintenance is minimal.

Figure 3 gives an example analysis. The risk impact of EDG maintenance (in terms of conditional CDF) was evaluated for full power operation, and also, for POSs 4 through 12 during a shutdown. The reason for choosing these POSs is that EDG maintenances are performed during these POSs, as indicated in plant records.

The figure shows the conditional CDF given EDG in maintenance, for different POSs. The baseline CDF for each of the POSs also is shown. The risk of EDG maintenance during early stages of cold shutdown (POS 4, 5), and the midloop operations (POS 6, 10) is relatively high. Times when the risk impact of EDG maintenance is low are POS 8 and 12, i.e., during refueling, and when the RCS is filled following refueling.



POS1 -Low Power Operation and Reactor Shutdown
POS2 -Cooldown with SGs to 345°F
POS3 -Cooldown with RHR to 200°F
POS4 -Cooldown with RHR to 140°F
POS5 -Draining the RCS to Midloop
POS6 -Midloop Operation
POS7 -Fill for Refuelling
POS8 -Refuelling
POS9 -Draining RCS to Midloop after Refueling
POS10-Midloop Operation after Refueling
POS11-Refill RCS Completely
POS12-Bubble

Figure 3: CDF for SBO Sequences due to EDG Maintenance During Different Shutdown POSs. (Scale in x-axis is proportional to average POS duration.)

The insights from this type of analysis can be used in making the decision to schedule EDG maintenance during power operation versus shutdown.

- The risk impact of EDG maintenance during certain shutdown periods is comparable to that during power operation. From risk considerations, scheduling short duration EDG maintenance during power operation is acceptable. The risk impact then can be controlled by defining allowed periods, by the availability of redundant equipment, and by taking precautions during the maintenances such that chances for loss-of-offsite power are reduced.

- The risk impact of EDG maintenance during certain shutdown periods, including early stages of cold shutdown, is considered high, and any EDG maintenance should be avoided.

- The risk impact of EDG maintenance during certain shutdown periods (e.g., refueling POS) is negligible, so long EDG maintenance preferably should be scheduled then.

SUMMARY

A handbook is being developed to present methods for the risk-based analysis of Technical Specification requirements in nuclear power plants. The scope of the handbook includes reliability and risk-based methods for evaluating allowed outage time (AOTs), action statements requiring shutdown where shutdown risk may be substantial, surveillance requirements (SRs), treatment of common-cause failures, managing the outage configuration of equipment, and scheduling maintenances. The handbook is expected to result in consistency both in the application of risk-based methods to improve TSs, and in the review of such analyses.

REFERENCES

1. U.S. Nuclear Regulatory Commission, "Technical Specifications - Enhancing the Safety Impacts," NUREG-1024, November 1983.

2. R.L. Jansen, L.M. Lijewski, and R.J. Masarik, "Evaluation of Surveillance Frequencies and Out-of-Service Times for the Reactor Protection Instrumentation System: WCAP-10271," January 1983.

3. W.P. Sullivan et al., "Technical Specification Improvement Analysis for BWR Reactor Protection Systems," NEDC-30851P, General Electric Proprietary Information, May 1985.

4. Houston Lighting and Power, "Proposed Amendment to South Texas Project Unit 1 and Unit 2 Technical Specifications Based on Probabilistic Risk Analysis," ST-HL-AE-3283, February 1, 1990.

5. P.K. Samanta, S.M. Wong, J. Carbonaro, "Evaluations of Risks Associated with AOT and STI Requirements at the ANO-1 Nuclear Power Plant," NUREG/CR-5425, BNL-NUREG-52213, August 1988.

6. D.P. Wagner, W.E. Vesely, and L.A. Minton, "Risk-Based Evaluation of Technical Specifications," EPRI-NP-4317, Electric Power Research Institute, March 1982.

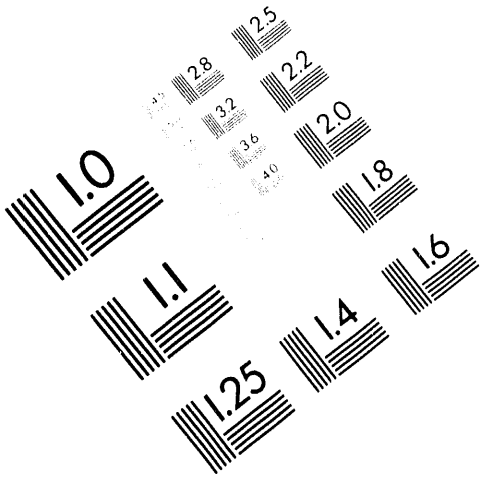
7. IAEA-TECDOC-599, "Use of Probabilistic Safety Assessment to Evaluate Nuclear Power Plant Technical Specifications," Report of a Technical Committee Meeting, Vienna, June 18-22, 1990.

8. K. Laakso, (Ed.), Optimization of Technical Specifications by Use of Probabilistic Methods - A Nordic Perspective, NKA/RAS-450, Nordic Liaison Committee for Atomic Energy, November 1989.

9. T. Mankamo, I. Kim, and P. Samanta, "Technical Specification Action Statements Requiring Shutdown: A Risk Perspective with Application to the RHR/SSW Systems of a BWR," NUREG/CR-5995, Brookhaven National Laboratory, November 1993.

10. I.S. Kim, S. Martorell, W.E. Vesely, and P. Samanta, "Quantitative Evaluation of Surveillance Test Intervals including Test-Caused Risks," NUREG/CR-5775, Brookhaven National Laboratory, February 1992.

11. P.K. Samanta, I.S. Kim, S. Uryas'ev, J.P. Penoyar, and W.E. Vesely, "Analysis of Emergency Diesel Generator Unavailability and its Risk Impacts," NUREG/CR-5994, Brookhaven National Laboratory (to be published).

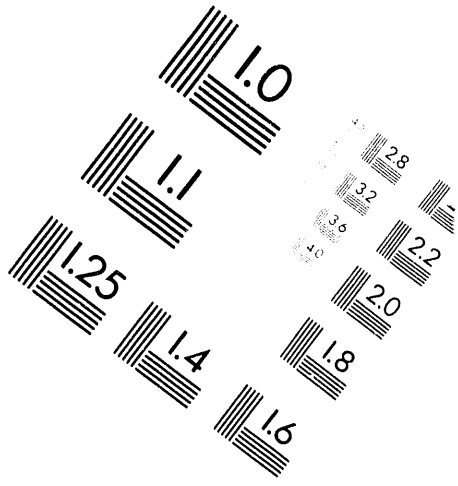


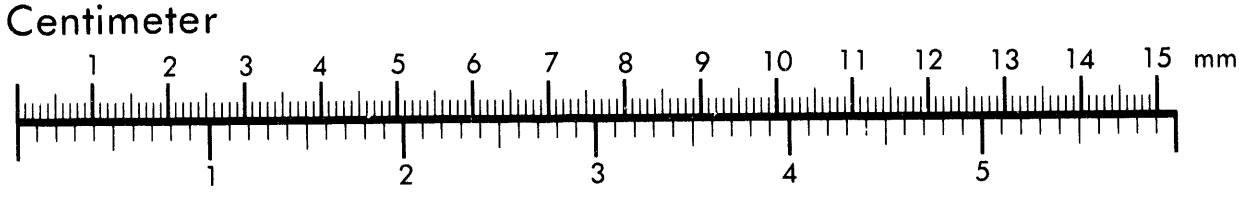


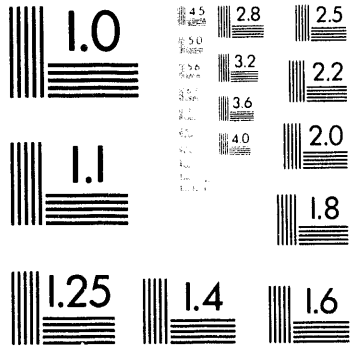
Association for Information and Image Management

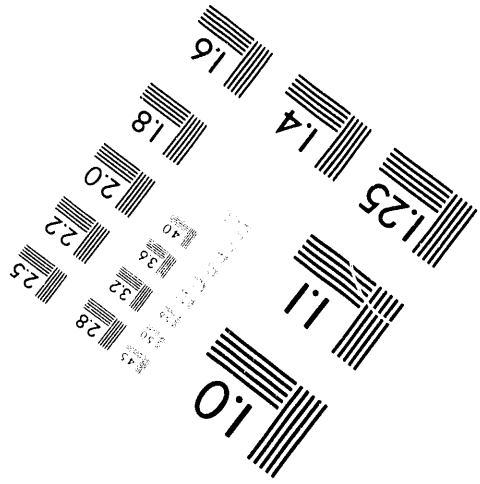
1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910

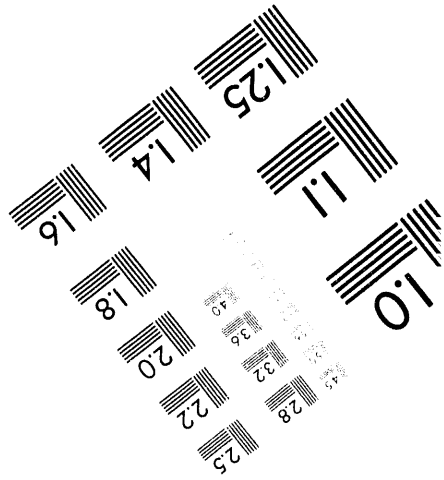
301/587-8202











MANUFACTURED TO AIIM STANDARDS
BY APPLIED IMAGE, INC.

5 of 7

Overview of AEOD's Program for Trending Reactor Operational Events

Patrick W. Baranowsky, Patrick D. O'Reilly,
Dale M. Rasmuson, and James R. Houghton

Trends and Patterns Analysis Branch
Division of Safety Programs
Office for Analysis and Evaluation of Operational Data
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Abstract

This paper presents an overview of the trending program being performed by AEOD. The major elements of the program include: (1) system and component reliability trending and analysis, (2) special data collection and analysis (e.g., IPE and PRA component failure data, common cause failure event data), (3) risk assessment of safety issues based on actual operating experience, (3) Accident Sequence Precursor (ASP) Program, and (4) trending U. S. industry risk. AEOD plans to maintain up-to-date safety data trends for selected high risk or high regulatory profile components, systems, accident initiators, accident sequences, and regulatory issues. AEOD will also make greater use of PRA insights and perform limited probabilistic safety assessments to evaluate the safety significance of qualitative results. Examples of a system study and an issue evaluation are presented, as well as a summary of the common cause failure event database.

1. INTRODUCTION

After the accident at Three Mile Island in 1979, the U. S. Nuclear Regulatory Commission (NRC) recognized the need to have a program for systematically screening and analyzing data from operating nuclear power plants. A capability to perform independent analyses of operational data was added to the NRC in 1980 to help identify previously unrecognized safety concerns and supplement reviews conducted by regional and headquarters program offices.

Today, the NRC continues its heavy emphasis on safe plant operations and analysis of operational data. In this regard, the Office for Analysis and Evaluation of Operational Data (AEOD) has as one of its responsibilities the systematic screening and analysis of operational data to identify historical trends and patterns of nuclear power plant operations and safety implications of these trends. AEOD's traditional approach of identifying and analyzing safety issues based on reported operating experience is being heavily supplemented with the application of reliability and risk methods. Reliability and risk analysis techniques are being systematically applied to: (1) identify and provide a quantitative context for new safety issues; (2) evaluate the effectiveness of current

regulations, regulatory actions, and initiatives taken by licensees to resolve safety concerns; (3) help guide and focus follow-on studies; (4) facilitate comparison between licensee event report (LER) actual operating experience and PRA/IPE assumptions, input data, and results; and (5) provide failure rate data for agency-wide use that is directly related to operating experience.

In the past, most trends and patterns analyses involved statistical analyses of data from the Sequence Coding and Search System (SCSS) data base and Nuclear Plant Reliability Data System (NPRDS) component failure data. Risk insights were not routinely incorporated into these analyses or used to identify which components or systems should be analyzed. Under its new charter, the Trends and Patterns Section (TPS) in the Trends and Patterns Analysis Branch, Division of Safety Programs, AEOD, is responsible for analyzing operational data to achieve the objectives identified above.

Section 2 presents an overview of AEOD's trending analysis program. Section 3 summarizes the methods and procedures being formalized to perform these studies. System trending studies are discussed in Section 4, where the results of a reliability analysis of the BWR High Pressure Core Injection system are summarized. Section 5 provides an example of safety issue trending. Component studies are discussed in Section 6. Section 7 discusses special databases and uses common cause failure events as an example. Section 8 provides a listing of additional activities being pursued or planned.

2. OVERVIEW OF THE TRENDING ANALYSIS PLAN

Figure 1 contains an overview of the planned trending activities. The center box (**Trending Analyses**) is the main activity. These trending analyses will consist of a disciplined, systematic process for analyzing operational experience data for trends and patterns. To focus the efforts and resources of the AEOD, risk insights from past PRAs, NUREG-1150 studies, the Individual Plant Examinations (IPEs), and other risk and reliability studies will be used to determine which hardware items should be trended. Such items include components, trains, systems, initiating events, and accident sequences. The identification of risk-important items is the objective of the box labeled "**Identification.**" In addition to hardware items, AEOD plans to trend important regulatory issues and industry initiatives. Other sources of information, such as Augmented Inspection Team (AIT) reports and Incident Investigation Team (IIT) reports, will also be used to identify important hardware items and issues.

The main sources of operational event and component data to be used by the Section are still SCSS and NPRDS, as indicated by the "**Data Sources**" box. Other data sources, such as inspection reports and information provided in response to generic letters and bulletins, will also be used. These data bases will be searched using strategies developed to identify information pertinent to the analysis of the specific hardware or safety issue being considered.

Where appropriate, statistical analyses will be performed as part of the trending assessments. In addition, risk-related evaluations will be made (e.g., evaluation of the impact of a industry failure rate on PRAs loaded into IRRAS). The trending assessments will produce statistical results and PRA-related results which can be used by others at the NRC and may be used in future trending analyses. It is planned that the analysis of risk-important hardware items and safety issues will be updated on a periodic basis.

The box on the right labeled "**Special Data Bases**" is an important part of the analysis activities. Some issues (e.g. common cause failures and loss of off-site power events) require a significant expenditure of resources to properly assess, especially in the data collection and searches. Thus, it is cost beneficial to develop special data bases for use with these types of data. These data bases will be used regularly in trending analyses and inputs into staff regulatory analyses as needed.

The top box is labeled "**Industry Risk Profile.**" As risk-important hardware is trended and updated risk impacts are calculated, these results can be used, either directly or indirectly,

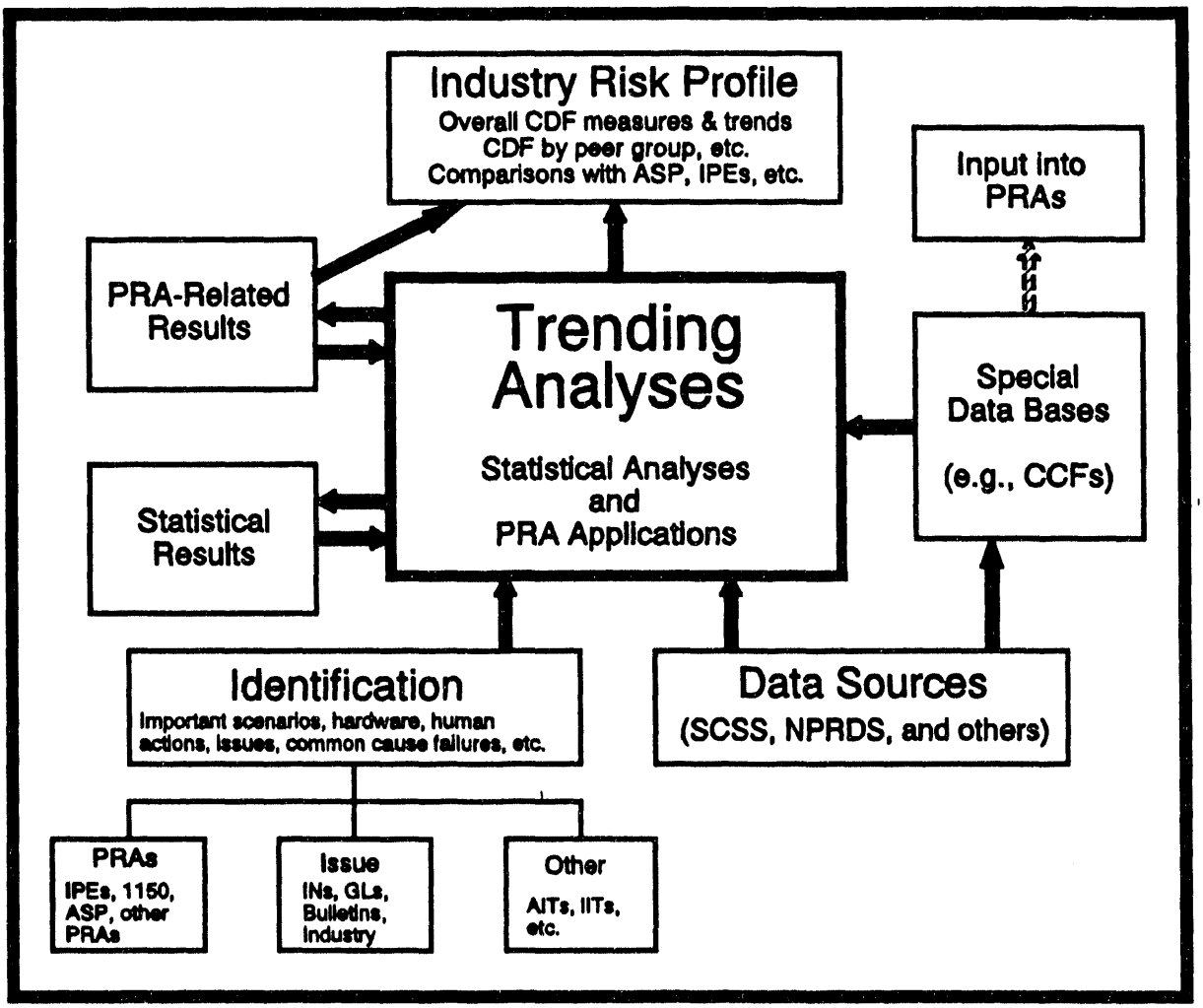


Figure 1. Overview of Trends and Patterns Planned Activities

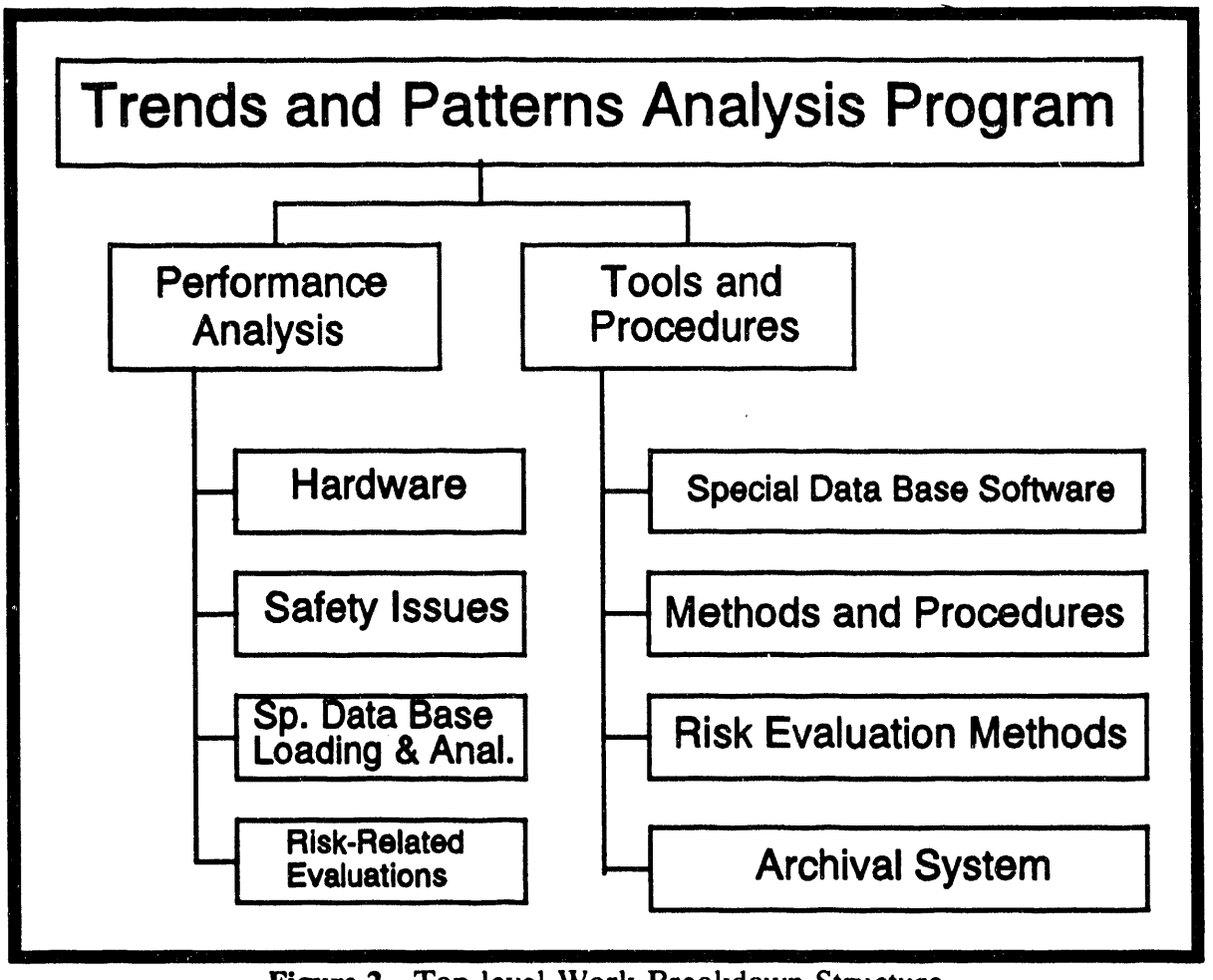


Figure 2. Top-level Work Breakdown Structure

to characterize overall risk of nuclear power plants. This concept will be developed and implemented as the trending analyses progress. It is meant to be complementary to the Accident Sequence Precursors (ASP), but it will make use of lower level (component) data.

For those items identified as important for trending, an initial analysis will be performed. This analysis is governed by a procedure. These items will be updated on a periodic basis. The frequency of the update will depend upon the particular item.

Another type of analysis which is performed by AEOD is a special or statistical study. These studies are usually undertaken in response to a specific request or need (e.g., it may be initiated by a request from the Commission or the Executive Director of Operations). The issue or item of interest may be entirely unrelated to the routine trending activities.

Figure 2 shows a further breakdown of the Trends and Patterns Analysis Program. The program contains two major elements: (1) performance analysis of hardware items and issues, and (2) development of procedures, guidance, and methods necessary for performing the analyses. Each activity is further divided into (program activity) elements.

Performance analysis has been separated into four major elements. The first element is hardware performance. Trends in risk-important components, systems, initiating events, and sequences will be identified and analyzed. The second element consists of trending of important regulatory and safety issues, including industry-sponsored initiatives. The third element focuses on issues and concerns for which special data will be collected and analyzed. Examples of such items are common cause failures, human performance, loss of offsite power, and diesel generators. The last element consists of risk-related evaluations of trends.

To perform these types of analyses and evaluations in a consistent and technically sound manner, appropriate guidance and methods are needed. That is the focus of the second program activity shown in Figure 2. Its first element includes developing the software needed for the special data bases. The second element addresses the development of guidance and methods for performing routine trends and patterns analyses. The guidance will include selection and use of statistical techniques for assessing trends, ways of displaying information, etc. The third element focuses on the use of risk evaluation methods for trending studies and in the trending of an industry risk profile. The fourth element is the development of an archival and retrieval system so that the information from prior studies can be saved and easily retrieved when needed in the future.

3. METHODS AND PROCEDURES

To ensure that system, component, and issues trending analyses and their updates are performed in a systematic and scrutable manner, AEOD is developing procedures for their performance. The main steps in the procedures consist of: (1) precise definition of the item being analyzed and its related success criteria, (2) collection and characterization of the failure data, (3) verification of the statistical assumptions, (4) calculation of the appropriate reliability characteristics of the item with uncertainty, (5) comparison with PRA results (if appropriate), and (6) characterization of engineering insights.

A working meeting was held in September 1992 to discuss appropriate statistical analyses and methods which meet the analysis objectives identified in Section 2. Using valid statistical procedures and checking the validity of basic statistical assumptions upon which the statistical methods rely produces a credible analysis.

The types of statistical procedures AEOD is documenting include:

- statistical methods for analyzing failures on demand,
- statistical methods for analyzing failures in time,
- guidance on gathering failure data for statistical and engineering analyses,
- tests of hypothesis of constant Poisson failure rate,
- investigation of time trends of binned Poisson data, and
- guidance on applying statistical methods appropriately (e.g., how to look further when a chi-square test rejects a simple model).

4. SYSTEMS STUDIES

Table 1 contains a list of the risk-important systems identified for trending from a limited set of PRAs that are available in the MAR-D data base. AEOD is trending these systems for overall performance using actual demand data from the LER database. The initial time period is from 1987 through 1992. System success criteria will be identified and a simple train level logic model developed for each system. Support system failures will, in general, not be included in the evaluation. The reactor protection system and emergency AC power system are being analyzed separately. The service water system was analyzed as an issue.

The evaluation consists of identifying which LERs pertain to the given system, reading the full-text LERs to determine the applicability of the event to the system, binning the demands and failures according to the logic model, and calculating the overall system performance using appropriate statistical techniques. The results of the performance evaluation, engineering insights gained from the LER review, and comparisons with PRA models will be documented in a report. The report will receive a peer review before it is published.

Table 1. Initial List of Risk-Important Systems for Trending

Boiling Water Reactors	Pressurized Water Reactors
High Pressure Core Injection	Auxiliary Feedwater System
High Pressure Core Spray	High Pressure Spray Injection
Isolation Condenser	Low Pressure Spray Injection
Reactor Core Injection and Cooling	Purification and Letdown
Residual Heat Removal	Primary Pressure Relief
Reactor Protection System (Detailed)	Reactor Protection System (Detailed)
DC Power	DC Power
Service Water System (Issue)	Service Water System (Issue)
Emergency AC Power (Detailed)	Emergency AC Power (Detailed)
Primary Pressure Relief System	

High Pressure Core Injection System

The High Pressure Coolant Injection (HPCI) System analysis will be used as an example of the types of analyses AEOD is performing. These results are preliminary since the report has not received a peer review.

The HPCI system is the high-pressure subsystem of the Emergency Core Cooling System for BWR/3 and BWR/4 plants. The HPCI is a single-train system comprised of a steam turbine-driven pump that is supplied with steam form one of the main steam lines and exhausts into the suppression pool. It is found in 23 operating BWRs.

The HPCI system scope for this study includes the pump, valve and valve operators, and associated piping from the normal and alternate pump suction source including the HPCI pump discharge up to the penetration of the feedwater line, and the last check valve of the normal feedwater discharge line. The steam turbine-driven pump included all steam piping, valves and valve operators, gland sealing steam and the turbine auxiliary oil system. HVAC systems and room cooling associated with the HPCI system were included, with the exception of the service water system that supplies cooling to the room coolers. Only specific losses of service water to individual HPCI room coolers were included and not the entire service water system loss.

The success criterion used in the study for system operability on demand was the system being capable of providing at least 90% of the design coolant flow rate to the reactor vessel and maintaining the core covered with coolant for the entire PRA mission time. The mission time may include periods of recirculation rather than injection, but the system must be capable of injecting at any time during the event. The failure modes used in the study were failure to start (FTS) and failure to run (FTR). Non-recovery of each failure mode was also treated in the analysis. They are denoted by NR(FTS) and NR(FTR). In addition, unavailability due to maintenance out-of-service (MAINT) was also treated in the evaluation. Bayesian statistical methods were used in the analysis. Figure 3 contains the 90% Bayes intervals for each failure mode.

For the pooled data and each failure mode, FTS and FTR, the counts were summed over the plants by year, yielding a total number of failures and demands for each year from 1987 through 1992. A contingency table was used to see if there were any statistically significant differences between the years. No statistically significant difference was seen between years.

The *operational unreliability* of the HPCI system was obtained using the following:

$$P\{[FTS \text{ AND } NR(FTS)] \text{ OR } [FTR \text{ AND } NR(FTR)] \text{ OR } MAINT\}.$$

The distribution for the operational unreliability was found by computing the mean and variance of each of the five input beta distributions using simple formulas for the moments of a beta distribution, computing the mean and variance of the operational unreliability (assuming only that the input distributions are statistically independent). The 5th and 95th percentiles of this distribution form a 90% interval for the operational unreliability. Although the final moment matching step is an approximation, the resulting end points are close to the values obtained from a Monte Carlo simulation with the above beta distributions. This probability interval is also shown in Figure 3.

The calculations for operational unreliability were also performed for each year. The resulting unreliabilities by year are shown in Figure 4, with the Bayes means and 90%

intervals. The bounce in 1989 is misleading. It appears because the only maintenance out-of-service event occurred in 1989, making the unavailability for that year appear high. In addition, the unreliability using the pooled data is shown and labeled "Total." The estimated annual unreliabilities tend to be larger than the estimated total unreliability. The reason is that the prior distribution has more influence on the relatively sparse data for a single year than when the data are pooled. Therefore, it pulls the annual estimates of the various failure probabilities farther towards the prior mean of 0.5. Because there was no significant difference seen between years for any of the failure modes, the total unreliability is the appropriate estimate to use in any analysis.

To put the failure probabilities into perspective, HPCI evaluations from two full-scale plant probabilistic risk assessments were reviewed. The distributions of the five failure modes were input into a fault tree combining the failure modes, and the HPCI unreliability was estimated by Monte Carlo simulation. The results were very close to the calculated unreliability shown in Figures 3 and 4. A comparison with the plant PRAs is shown in Table 2. Note that the two PRAs and the historical experience analyzed in the study are in general numerical agreement.

Because of differences between severe accidents modeled in PRAs and the types of events entering the data-based estimate of the probability of failure to run, the calculated probability of failure to run should be used in probabilistic studies with caution. The mission times in the operational event data were much shorter, and HPCI was often used in more operating modes than in the severe accidents typically modeled in a PRA. The data alone do not support an assumption that operability of the HPCI system in a severe accident is the same as in the operational data.

Table 2. HPCI Results Comparison

Study	System Results		
	5th Percentile	Mean	90th Percentile
Peach Bottom	2.1E-2	9.5E-2	2.7E-1
Brunswick 1	5.3E-2	1.8E-1	4.5E-1
Brunswick 2	4.2E-2	1.4E-1	3.4E-1
Historical Experience	3.5E-2	1.0E-1	2.1E-1

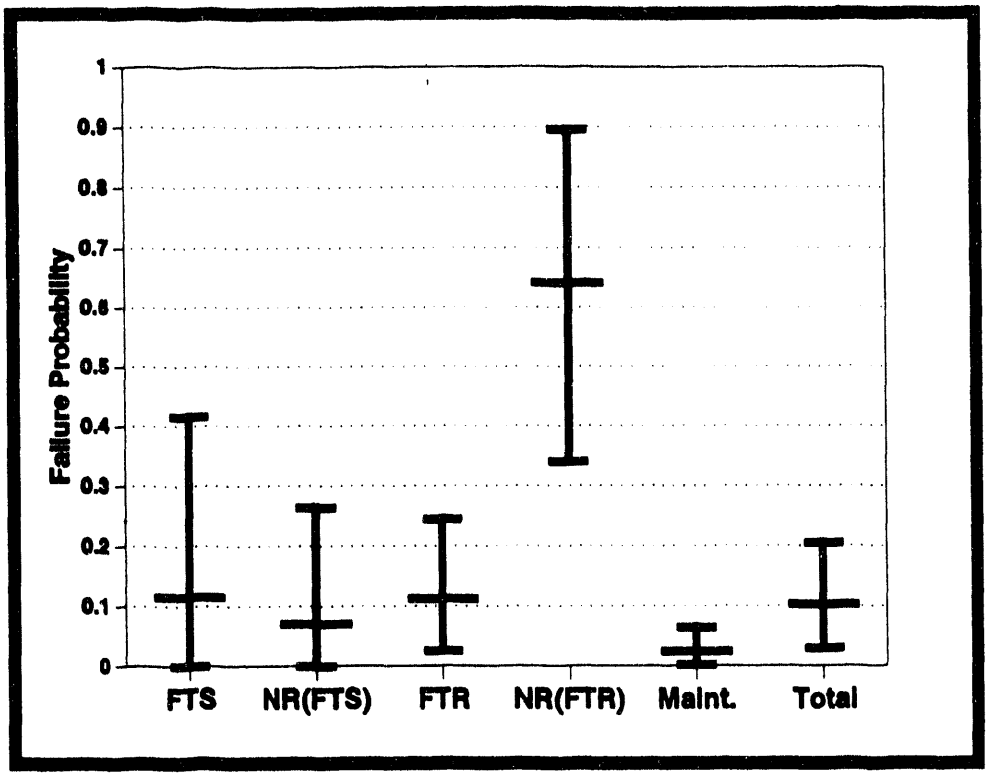


Figure 3. HPCI Failure Probability by Failure Mode.

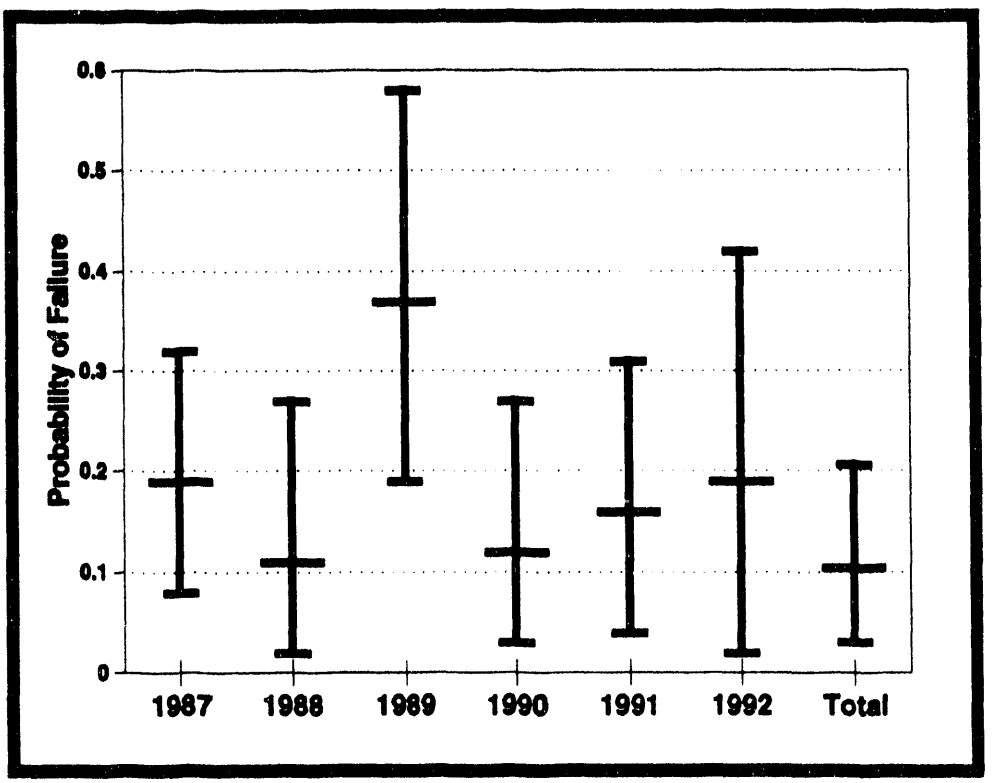


Figure 4. HPCI Operational Unreliability by Year.

5. SAFETY ISSUE TRENDING

Safety and regulatory issues and concerns will be analyzed on a regular basis. Safety and regulatory issues can be identified by any NRC headquarters or regional office. An example of a safety issue is Service Water System (SWS) degradation. Another example is in the evaluation of low power/shutdown events. Another way these issues will be identified is by a systematic review of generic letters, bulletins, information notices, etc. Industry initiatives sponsored by NUMARC, EPRI, and INPO in response to NRC efforts will also be evaluated as candidates for trending.

Service Water System Performance

In 1989, the NRC issued Generic Letter 89-13, Service Water System Problems Affecting Safety-Related Equipment." Since that time, SWS problems appeared to be continuing since the issuance of GL 89-13. NRR developed a task action plan to resolve these continuing problems.

To monitor the effectiveness of the task action plan, NRR requested AEOD support in analyzing and developing trends in SWS operating experience. This study was an update of the 1988 AEOD study published in November 1988 as NUREG-1275, Vol. 3, "Operating Experience Feedback Report - Service Water System Failures and Degradations." The more recent study used LER SWS events over the time period 1986 through 1991. The total number of events involving SWS was 361. The yearly distribution of these LERs is shown in Figure 5. Sixty-four of the events were identified as involving system failure/degradation as shown in Table 3.

The events were classified into three: cause categories mechanistic, personnel/procedures, and design/seismic. The yearly distribution of these failure categories is shown in Figure 6. The mechanistic cause category was further subdivided into four classes - silting/sediment, biofouling, corrosion/erosion, and foreign material/debris. The yearly distribution of the mechanistic causes is shown in Figure 7.

This updated SWS study concluded that analyzing and developing trends for SWS events represents a useful method for monitoring whether industry is resolving failure and degradation problems associated with the SWS. Use of the mechanistic cause categories, both separately and combined, will provide data that is more applicable to trending. The study also identified that a majority of events and component failures occurred at plants located in Regions I and II. Finally, the study indicated that baseline operational event data for 1986 through 1991, and for a shorter, more recent period (1990-1991) have not provided conclusive evidence that the issuance of GL 89-13 has resolved SWS degradation problems.

Table 3. Distribution of SWS Degradation Events

Severity of Event	Number of Events
Complete Loss of Service Water System Function	0
Total Loss of SWS - Actual	0
Total Loss of SWS - Conditional	8
Potential Total Failure of SWS - Design Deficiency	11
Partial Failure/Degradation of SWS - Actual	15
Partial Failure/Degradation of SWS - Conditional	2
SWS-Caused Failure/Degradation of Another System	28

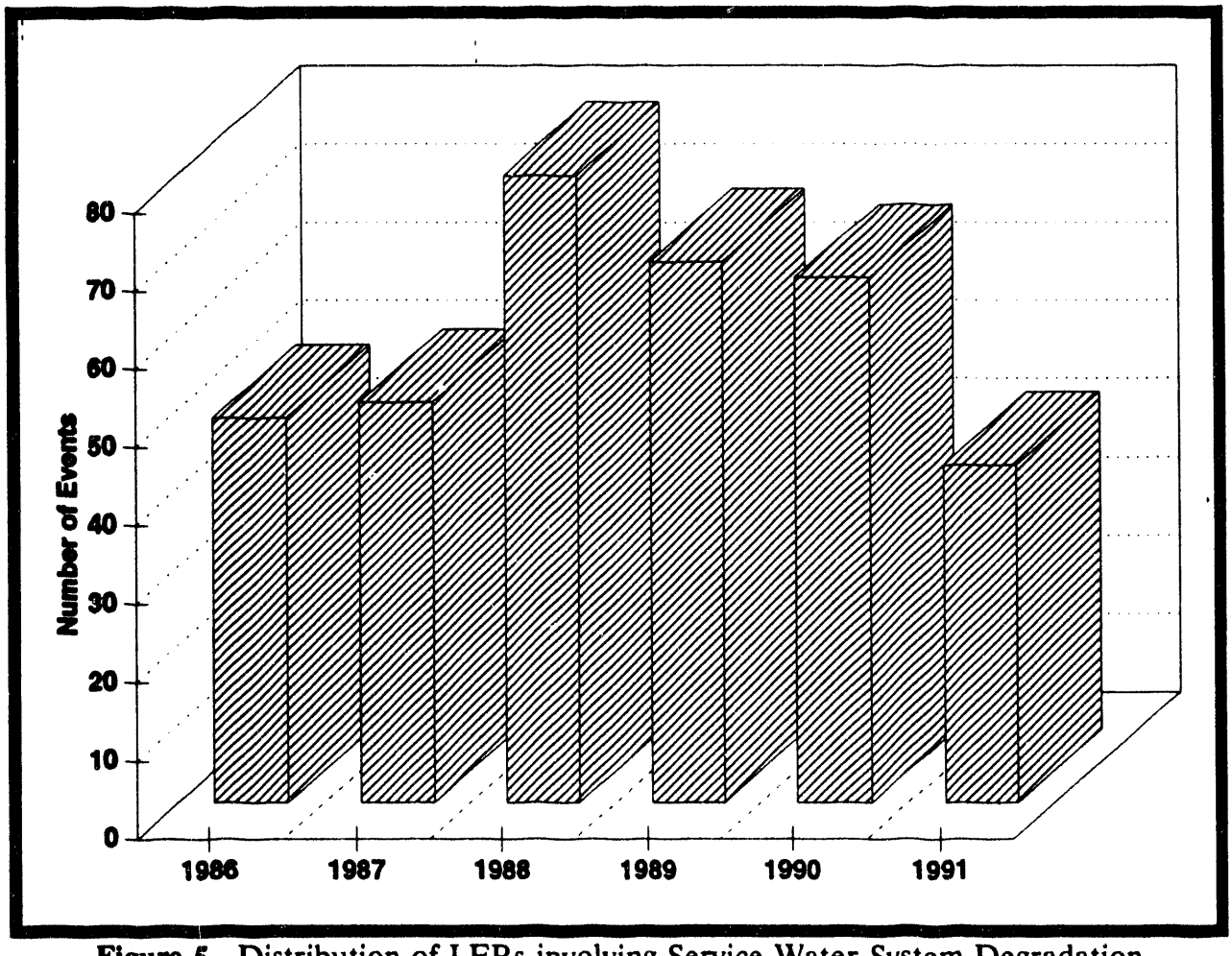


Figure 5. Distribution of LERs involving Service Water System Degradation

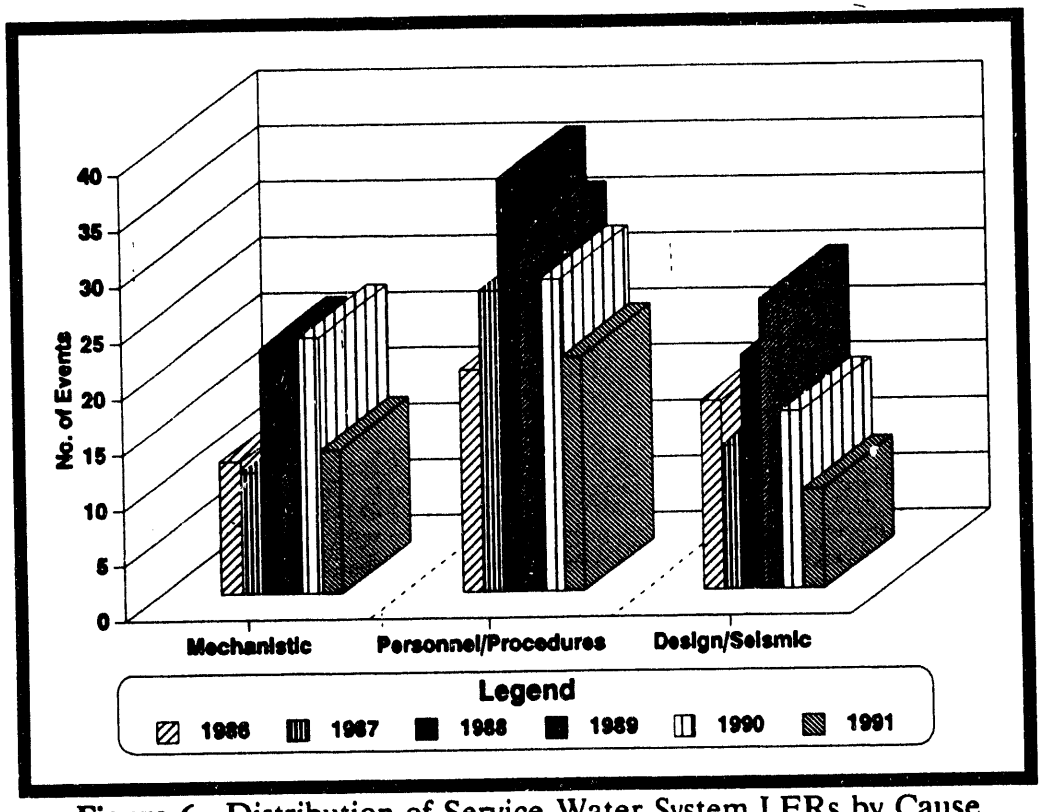


Figure 6. Distribution of Service Water System LERs by Cause

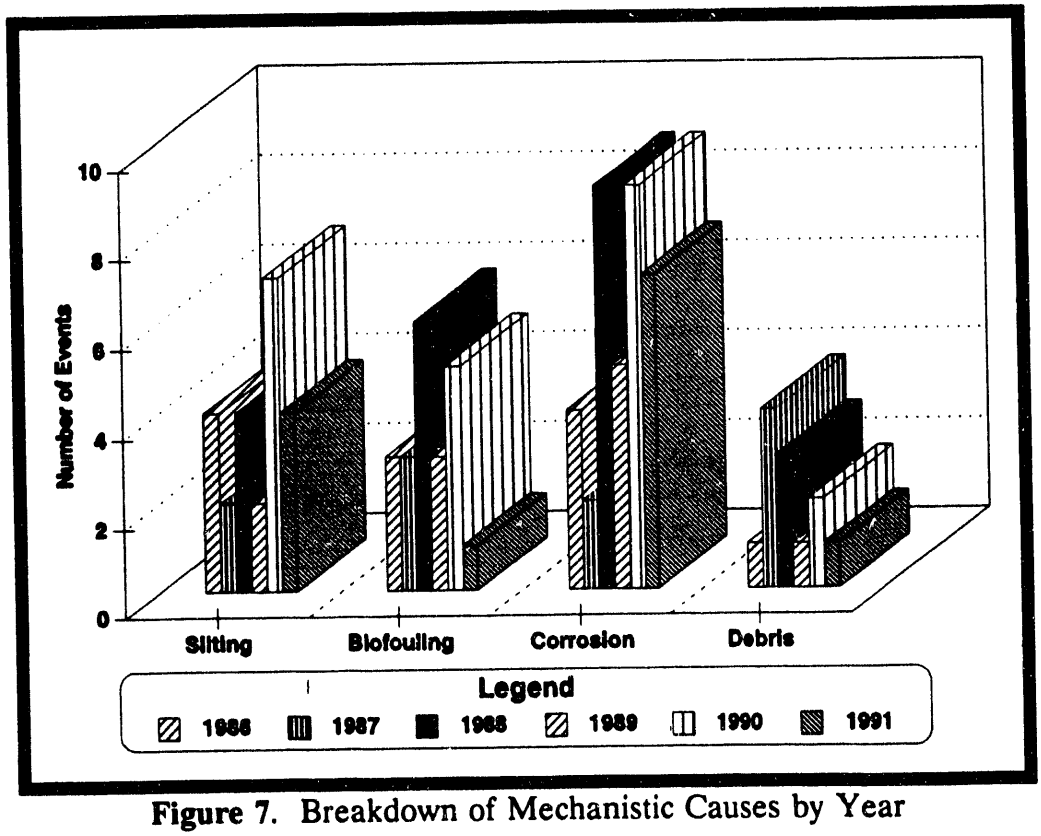


Figure 7. Breakdown of Mechanistic Causes by Year

6. COMPONENT STUDIES

Another activity is trending component performance. Risk-important components were identified from existing PRAs. The initial list of components includes:

- Air-operated valves,
- Motor-operated valves,
- Solenoid valves (process),
- Check valves,
- Circuit breakers,
- Motor-driven pumps,
- Batteries,
- Strainers,
- Pressure sensors,
- Heat exchangers,
- Turbine-driven pumps, and
- Emergency diesel generators.

The main database to be used in these studies is NPRDS. The first task is to express PRA component boundaries in terms of NPRDS-reportable components. For some components, such as pumps and valves, this is fairly straightforward. For others, such as diesel generators, it is a more formidable task. Only catastrophic failures for the failure mode of interest are used in these analyses.

One problem encountered when estimating demand data is the number of demands on the component. The surveillance testing frequency for a given component is contained in the engineering data in NPRDS, but this information is not verified by the NPRDS quality assurance process. However, reasonable results may be obtained using this information. It is probable that these surveillance testing frequencies are conservative (i.e., the actual number of demands is larger than the reported testing frequency). This implies that the estimate of the probability of failure on demand for the given component will be larger than estimates obtained using the actual number of demands.

The initial studies will use data from 1987 through 1992. Calculations for individual plants will be performed when there is sufficient data. This will allow for an estimate of between-plant variability.

7. SPECIAL DATA BASES

There are a number of areas and items (e.g., common cause failures, human performance, loss of offsite power, and diesel generators) for which data are not captured adequately in global data systems. This element consists of taking a subset of data for a special area from such a global system and converting the data into more useful information through the use of an analytical process. In this process, qualitative information is derived that goes beyond the numbers captured in the raw experience data. An intrinsic advantage in the creation of such a data base in this manner is that it yields traceable results. The activities relevant to some of these special data bases are discussed separately in the following sections.

Common Cause Failure Event Database

A generic conclusion from PRAs of nuclear power plants is that common cause failures (CCFs) are a significant contributor to the unavailability of safety systems. Efforts in the past ten years to improve the ability to understand and model CCFs have produced several models, procedures, computer codes, and databases. In each category, weaknesses and shortcomings have been discussed to various degrees in the literature.

Lack of common cause failure event data is still a major problem, though significant progress has been made, particularly with the publication of Reference 1. Two of the known problems are: 1) limitation of the database period to approximately before 1982, and 2) the lack of details regarding independent events. In the area of data classification and analysis and model parameter estimation, the detailed procedures of References 2 and 3 have been viewed as too time consuming, despite wide acceptance of the basic approach.

Alleviating these problems is one of the motivations behind an AEOD-sponsored project with the objectives of: 1) developing a comprehensive database of common cause failure events using several data sources, such as LERs contained in SCSS, and NPRDS; and 2) automation of data analysis and parameter estimation procedures of References 2 and 3. This paper summarizes the achievements of the project in both areas and offers some conclusions based on analysis of a subset of the data. The steps in the CCF event identification process and the LER and NPRDS search strategies are also summarized.

The first task in the CCF event database effort was the development of specific guidance to be used by the data analysts to determine common cause failure events. The basic concepts and characteristics, which had been defined in a PRA context, were translated into engineering terms, with examples, to illustrate the definitions and concepts. The initial CCF event criteria include similar components, same failure mode, and failure of components involved in a short time interval. These characteristics are necessary for an event to be considered a common cause event. However, they are not sufficient. That is, the failures of the components must involve a shared cause.

Table 4. Event Cause/Mechanism Codes

State of another Component. The cause of the state of the component under consideration is the state of another component. Examples are loss of power and loss of cooling.

Design/Manufacturing/Construction Inadequacy. This category of causes encompasses actions and decisions taken during design or manufacturing or installation of components both before and after the plant is operational.

Procedures Inadequacy. This category refers to ambiguity, incompleteness, or error in procedures for operation and maintenance of equipment. These include inadequacy in construction or modification procedures, and administrative, operational, maintenance, test, and calibration procedures.

Human Actions, Plant Staff Error. represents causes related to errors of omission and commission on the part of plant staff, such as failure to follow a correct procedure. This category includes accidental actions, and failure to follow procedures for construction, modifications, operation, maintenance, calibration, and testing.

Abnormal Environmental Stress. This category includes all causes related to a severe environment that are not within the component's design specifications. Specific mechanisms include: chemical reactions, electromagnetic interference, fire/smoke, impact loads, moisture (sprays, floods, etc.,) radiation, abnormally high or low temperature, vibration load, and acts of nature.

Internal. The component state is due to malfunctioning of something internal to the component as a result of normal wearout or other intrinsic failure mechanism. It includes the influence of the ambient environment of the component. Specific mechanisms include erosion/corrosion, internal contamination, fatigue, and wearout/end of life.

Other. Cause is known, but it is not covered by the other categories in this scheme.

Unknown. The cause of the component state cannot be identified.

The next task was to revise existing classification schemes for use in the engineering review and with the database software. The classification schemes suggested in Reference 1 were picked as a starting point. One criterion used in the modification of the classification schemes was to make them simple and practical. Table 4 contains the modified failure cause/mechanism classification scheme. These coding schemes help the engineer classify the events in a consistent manner. They will provide the database user with useful information about CCF events.

In addition to these efforts, definitions and coding schemes for coding coupling strength (a measure of how closely the coupling factor ties two components together), time delay factor (how close in time the multiple failures occur), and failure mode applicability factor (the likelihood the failure mode will affect multiple components) were also developed and tested. These concepts and definitions are documented in a report which will be published.

Figure 8 contains the major steps in the CCF event classification process. The initial step is to identify those components for which CCF events are desired. The initial list was obtained from identifying the CCF events that are risk-important in several PRAs. The list includes such components as batteries, auxiliary feedwater system pumps, and emergency diesel generators. At this time, only components which are typically modeled in PRAs are being considered.

The next step is to perform CCF searches using available data sources. The main data sources available to the NRC for failures are LERs contained in the SCSS and component failure data contained in NPRDS. The search strategies were developed using the basic characteristics of a CCF event described above. The output from the search strategies are "potential" common cause failure events.

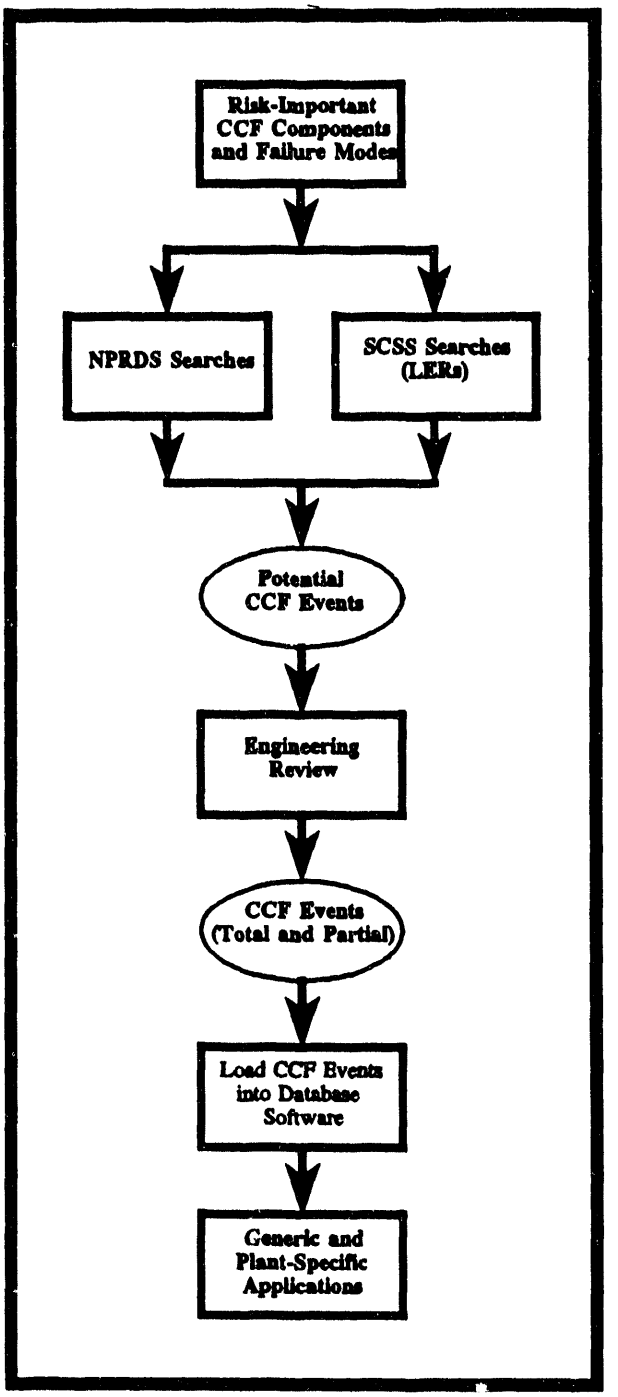


Figure 8. CCF Event Classification Process

The potential CCF events are then screened by engineers to determine when all the criteria for a CCF event are satisfied. The engineers read the failure narrative and cause descriptions of the NPRDS reports of the failures comprising the CCF event. The LER (full-text) is read for the potential CCF events identified by SCSS. Using the developed coding schemes, the time delay factor, coupling strength, failure mode applicability, and component degradation are determined.

The output from the engineering review are coding forms which contain the information related to the total and partial common cause failure events. This information for the events, from NPRDS and SCSS, are coded into the CCF event database for use by the NRC staff.

The database software allows the user to perform searches of the CCF events to meet the specific needs of the analysis. The user then has the choice of using the basic parameter model, the multiple Greek letter model, or the alpha factor model for quantifying the CCF basic event related to the particular component.

The computer code CCF, which has been developed as part of this activity uses the impact vector method of Reference 2 and the approach introduced in Reference 3 for assessing the event impact vector based on physical characteristics of the event. These include component degradation parameter, time delay factor, and coupling factor strength. In addition, the software allows the user to modify the generic event impact factors for plant-specific applications, including mapping the impact vectors to account for system size difference between the plant in which the event occurred and the plant the data are being modified for. Other features of the software include estimation of the parameters of the parametric models including the scaled basic parameter model, the alpha factor model, and the multiple Greek letter model.

Figure 9 through Figure 13 are examples of some of the screens from the CCF software. This screen shows the final event statistics after event screening analysis for a particular component. Figure 9 is the initial screen. The main menu is shown is Figure 10. Figure 11 shows the results of an impact vector evaluation for a specific event. Figure 12 contains the summary statistics used in the parametric models. Figure 13 contains the common cause failure parameters for the scaled basic parameter model for a specific application with a redundancy level of 3.

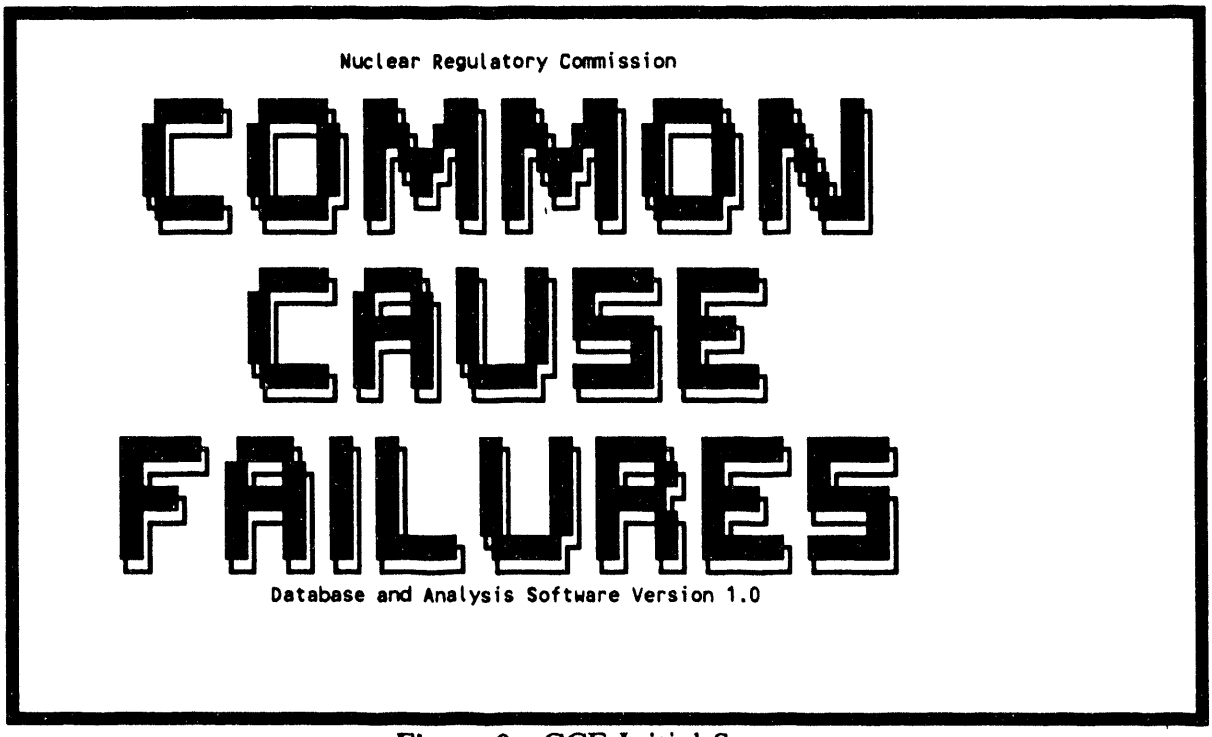


Figure 9. CCF Initial Screen.

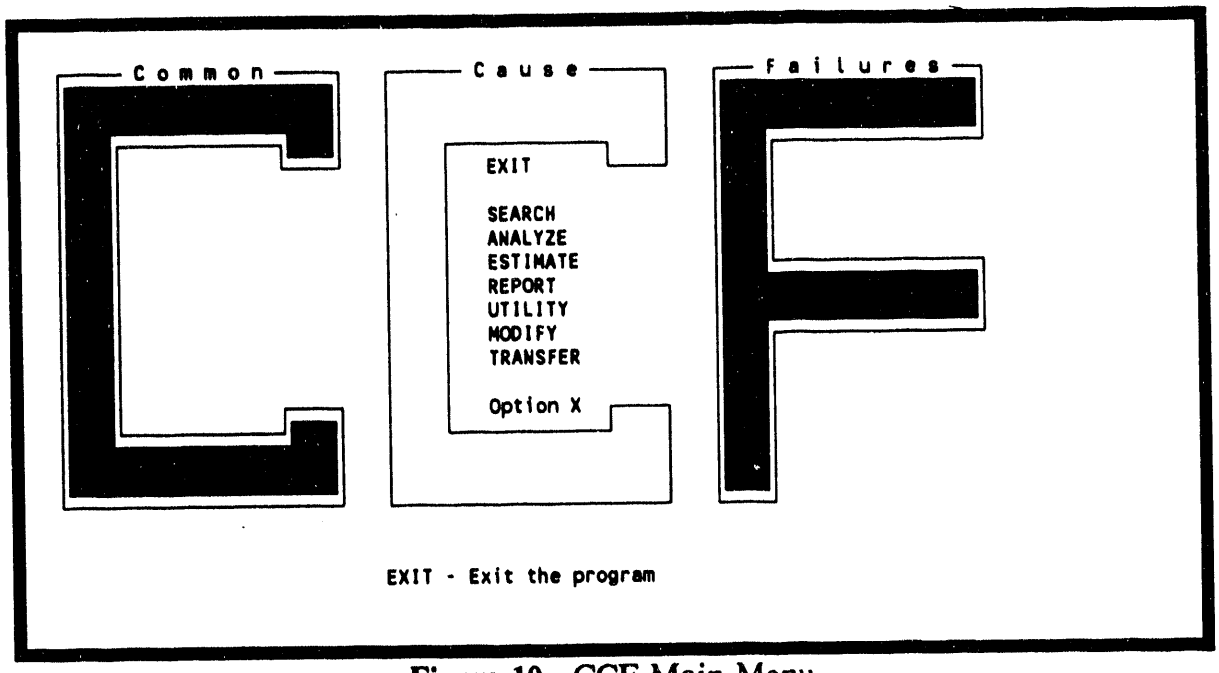


Figure 10. CCF Main Menu.

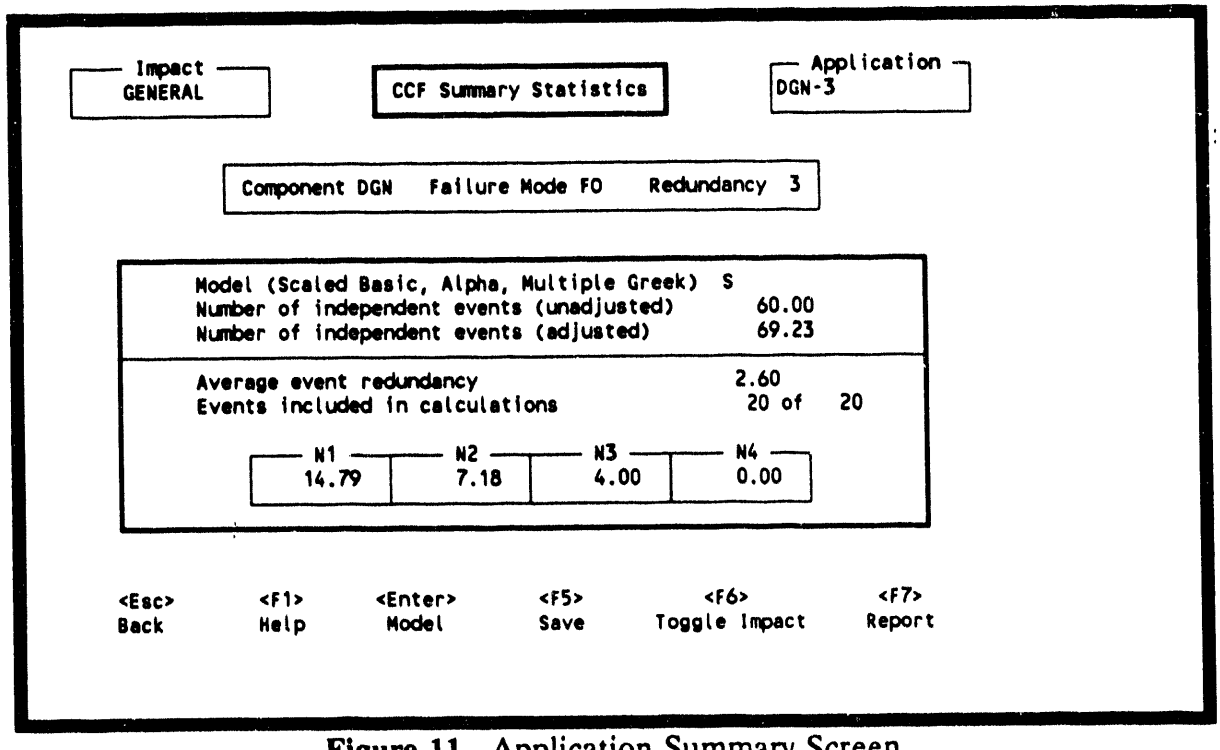


Figure 11. Application Summary Screen.

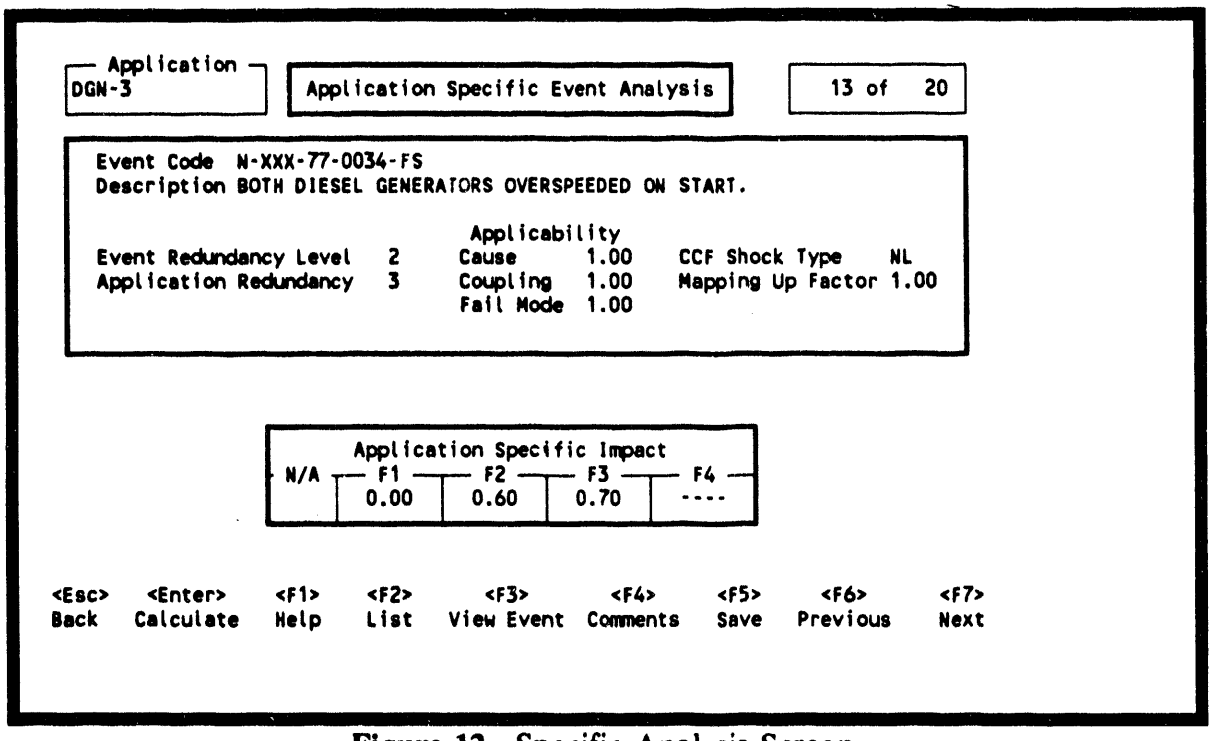


Figure 12. Specific Analysis Screen.

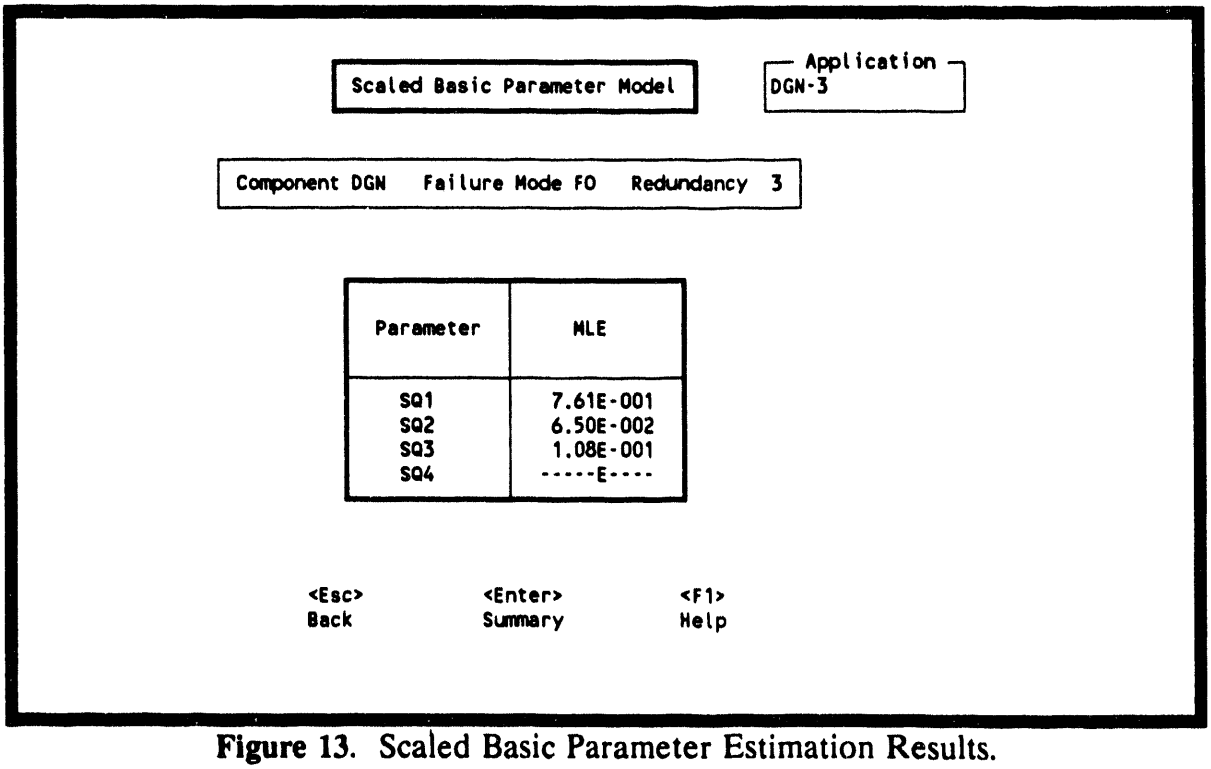


Figure 13. Scaled Basic Parameter Estimation Results.

8. OTHER STUDIES AND EFFORTS

Other activities of interest include development of Reactor Protection System logic models, evaluation of component failure probabilities and initiating event frequencies from the IPEs, an update of initiating event frequencies, an a detailed analysis of the Emergency AC Power System. AEOD is developing detailed plans of the efforts required to characterize U. S. industry risk trends based on aggregating results from our trending studies, available PRA results, IPE results, and ASP results. In addition, onsite data collection at a selected group of plants is planned to occur each year. This will help AEOD check the validity of trends and obtain additional insights for focusing future efforts.

9. REFERENCES

1. K. N. Fleming and A. Mosleh, *Classification and Analysis of Reactor Operating Experience Involving Dependent Events*, EPRI NP-3967 (June 1985).

2. A. Mosleh, et al, *Procedures for Treating Common Cause Failures in Safety and Reliability Studies*, NUREG/CR-4780, Volume 1(January 1988) and Volume 2 (January 1989).

3. A. Mosleh, *Procedure for Analysis of Common-Cause Failures in Probabilistic Safety Analysis*, NUREG/CR-5801 (April 1993).

THE CAPABILITIES AND APPLICATIONS OF THE SAPHIRE 5.0 SAFETY ASSESSMENT SOFTWARE[a]

Kenneth D. Russell, S. Ted Wood, and Kellie J. Kvarfordt
Idaho National Engineering Laboratory
P.O. Box 1625
Idaho Falls, Idaho 83415

ABSTRACT

The System Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) refers to a suite of computer programs that were developed to create and analyze a probabilistic risk assessment (PRA) of a nuclear power plant. The programs in this suite include: Models and Results Data Base (MAR-D) software, Integrated Reliability and Risk Analysis System (IRRAS) software, System Analysis and Risk Assessment (SARA) software, and Fault tree, Event tree, and Piping and instrumentation diagram (FEP) graphical editor. Each of these programs performs a specific function in taking a PRA from the conceptual state all the way to publication.

This paper provides an overview of the features and capabilities provided in version 5.0 of this software system. Some major new features include the ability to store unlimited cut sets, the ability to perform location transformations, the ability to perform seismic analysis, the ability to perform automated rule based recovery analysis and end state cut set partitioning, the ability to perform end state analysis, a new alphanumeric fault tree editor, and a new alphanumeric event tree editor. Many enhancements and improvements to the user interface as well as a significant reduction in the time required to perform an analysis are included in version 5.0. These new features and capabilities provide a powerful set of PC based PRA analysis tools.

INTRODUCTION

The U. S. Nuclear Regulatory Commission has developed a powerful suite of personal computer programs for the performance of probabilistic risk assessments (PRAs). This suite of programs, known as the System Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE), allows an analyst to perform many of the functions necessary to create, quantify, and evaluate the risk associated with a facility or process being analyzed. These programs include software to define the data base structure, to create, analyze, and quantify the data, and to display results and perform sensitivity analyses. The programs in this suite include: Models And Results Data Base (MAR-D) software, Integrated

a. Work supported by the U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, under DOE Idaho Operations Office Contract DE-AC07-76ID01570.

Reliability and Risk Analysis System (IRRAS) software, System Analysis and Risk Assessment (SARA) software, and Fault tree, Event tree, and P&ID (FEP) graphical editor software. Each of these programs performs a specific function in taking a PRA from the conceptual state all the way to publication.

Throughout the development of these software packages, various versions of each program were released. Because the programs functioned as an integrated package, and much confusion resulted from unknown compatibility of packages with different version numbers, it was determined in 1992 to combine these separate software packages under one umbrella known as SAPHIRE. The first version of this integrated system was released in 1992 and was identified as SAPHIRE 4.0. This version of the SAPHIRE system has proven to be a very powerful set of tools for the performance of risk assessments. Many new enhancements have been made to SAPHIRE 4.0. These enhancements will be released in the near future as SAPHIRE version 5.0. This paper will provide an overview of the new features contained in SAPHIRE 5.0. This overview will present a description of the general changes and a description of the more specific changes by functional area.

GENERAL FEATURES

SAPHIRE 5.0 has many new features that are of a general nature. These features affect many different areas of the software and may not be readily noticeable.

Unlimited Cut Set Storage

Previous versions of SAPHIRE had a limit on the number of cut sets that could be stored in the data base. These versions of SAPHIRE generated all the cut sets for a large problem and then only stored a subset of the cut sets in the data base. However, this subset was not the most probable cut sets of the total. Version 4.16 and later stored the most probable cut sets. With version 5.0, all the cut sets generated by SAPHIRE can be stored in the data base and can be requantified, listed, reported on, etc. The only limit in this area is the amount of free disk space available for storage of cut sets.

New Cut Set Editor

In SAPHIRE 5.0, the cut set editor has been completely rewritten. This new editor adds many new and powerful features and simplifies the user interface. Figure 1 shows the main screen of the new cut set editor. From this screen the user can modify any of the fields displayed by simply typing over the information on the screen. In previous versions, the user was required to enter a command such as "Modify" or "Add" before changing a field.

The <F1> function key provides a complete list of events to select from, as shown in Figure 2. Events that do not currently appear in the cut sets are marked with a "-". When dealing with large cut sets containing many events, this can be quite helpful. The event list is easily searched using a "quick search" method. Simply begin typing the name of the event you're looking for, and as each letter is entered, the first event in the list that matches your entry will be highlighted. When you have located an event, press the <Enter> key to add it

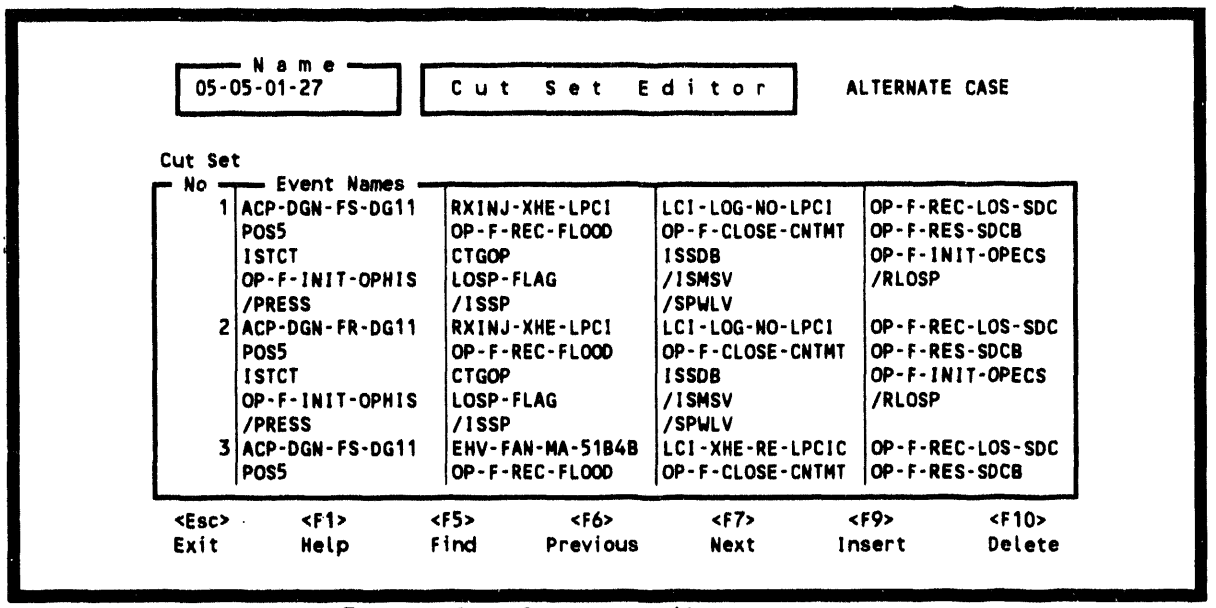


Figure 1. Cut set editor screen.

to the cut set. This feature serves as a memory aid and reduces the possibility of typing errors. The amount of typing is also reduced, as it may take only three or four letters to identify the event you are looking for. From this list, you may also press <F8> or <F9> to edit or add an event to the data base.

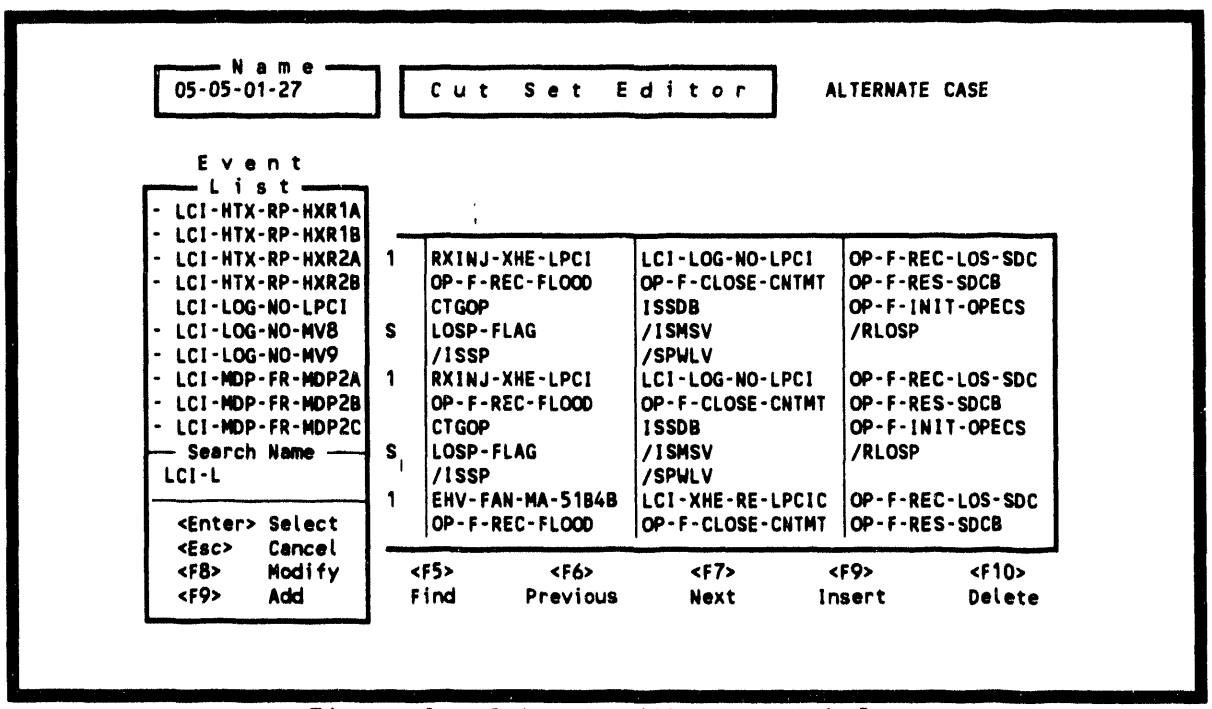


Figure 2. Cut set editor event help.

The <F5> function key allows the user to search for cut sets containing one or more specified events, using "And" or "Or" logic. The user may mark the desired items or perform a wild card search, then "Find," "Delete," or "Copy" each qualifying cut set, "Insert" additional events, or "Replace" events within a cut set (Figure 3). Depending on user preference, the editor will perform the changes at once, or highlight each match and prompt the user to either perform the change, skip it, continue, or end. Figure 4 shows an example of the prompted "Insert" option.

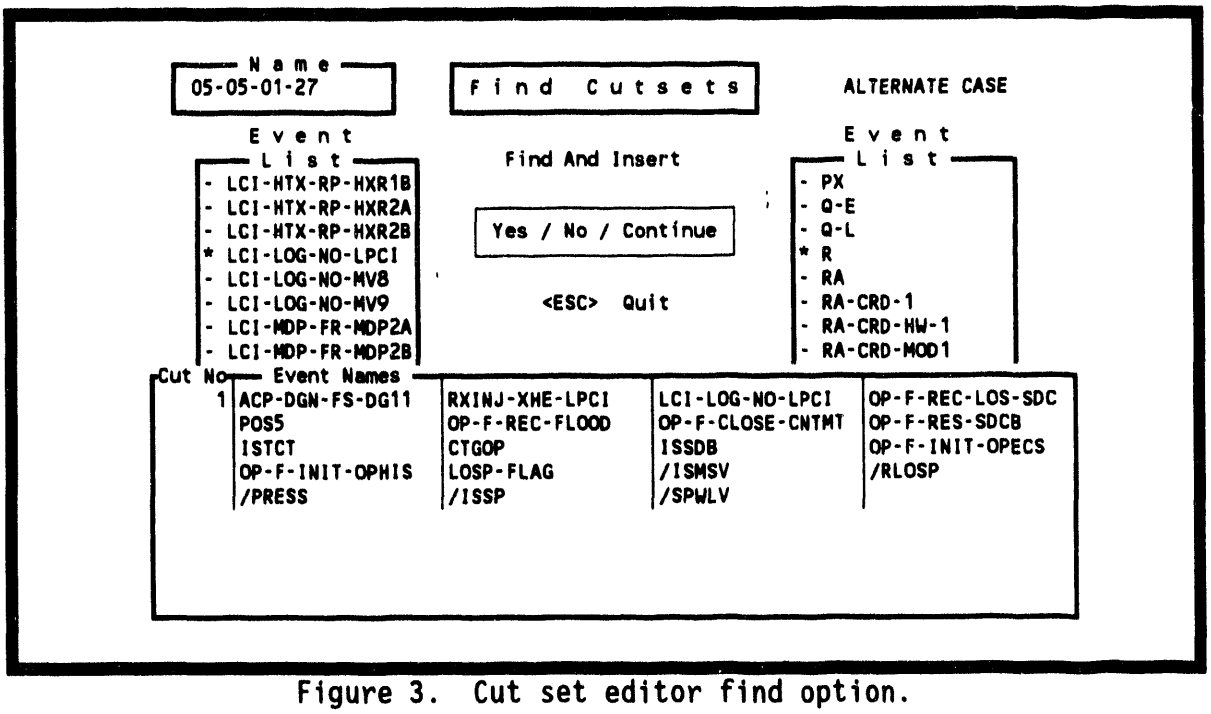


Figure 3. Cut set editor find option.

Automated Recovery Analysis

New to SAPHIRE version 5.0 is the ability to perform automated, rule based recovery on sequence and system cut sets. This allows the user to address the potential effects of recovery actions separately from the actual sequence or system logic. Figure 5 shows the options available in the Recovery Analysis module. Rules can be defined for a particular system or sequence, an event tree, or the entire family, depending on the scope of the recovery action. Once these rules have been defined, they can be applied to the relevant cut sets, and reapplied every time the cut sets are regenerated or modified.

Rules are defined using a powerful new free form editor that allows complex rules to be stated clearly and concisely. Figure 6 shows an example of a rule defined in this editor. A rule consists of a set of conditions that a cut set must meet in order to qualify to have one or more recovery events added to it. When the <Ctrl-R> option is invoked on Figure 6, recovery events can be added to the data base on the spot as shown in Figure 7.

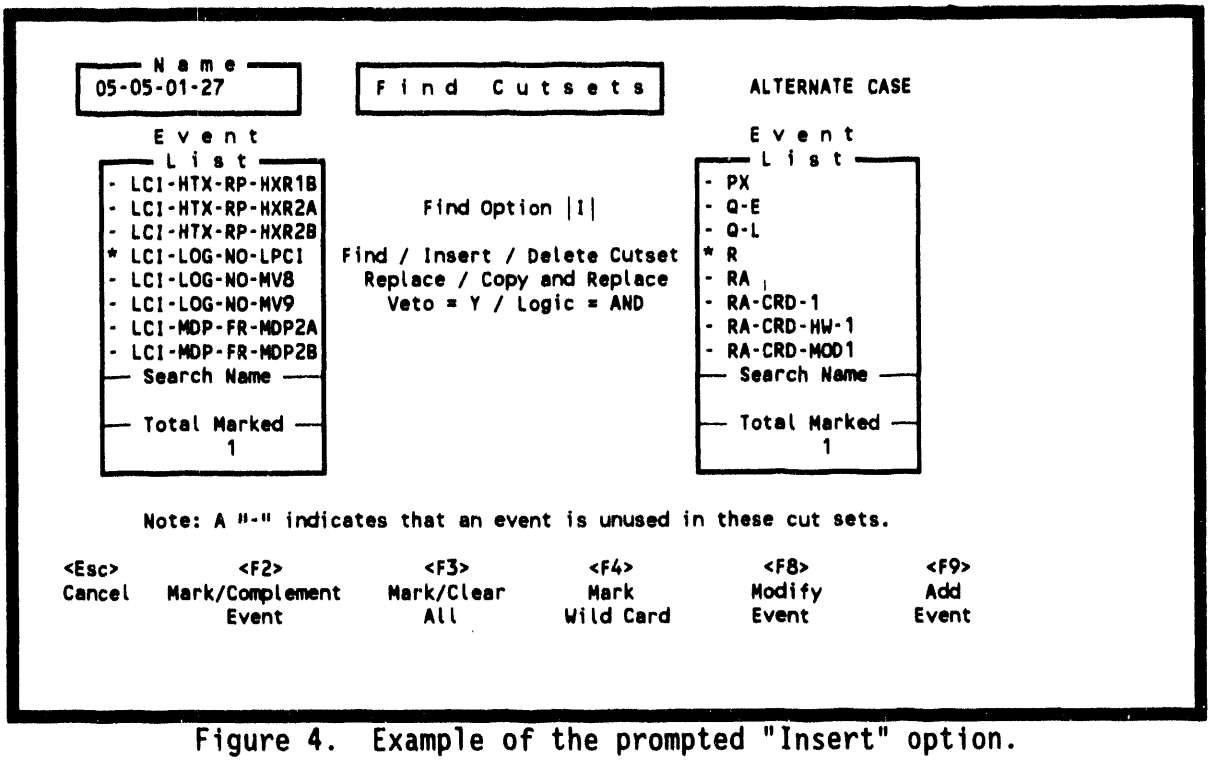


Figure 4. Example of the prompted "Insert" option.

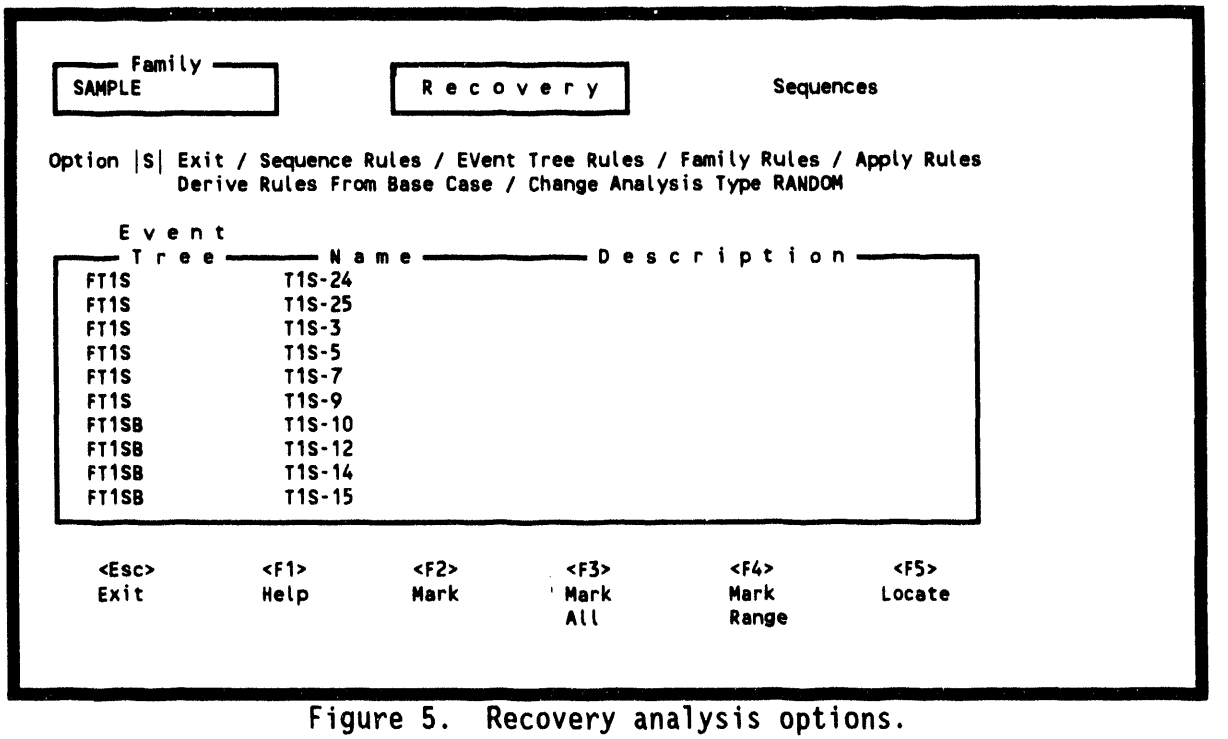


Figure 5. Recovery analysis options.

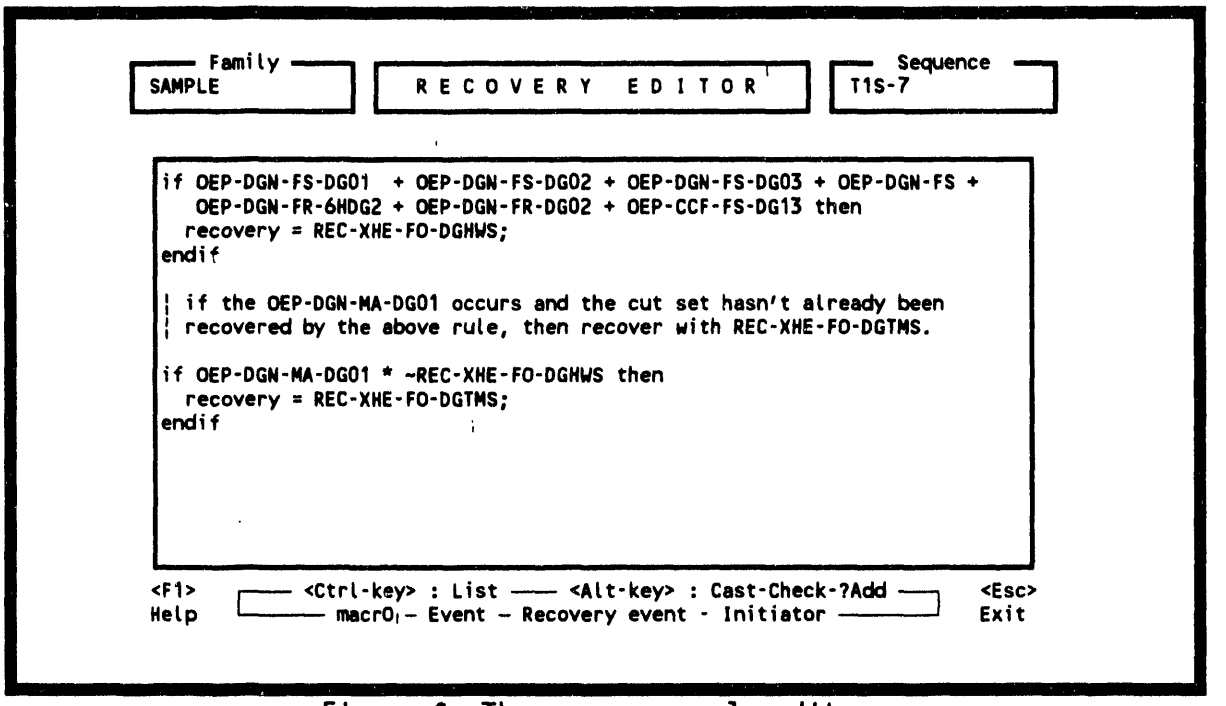


Figure 6. The recovery rule editor.

Once the rules have been applied to the cut sets by invoking the "Sequence Rules" option on Figure 5, the effects of the recovery can be viewed (see Figure 8). This will display the requantified cut sets, along with an asterisk indicating the cut sets that have had recovery events added to them.

If, using previous versions of SAPHIRE, a user has manually edited cut sets to perform recovery analysis, the "Derive" option can be used to create a set of rules that can reproduce those recovery actions. These rules will likely be verbose and rather inflexible, but may do until a more optimal set of rules can be defined.

User Error/Message File

Many comments have been received indicating that the user would like to have a message file where they could go to get additional information on what occurred during batch processing of a set of systems or sequences. This file has been provided in version 5.0. The SAPHIRE system automatically echoes any informational processing messages to a file for the user. This file can be scanned to determine the results of a batch process where the user is processing many sequences or systems and may not see all the messages that appear. The user can also look at a file called "SCREEN.CPY" for the results of cut set generation, quantification and uncertainty analysis.

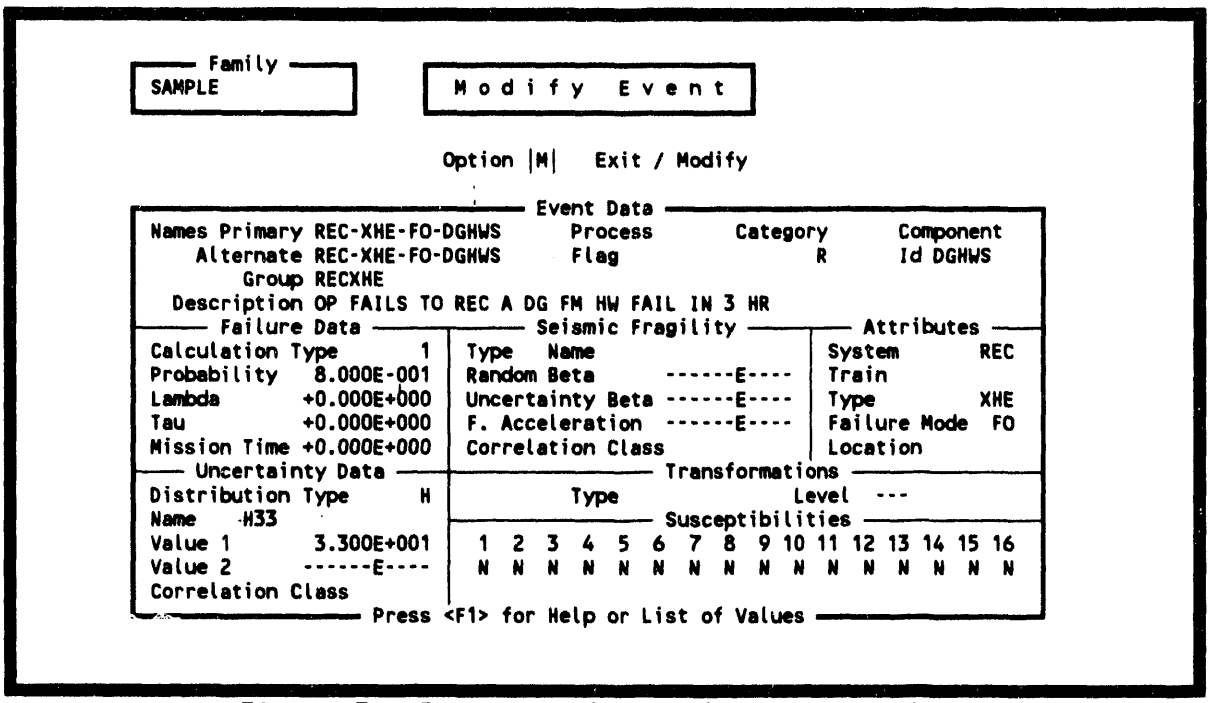


Figure 7. Recovery editor edit event option.

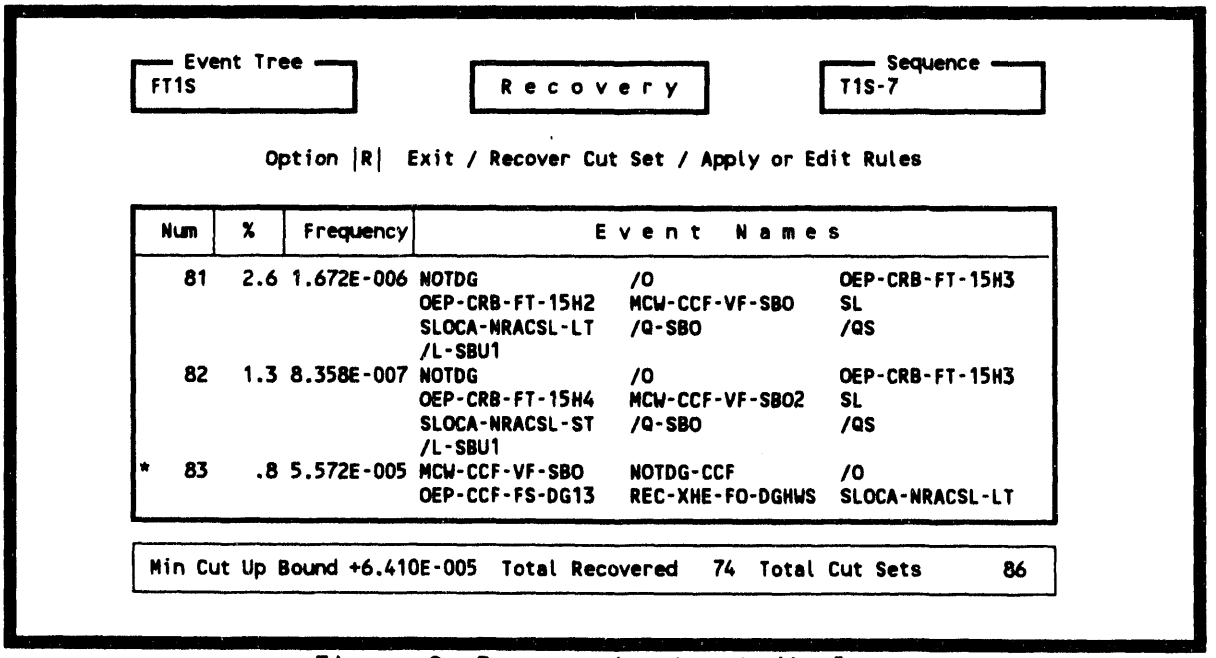


Figure 8. Recovered cut set display.

MAR-D Output Formats and Interface

The MAR-D data interchange program user interface has been completely rewritten. This program now allows the user a greater flexibility in deciding how information is to be output. The user can select data to output and usually select whether the data are to be written to a single file or to multiple files.

MAR-D output formats have been added for all new information included in SAPHIRE 5.0. This includes histograms, end states, basic events, systems, sequence, and gates. These ASCII formatted files can be used to interface with other programs or software packages not directly supported by SAPHIRE. These files can also be used to edit the information in SAPHIRE with a text editor to make bulk modifications not provided by SAPHIRE.

Archive Routines

An automated archive feature has been added to SAPHIRE to allow the user to automatically compress and archive data on the hard disk. These routines can optionally use the industry standard PKZIP utility to compress and uncompress data accessed by the analyst. This data can also be backed up to floppy disks and restored to the hard disk with this utility.

New Reports

Many new reports have been added to SAPHIRE 5.0 to allow the analyst to get a better view of the information stored in a SAPHIRE data base. These reports include summary information as well as detailed cross reference data. All reports are menu driven and modifiable to meet the user's needs.

Windows Version of Graphical Fault Editor

A new Windows 3.1 based version of the graphical fault tree editor has been developed. This editor is a Windows 3.1 compatible program. It allows the user to access the Common User Interface (CUI) features of Windows. It also allows the user to access the integrated fonts and printing capabilities.

386 Protected Version

SAPHIRE 5.0 includes a 386 protected mode version. This version requires a PC with a minimum of a 386 processor and at least four megabytes of random access memory. The advantage of the 386 version is that it takes up less hard disk space for the executable and can use all the extra random access memory on a computer. The result is a program that runs faster and has fewer hardware limitations. If you have extremely large models or require extra speed, then the 386 version is for you. It is likely that in the future all versions of SAPHIRE will require a 386 processor due to the increased power and simplicity of programming with many megabytes of memory rather than the paltry 640k bytes available to a DOS program.

Miscellaneous User Interface Features

The SAPHIRE system is becoming a very large and comprehensive set of tools for performing PRA analyses. The very size and power of the SAPHIRE tools tend to produce a complex system. To address this issue in SAPHIRE 5.0, much attention has been given to simplifying the user interface. Some things that could be done to make the program easier to use are difficult to implement given the memory constraints of the DOS versions of SAPHIRE; however, many new features have been added to help the analyst accomplish their work quicker and easier.

An example is the ability to access associated data from various points in the program. For instance, in the new fault tree editor the user can add or modify gate and basic event information directly from the editor. Previously, the user was required to exit the editor and invoke the "Modify Database" option to change this information. The ability to modify the data associated with an event at the time it is created makes for fewer errors and a more natural approach to model development.

Another example is the way commands are entered on a menu. Previously the user was required to enter a command and then highlight an item to process. If the user forgot to enter the command before they highlighted the item, then they would have to enter the command then rehighlight the selected item. This was very annoying to say the least. In SAPHIRE 5.0, when the user enters a command, the currently select item remains highlighted.

These are a few of the subtle new features that greatly simplify the process of performing an analysis using SAPHIRE 5.0. Many others that have been implemented may not even be noticed by the user, but will result in greater productivity. These new features contribute to make a complex process simpler.

System Analysis

The primary modification in the systems analysis area is the development of a new alphanumeric fault tree logic editor. This editor has been completely rewritten incorporating many suggested enhancements and user interface techniques.

New Alphanumeric Fault Tree Logic Editor

From the first version of SAPHIRE, both a graphical and an alphanumeric format editor for entering fault tree models have been supported. It was recognized that each method had advantages and that both needed to be supported. In the past, a great emphasis has been directed toward improvements in the graphical fault tree editor. This has resulted in a comprehensive graphical editor with substantial capabilities. The alphanumeric editor, however, has remained essentially unchanged. With SAPHIRE 5.0, the alphanumeric fault tree editor has been completely rewritten. This new version incorporates many new features and suggested enhancements from the users.

Figure 9 shows the main menu of the new fault tree editor. Upon entering this menu, the currently loaded fault tree is displayed on the screen. The user

can change any item on the screen by spacing or typing over the information directly. The various types of information are color coded for easy differentiation. Context-sensitive help is available for any field on the editor by pressing the <F1> function key. For instance, if the user is highlighting the CCS gate and presses the <F1> key, then a list of all the gates in the data base is displayed (see Figure 10). If the user is highlighting a gate type, then the list of available gate types is displayed.

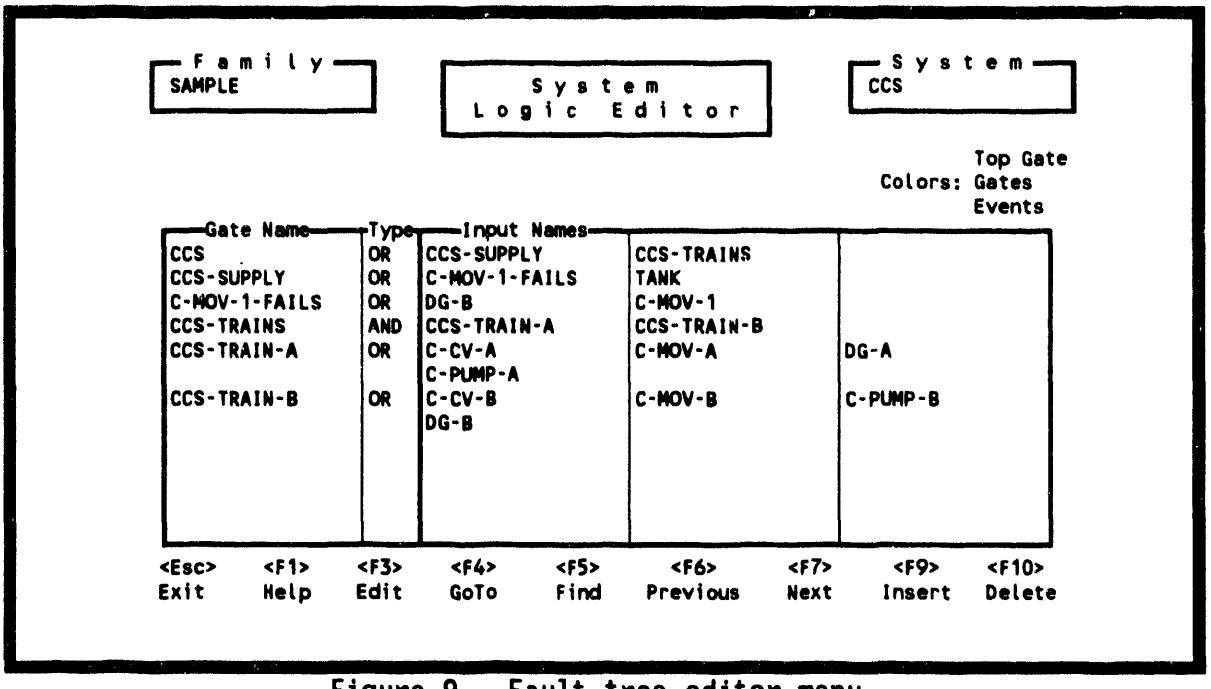


Figure 9. Fault tree editor menu.

The user can modify the information in the data base associated with a gate or basic event by highlighting the gate or event and pressing the <F3> function key. Figure 11 shows the result of highlighting the TANK basic event and pressing the <F3> key. The user can also modify the gate information in the same manner.

The <F4> function key allows the user to transfer between gate references and definitions. If the user highlights a gate reference on the Input Names side of the display and presses the <F4> function key, then the editor will transfer to the place on the Gate Name side where the gate is defined. If the key is pressed again, the editor transfers back to the reference position. If the user highlights the gate type of a transfer gate, then the editor loads the logic associated with the transfer gate and displays the logic. The user may then edit this logic. When the user exits, the editor transfers back to the previous logic.

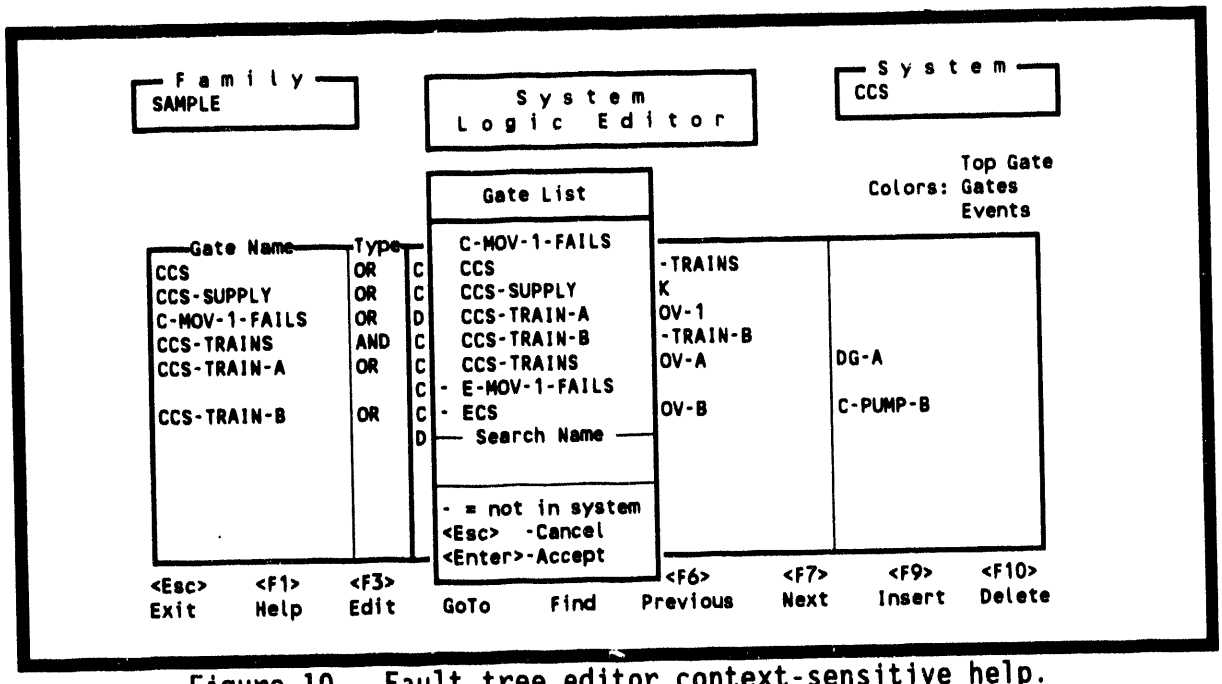


Figure 10. Fault tree editor context-sensitive help.

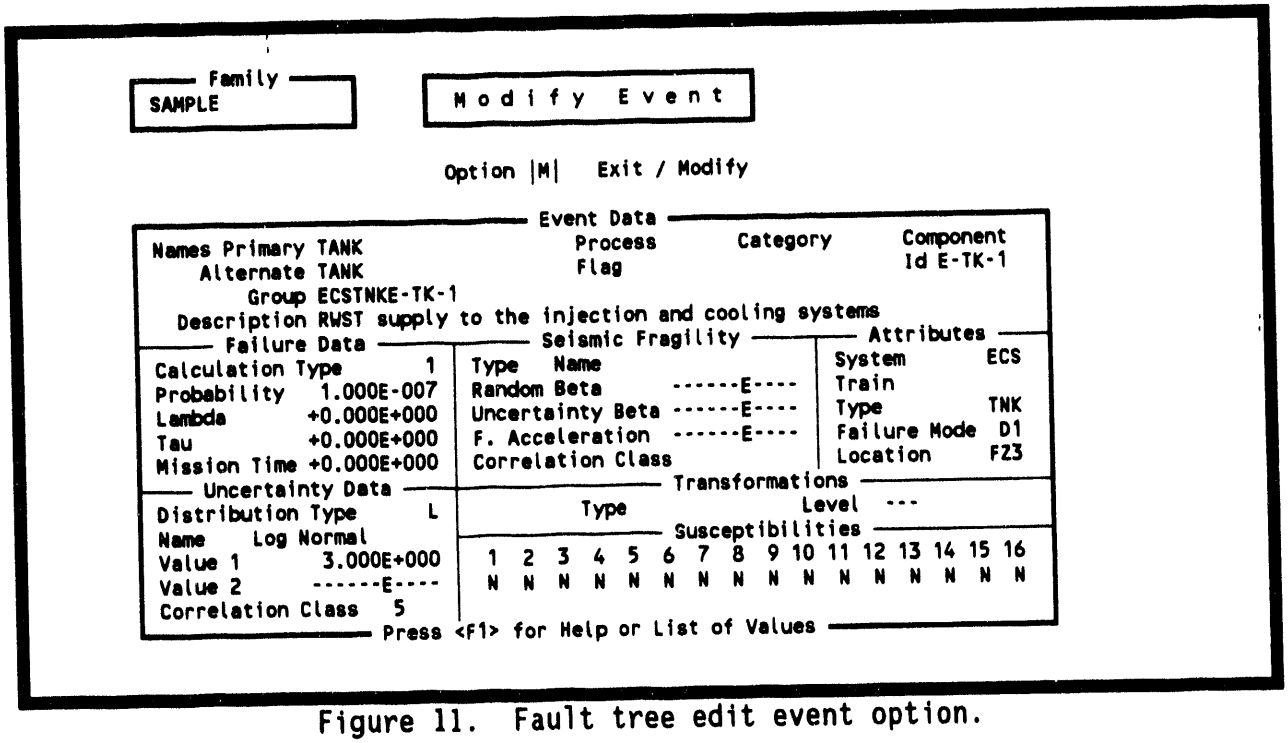


Figure 11. Fault tree edit event option.

The <F5> function key allows the user to search the logic for certain gates and events. When the user presses the <F5> key the menu shown in Figure 12 is displayed. This menu allows the user to select from a list of events, gates, and types of gates to locate. The user may mark the desired items, then choose to "Find" the gates, "Replace" the inputs, or "Add" inputs to gates that qualify. This menu also provides an option to allow the user to perform a wild card search on event and gate names. Once the search is complete, the editor highlights the first qualifying entry and optionally prompts the user to continue or end. This feature provides a powerful mechanism to apply bulk changes to many gates at once.

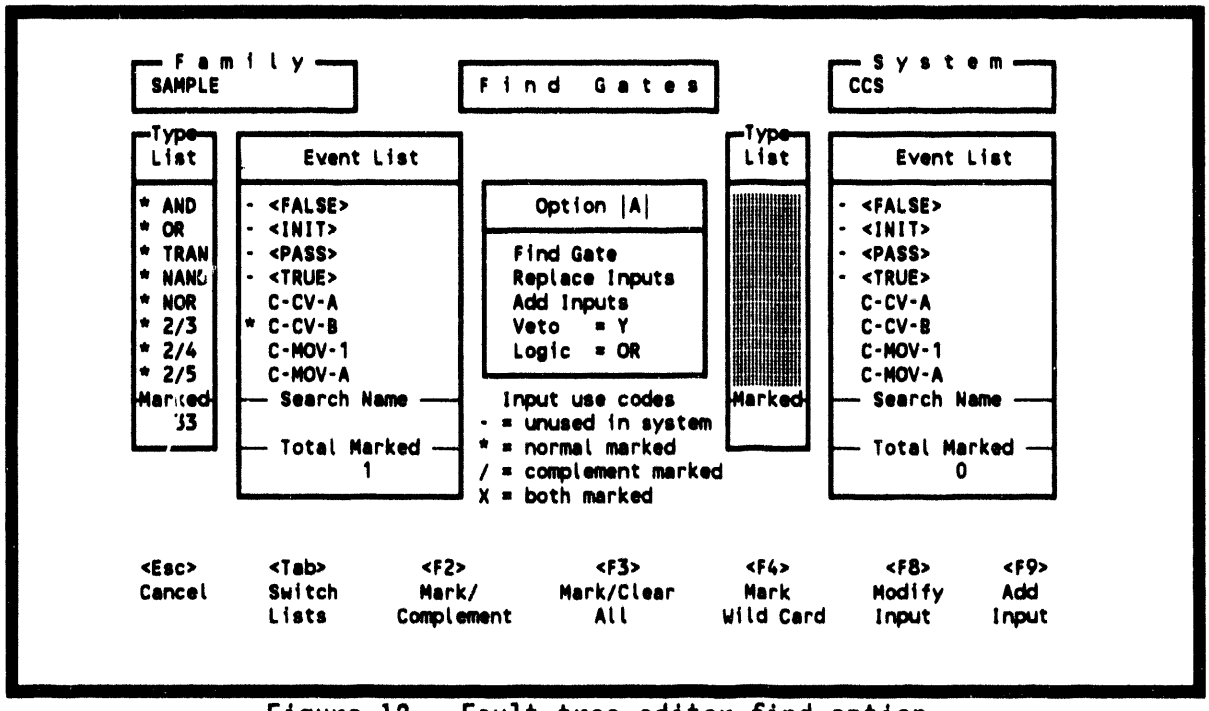


Figure 12. Fault tree editor find option.

The new fault tree editor is a powerful addition to the SAPHIRE system and provides the user an alternative to the graphical editor for modifications to fault tree logic.

Event Tree Analysis

Many modifications have been made to the event tree analysis modules. These include a new macro based event tree rule editor, new sequence logic generation options, faster cut set generation, and the addition of seismic analysis capabilities.

New Macro-based Event Tree Rule Editor

The event tree rule editor has been completely redesigned to provide better support for larger, more complex event tree substitution rules. This new rule editor is a free format line editor that provides the user with an if-then-else

logic structure. An example of a set of rules in the rule editor is shown in Figure 13. The first two lines of the display demonstrate the ability the user has to add a comment to a set of rules. The user can use the vertical bar character to signal a comment. All information following a vertical bar to the end of the current line is ignored. This allows the user to add a comment to the end of a line of data.

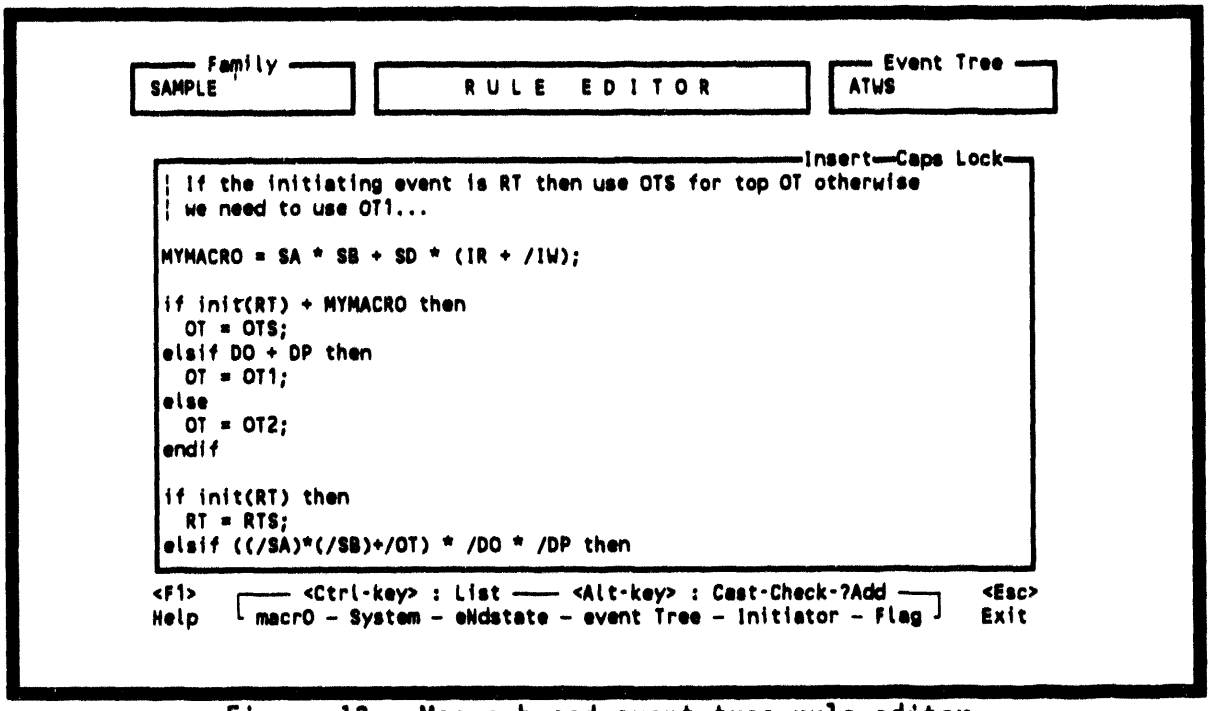


Figure 13. Macro based event tree rule editor.

The third line of data is a macro. Macros allow the user to define a complex set of instructions more concisely for repeated use later in a set of instructions. The macro defined in this example, MYMACRO, returns a true or false value depending on the result of the evaluation of the expression on the right of the "=" sign. The user can use several operators in the expression. The "*" character is an AND operator. The "+" character is the OR operator. The "/" character is the NOT operator. The displayed macro reads as follows: If SA fails and SB fails or SD fails and (IR fails or NOT IW fails) then TRUE else FALSE. The "NOT IW fails" part of the instruction converts to IW successful.

The fourth line of this sample set of rules is where the actual substitution logic begins. As shown, the new editor allows the user to specify a set of logic containing if-then-else structures to define top substitutions. In the displayed example, the rules define a substitution for top OT. If the initiating event is RT or the macro MYMACRO is true then the fault tree OTS is used for top OT. If the top DO has failed or if the top DP has failed, then fault tree OT1 is used for top OT. If neither of the previous two conditions occur, then the default fault tree OT2 is used for top OT.

By default, the type of entity in the editor is assumed to be a system. If the user desires, the type of entity can be changed by enclosing the entity with a type cast function. For instance, the init() function converts an entity to an initiating event reference. The user is provided with type cast functions for event trees, initiators, systems, flags, or end states. With these functions, the user can define substitutions for the end state or flag set of a sequence, or define a new transfer event tree for the sequence. This feature provides a powerful method to define substitution logic for an event tree.

Once the user has defined the desired rules, the editor compiles the information to check for syntax errors and to provide a more efficient format for evaluation. The compiled format is designed to provide rapid evaluation of top substitutions. With this format, SAPHIRE can immediately determine if a substitution is to be made for a given top and which substitution fault tree to use. For large event trees with many rules for substitutions, this new editor provides a flexible input tool and a very efficient evaluation processor. This same editor is used for the recovery analysis rules and the end state partitioning rules. This provides a powerful common interface for building and evaluating rules in SAPHIRE 5.0.

New Sequence Logic Generation Options

Previous versions of SAPHIRE were based on the Small Event Tree/ Large Fault Tree model. The sequence logic generation process in version 5.0 has been updated so that both Large Event Tree / Small Fault Tree based studies and Small Event Tree / Large Fault Tree based studies can be processed. Many new and powerful features have been added and the process has been streamlined to increase the speed of sequence logic generation. Figure 14 shows the sequence logic generation screen. The new options are numbers of levels to process, truncate on probability, and generate sequence cut sets.

Levels to Process

A level is defined as a transfer to a subtree. The default level of 99 will generate sequences whose logic will contain all tops for all the subtrees. If the level is set to less than 99, the generated sequences will only contain tops from subtrees less than the specified level. For example, an event tree A transfers to B that transfers to C that transfers to D. If the number of levels to process is set to two, the valid sequence logic will terminate before the transfer to event tree D and contain only the tops defined in trees A, B, and C. The number of sequences is also limited. At that point the cut sets for the sequences can be generated and quantified and the nondominant sequences can be removed from the event tree logic before more sequence logic is generated with a higher level. This provides the ability to limit the number of sequences processed when the tops are not independent.

Truncation on Probability

If the tops are independent, then the sequence logic can be truncated on probability. Each top is treated as a basic event with its probability assumed to be the value of its split fraction. As the sequence logic is being created

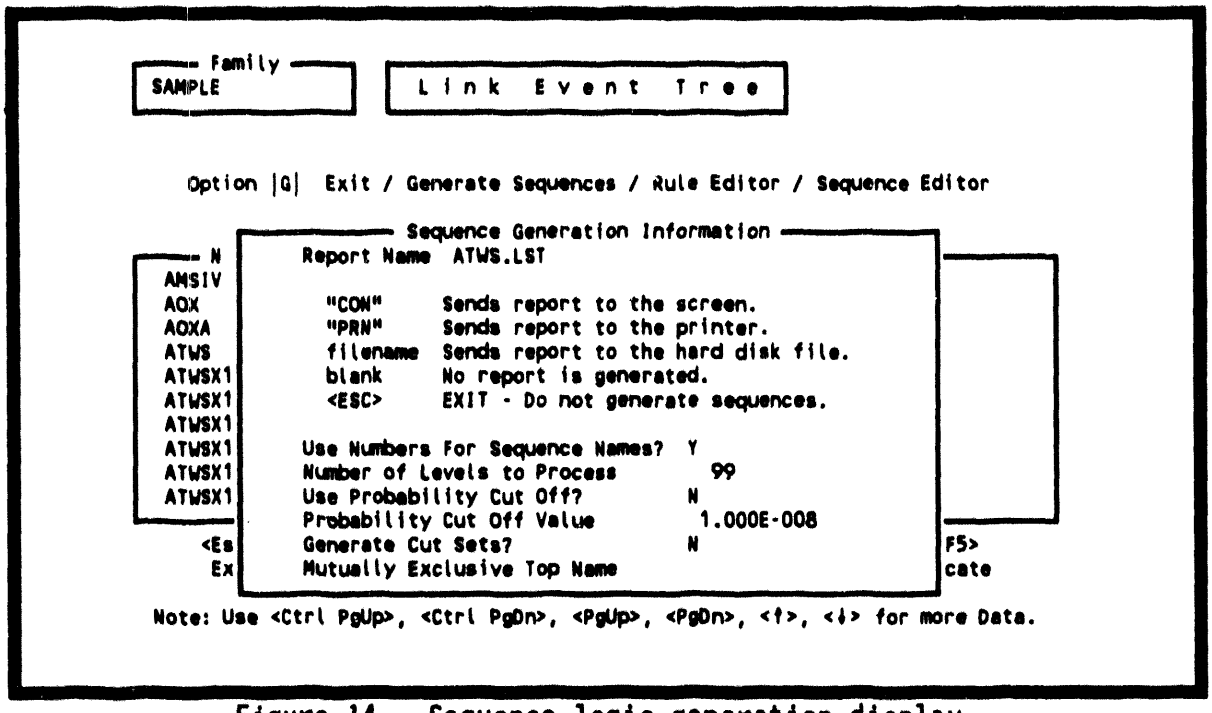


Figure 14. Sequence logic generation display.

and each top is added to the logic, the probability for the sequence is checked to ensure that its probability is greater than the truncation value. All sequences whose probability is less than the truncation probability are discarded at that point and the logic is not followed any further. This speeds up the processing because nondominant sequences can be discarded early in the process and the dominant sequences can be focused on.

Cut Set Generation

A sequence cut set can now be generated when the sequence logic is generated. Each top, whether failed or successful, is treated as a basic event and placed in the cut set for the generated sequence. Quantification, uncertainty analysis, recovery analysis, and partition analysis can be performed on these cut sets because they are no different from the cut sets created by the cut set generation process.

Faster Cut Set Generation Algorithm

The sequence cut set generation algorithm has been speeded up. This new algorithm solves many sequences in 1/5 to 1/10 of the time previously required. Previous versions of SAPHIRE solved each accident sequence as a separate tree. The logic for each system in the sequence was combined to form a large fault tree that was then solved to get the sequence cut sets. In version 5.0, all the sequences for an event tree are processed at once. This is done by finding all the systems used by all the sequences in an event tree, then creating a single tree representing this logic and solving it down to the system level. The cut sets for each system from the previous step are then combined according to the

sequence logic to get a solution for each accident sequence. This process greatly reduces the amount of work required to solve all the sequences for an event tree.

Seismic Analysis Capability

SAPHIRE 5.0 has the capability to perform seismic analyses. This user can define site hazard curves and seismic event failure data, generate seismic cut sets using special processing methods, perform uncertainty analysis on seismic cut sets, and calculate and display seismic importance measures and results. Seismic analyses require special handling of cut sets and failure data. SAPHIRE 5.0 provides an integrated environment for handling all this information in a simple integrated way.

Rule Based End State Partitioning

A major enhancement to the capabilities of SAPHIRE is the rule based cut set partitioning processor. Previous versions of SAPHIRE only allowed the user to identify an end state for each sequence. SAPHIRE 5.0 allows the user to store a different end state for each cut set in a sequence. To do this, the user defines a set of partitioning rules. These rules are developed using the same new macro based editor as is used for event tree rule creation and editing and automated recovery analysis. This editor allows the user to define a rule that maps a cut set to a specific end state. These end states can be up to 16 characters long. They can be completely defined by a rule or built up incrementally by using a wild card to define character positions to be replaced.

Once the end states are defined they can be gathered into a single bin using the end state partitioning feature described later. This new end state partitioning editor and the end state processing option provide a powerful method end state analysis tool.

End State Analysis

SAPHIRE 5.0 extended its capability into the area of end state analysis by providing the user with a much more comprehensive end state analysis tool. Version 4.0 provided the user with a minimal end state analysis capability that merely summed min cut upper bound results according to accident sequence end state fields. In version 5.0, the user can gather all the cut sets that map to the same end state together in a single place. Using the rule based end state partitioning editor described previously, the user can define an end state for each cut set. This allows the partitioning to occur on a cut set by cut set basis or at a sequence level.

Once the user has gathered the end states cut sets together, all the capabilities available for accident sequence analysis are available for end states. The user can quantify the cut sets, perform a cut set update, or do an uncertainty analysis on these end state cut sets. Also an end state display results module is available to allow the user to display cut sets, importance measures, and uncertainty information for end states. A cut set editor allows the user to edit the cut sets for an end state. The reports generation module

provides a number of reports specifically for end state information. The MARD output format has also been updated to provide access to end state information through the ASCII formatted interchange files. These features combine to provide a powerful end state analysis capability in SAPHIRE 5.0.

Data Base Enhancements

The data base for SAPHIRE has had many changes. These changes have been made necessary to incorporate the new functionality in SAPHIRE 5.0 and include changes to basic event, gate, and end state relations. Also provided in SAPHIRE 5.0 is and automated data base version upgrade option.

Basic Event Changes

The basic event relation has been enhanced to include many new fields. Many of these fields are associated with the location or vital area analysis capability in SAPHIRE. SAPHIRE now has the ability to store information for Seismic failure events. This information includes all the failure information associated with a seismic event.

SAPHIRE also allows the user to define a mission time for each basic event. This mission time overrides the global mission time on an event by event basis. With this new feature, the SAPHIRE user has total control over the mission time used for a basic event failure probability calculation.

SAPHIRE now has the capability to automatically perform event transformations during fault tree analysis. This is accomplished by allowing the user to specify a transformation for each basic event in the data base. This transformation can be one of three types, AND, OR, or ZOR and can define an optional level number. The user also specifies a list of basic events that make up the transformation. When a fault tree is solved, the user can specify that the logic for the fault tree be transformed by replacing each event that has a transformation defined for it by a gate with the events in the transformation as inputs. A simple example fault tree follows:

```
TOP       AND   GATE1, GATE2
GATE1     OR    EVENT1, EVENT2
GATE2     AND   EVENT1, EVENT3
```

The user specifies the following event transformations:

```
EVENT1    OR    LOC1, LOC2, LOC3, CABLE1
EVENT2    OR    LOC2, LOC4, CABLE2
CABLE1    OR    LOC4, LOC5
CABLE2    OR    LOC5, LOC6, LOC7
```

The CABLE events may represent the locations a cable passes through. The OR transformation type indicates that the specified event is to be replaced by an OR gate with the locations as inputs. The user then chooses to expand the transformations resulting in the following logic:

```
TOP         AND   GATE1, GATE2
GATE1       OR    TRAN1, TRAN2
GATE2       AND   TRAN1, TRAN3
TRAN1       OR    LOC1, LOC2, LOC3, CABLE1, EVENT1
TRAN2       OR    LOC2, LOC4, CABLE2, EVENT2
CABLE1      OR    LOC4, LOC5
CABLE2      OR    LOC5, LOC6, LOC7
```

This logic is then reduced by combining like gate types to the following:

```
TOP         AND   GATE1, GATE2
GATE1       OR    TRAN1, TRAN2
GATE2       AND   TRAN1, TRAN3
TRAN1       OR    LOC1, LOC2, LOC3, LOC4, LOC5, EVENT1
TRAN2       OR    LOC2, LOC4, LOC5, LOC6, LOC7, EVENT2
```

When this fault tree is solved, the result is a list of cut sets in terms of independent failure events and locations. The user can also choose to do a zone transformation by defining the locations that map to a particular zone. A zone or ZOR transformation as it is defined in the following example, effectively takes groups of locations and maps them into a single zone. Assuming the user specified the following zone transformations,

```
ZONE1 ZOR   LOC1, LOC2
ZONE2 ZOR   LOC3, LOC4, LOC5
ZONE3 ZOR   LOC6, LOC7  .
```

Then, the previous fault tree would be transformed into the following logic.

```
TOP         AND   GATE1, GATE2
GATE1       OR    TRAN1, TRAN2
GATE2       AND   TRAN1, TRAN3
TRAN1       OR    ZONE1, ZONE2, EVENT1
TRAN2       OR    ZONE1, ZONE2, ZONE3, EVENT2
```

This logic is obtained by replacing any occurrence of an input to a ZOR transformation by the name representing the transformation. Thus, the user can map logic in terms of locations to logic in terms of zones, where a zone represents a collection of locations.

The susceptibility flags for each event are used to control which transformations are to be applied for a particular analysis type. For instance, if the user wants an event transformation to apply to a Fire analysis, then they must specify that the particular event is susceptible to Fire by setting the fire susceptibility flag to "Y."

This simple example of the automated logic transformation capability in SAPHIRE 5.0 only begins to show the power of the tool. The user has the ability to specify many other options that provide a vast array of output results. This tool can be used for any type of location or vital area analysis that require automated transformations.

Fault Tree Logic Gate Changes

The data base has been modified to include a relation for storing all the information associated with a gate. Also, the fault trees stored in the data base have been modified to use the gate number in the gate relation rather than the name. This change allows the user to modify a gate name in the gate relation and have the change reflected in the logic of all fault trees that use the gate. However, the graphics trees must still be rebuilt to reflect the change in gate names. This also allows the user to get a cross reference map of the fault trees that use a particular gate.

Cut Set Storage Enhancements

The data base has been modified to allow for the mapping of each cut set in a system or sequence to a different end state. Previously the user could specify only the end state on a sequence by sequence bases. Currently the only access to this feature is through the rule-based end state partitioning option described previously.

Automated Data Base Upgrade

With the many changes to the data base for version 5.0 it would be a substantial task for the user to convert the data from version 4.0 to 5.0. This task is made easier, however, by and automated version detection and upgrade facility build into version 5.0 of SAPHIRE. This facility checks the selected data base to determine its version number. If the version number is not the same as the current operating version of the software, then the user is prompted to determine if an upgrade to version 5.0 is desired. If the user chooses to continue, then SAPHIRE automatically converts all existing data to be compatible with the software. All new fields not already present in a data record are given a default value and all other values are converted to the new format. This conversion may take a few minutes to complete, after which the data will be available for immediate access. This process effectively eliminates version upgrade problems for the user. Once converted, however, the user will be unable to use the new data with previous versions of the software.

Conclusions

SAPHIRE 5.0 continues to provide an integrated set of tools for the PRA analyst. This version promises to be even more powerful and easier to user than previous versions. It eliminates many of the problem size restrictions in previous versions while improving the performance. The addition of seismic analysis, vital area/location analysis, and the support for large event tree analyses allows SAPHIRE 5.0 to extend its capabilities into many important areas for risk assessments. The addition of the 386 protected mode version of SAPHIRE and the Windows 3.1 version of the graphical fault tree editor keeps SAPHIRE current with the state of the art in computer technology. These changes help SAPHIRE continue to lead the way in user friendly, integrated, risk assessment software.

BIBLIOGRAPHY

1. K.D. Russell et al, *Integrated Reliability and Risk Analysis System (IRRAS) Version 4.0, Volume 1 - Reference Manual*, NUREG/CR-5813, EGG-2664, January 1992.

2. K.D. Russell et al, *System Analysis and Risk Assessment (SARA) System, Version 4.0, Volume 1 - Reference Manual*, NUREG/CR-5303, EGG-2628, February 1992.

3. K.D. Russell et al, *SAPHIRE Technical Reference Manual: IRRAS/SARA Version 4.0*, NUREG/CR-5964, EGG-2692, January 1993.

Notice

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights. The views expressed in this report are not necessarily those of the U.S. Nuclear Regulatory Commission.

EXPERIMENTS ON A SCALED LOOP

J. Michael Doster and Eric Giavedoni
Nuclear Engineering Department
North Carolina State University
P.O. Box 7909
Raleigh, NC 27695-7909

ABSTRACT

The Scaled PWR Facility (SPWRF) in the Nuclear Engineering Department at North Carolina State University is being used to study the effectiveness of two phase natural circulation and reflux cooling under conditions associated with loss of forced circulation, mid-loop coolant levels and noncondensables in the primary coolant system. Of interest are the conditions under which the noncondensables can be sufficiently compressed to expose significant portions of the heat transfer area to condensation. Of additional interest is the magnitude and time duration of the primary side pressure excursion resulting from loss of heat removal capability in the steam generators. The NCSU Scaled PWR Facility is a Freon based, 1/9 scale model of a two-loop Westinghouse Pressurized Water Reactor. Both primary and secondary sides are represented including such normal balance of plant components as condensers, condensate and feed pumps, and Feedwater heaters. The first phase of this work has involved measurements of steady state heat transfer rates under reflux cooling as a function of primary and secondary side pressure in the absence of noncondensables. Other key parameters measured include hot leg liquid and vapor temperatures, vapor velocities and liquid level. These results provide benchmark data for modeling of the reflux cooling process.

INTRODUCTION

Under loss of forced circulation, coupled with the loss or reduction in primary side coolant inventory, horizontal stratified flows can develop in the hot and cold legs of Pressurized Water Reactors (PWRs). Vapor produced in the reactor vessel is transported through the hot leg to the steam generator tubes where it condenses and flows back to the reactor vessel. Within the steam generator tubes, the flow regimes may range from counter-current annular flow to single phase convection. As a result, a number of heat transfer mechanisms are possible depending on the loop configuration, total heat transfer rate and the steam flow rate within the tubes. These include (but are not limited to), two-phase natural circulation where the condensate flows co-current to the vapor stream and is transported to the cold leg such that the entire reactor coolant loop is active, and reflux cooling where the condensate flows back down the interior of the coolant tubes counter-current to the vapor stream and is returned to the reactor vessel through the hot leg[1,2,3]. While operating in the reflux cooling mode, the cold leg can effectively be inactive. Heat transfer can be further influenced by noncondensables in the vapor stream which accumulate within the upper regions of the steam generator tube bundle[4,5,6]. In addition to reducing the steam generator's effective heat transfer area, under these conditions operation under natural circulation may not be possible and reflux cooling may be the only viable heat transfer mechanism. The Scaled PWR Facility (SPWRF) in the Nuclear Engineering Department at North Carolina State University is being used to study the effectiveness of two phase natural circulation and reflux cooling under conditions associated with loss of forced circulation, mid-loop coolant levels and noncondensables in the primary coolant system. Of interest are the conditions under which the noncondensables can be sufficiently compressed to expose significant portions of the heat transfer area to condensation. Of additional interest is the magnitude and time duration of the primary side pressure excursion resulting from loss of heat removal capability in the steam generators[6,7]. The first phase of this work has involved measurements of steady state heat transfer rates under reflux cooling as a function of primary and secondary side pressure in the absence of noncondensables. Other key parameters measured include hot leg liquid and vapor temperatures, vapor velocities and liquid level. These results provide benchmark data for modeling of the reflux cooling process.

Facility Description

The NCSU Scaled PWR Facility[9] is a Freon based, 1/9 scale model of a two-loop Westinghouse Pressurized Water Reactor. Both primary and secondary sides are represented including such normal balance of plant components as condensers, condensate and feed pumps, and Feedwater heaters. The only major mechanical component which has not been included in the SPWRF is the turbine-generator. The influence of the turbine on system behavior is simulated by the main steam throttling valve. A photograph of the facility is given in Figure 1. Glass viewing windows have been placed at key locations in the facility including the pressurizer, steam dome and tube bundle regions of the steam generators, reactor vessel, hot legs and crossover legs to enhance visualization and understanding of the governing physical processes. The viewing windows in the hot legs are contained within a flanged spool piece which constitutes the majority of the total length of the hot leg. The SPWRF distinguishes itself from most large scale thermal-hydraulics loops in that full operator interaction is possible for steady-state and transient conditions including normal operation, small break loss of coolant accidents, steam generator tube rupture, and main steam line breaks.

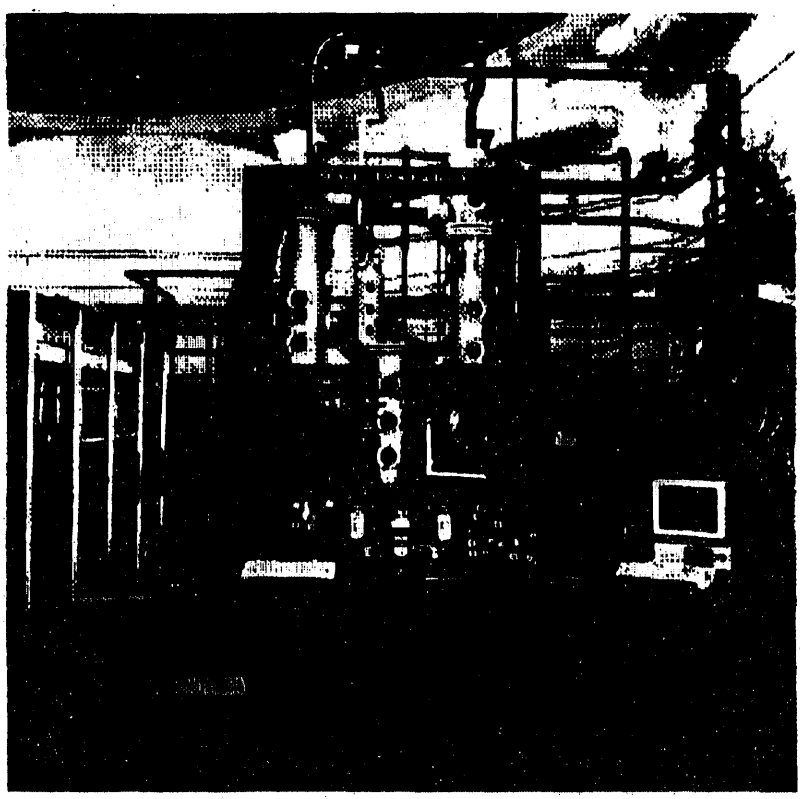


Figure 1. NCSU Scaled PWR Facility

The SPWRF provides the opportunity to study reactor system behavior beyond normal, steady-state, full power operation, where the ability to interpret plant instrumentation properly is important in mitigating core damage. The reactor core is simulated by electrically heated rods. Heater power can be governed by either a point reactor kinetics model, or set manually at an operator designated power level. The reactor kinetics model is coupled through the system's instrumentation such that reactivity feedback effects (Doppler, moderator temperature, etc.) control the reactor's dynamic response. The current instrumentation system is capable of monitoring 48 channels

of temperatures, pressures, flows, and level, as well as various valve positions and motor status signals. A brief description of the facility dimensions and nominal full power operating conditions is given in Table 1.

Core		
Nominal Full Power	80	kW
Electrical Heater Rods	106	
Rod Diameter	1.0	cm
Rod Height	0.38	m
Primary Coolant System		
Primary Loop Temperature	95	C
Primary Side Pressure	998	kPa
Reactor Vessel Height	1.2	m
Reactor Vessel Diameter	0.35	m
Secondary Side		
Steam Generator Height	2.1	m
Steam Generator Diameter	0.35	m
Steam Pressure	618	kPa
Steam Flow Rate	0.222	kg/s

Table 1. Scaled PWR Facility Dimensions and Nominal Operating Conditions

The Scaled PWR Facility utilizes two independent data acquisition and control computers such that process control functions are isolated from measurements for research purposes. Automatic control functions for such parameters as pressurizer pressure and steam generator level are handled through the process control computer. The second data acquisition system is a 25 MHz Intel 386 based personal computer supporting three 16 channel multifunction high speed analog/digital I/O expansion boards. The data acquisition computer has been configured to monitor and log (if desired) all process control variables, including pressurizer pressure, pressurizer temperature, steam generator level and pressure, loop temperatures, as well as custom instrumentation installed specifically for this research.

Facility Scaling

The original SPWRF design objectives were to construct a multi-use facility to provide high fidelity tracking of normal and operational transients. Uses envisioned included training of reactor operators and engineers, student training and education as well as research. As a result, sacrifices were made in the fidelity of time scaling associated with two-phase dominated phenomena as long as the evolution of the phenomena were essentially correct. The single phase scaling laws of Ishii and Kataoka[10] were used in sizing the facility. In addition to proper scaling of geometric parameters, additional dimensionless properties (e.g., Heat Source Number, Richardson Number, Friction Number, etc.) must be matched. These criteria specify the length and area ratios, time ratios (specified to be one for single phase flows in the primary side), nominal power level, core ΔT ratios, mass flow rate ratios, etc. Two-phase scaling requires satisfying several more dimensionless properties, which typically contain time varying two-phase properties, e.g. void fraction. It is highly unlikely therefore that time scaling will hold under these conditions. This is a concern if these results are to be scaled to those of other facilities.

Research Objectives

The SPWRF is being used to study the effectiveness of reflux cooling under conditions associated with loss of forced circulation, mid loop coolant levels and noncondensables in the primary coolant system. The approach to date has been to measure steady-state heat transfer rates, liquid and vapor temperatures and velocities as a function of primary and secondary side pressures while operating in the reflux cooling mode. It should be noted, that

steady-state is the only condition where heat transfer rates can be reliably measured on this facility. The original research objectives included using the steady-state data to develop and benchmark a model of the reflux cooling process sufficiently general to investigate scaling of results from the SPWRF to other facilities. Since it is unlikely that conditions in the SPWRF will provide two-phase similarity between the SPWRF and other facilities, a detailed physics model would likely be required.

REFLUX COOLING EXPERIMENTS ON THE SCALED PWR FACILITY

Experimental Procedure

A series of reflux cooling experiments have been run on the SPWRF to measure steady state heat transfer rates as a function of primary and secondary side pressure. The SPWRF is a two-loop facility, with the individual coolant loops designated as the A and B sides. Measurements are performed on the hot leg of the A loop. To minimize losses, the B side steam generator is drained, evacuated and isolated in each of the runs. Steam generator level was maintained such that the tube bundle region was completely flooded and the steam generator operated in its normal recirculation mode at constant level by addition of feed water. The SPWRF is brought to test pressures and temperatures using the reactor coolant pumps and core heaters. The primary side of the SPWRF is then drained to mid-loop coolant levels and stabilized prior to initiation of significant secondary side steaming. Counter-current, horizontal stratified flow in the hot leg and stagnant conditions in the crossover leg are verified visually through the glass viewing windows located in these areas. Core heater power is controlled through the reactor kinetics model. Primary side pressure is specified through simulated control rod position.

The reactor kinetics model receives reactivity inputs from three sources: (1) control rod motion, (2) moderator temperature and (3) core power. At this time no provisions have been made for the influence of voids on reactor power. Simulated control rod position is an operator input. The kinetics model includes a preprogrammed rod worth curve which gives reactivity as a function of simulated rod position. Moderator temperature coefficients and power coefficients are also built into the reactor kinetics model. Moderator temperature is assumed to be given by the average loop temperature as measured by the hot and cold leg RTDs. In these studies the average loop temperature is essentially the primary side saturation temperature and therefore directly related to the secondary side pressure. Core power is taken directly from the process control computer's power measuring channel. As a result, the SPWRF will "load follow" in a manner similar to an actual power plant. For these steady state studies, the reactor power is then controlled indirectly through the steaming rate and the corresponding steam generator pressure by manually opening and closing the main steam throttle valve. Primary side pressure and temperature are determined by simulated control rod position. For transient studies at a fixed power level, manual operation of the reactor power can be utilized.

Steam generator level is programmable through the Facility's automatic control system, or can be maintained by manual control of feed flow. At low steaming rates, system characterization studies have shown that the feed regulating valves tend to "chatter" at the settings dictated by the steam generator level controller. This results in oscillatory feed flow rates. As a result, reactor power never stabilizes when controlled by the point kinetics model. The feed flow rate was controlled manually in these studies to give a nearly constant steam generator level.

Instrumentation and Measured Parameters

For any given experiment, the following parameters are typically measured and logged by the data acquisition system.

a) Heat Transfer Rate - taken as the steady state electrical heater output from the reactor core.

b) Steam Generator Level - inferred from a differential pressure measurement between the steam generator down comer and a reference leg.

c) Feed Temperature - measured directly via an RTD located in the feed line.

d) Secondary Pressure - obtained from a pressure transducer located in the steam generator steam dome.

e) Primary Pressure - obtained from a pressure transducer located in the upper steam bubble region of the pressurizer.

f) Vapor Stream Temperature - measured via a thermocouple wand inserted in the A side hot leg, just down stream of the reactor vessel (Figure 2).

g) Liquid Stream Temperature - measured via a thermocouple wand inserted in the A side hot leg, just down stream of the steam generator (Figure 2).

h) Vapor Velocity - measured through the use of a pin wheel type, rotating anemometer placed in the hot leg (Figure 2).

i) Loop Level - is measured via a graduated scale on the A Hot Leg viewing window.

j) Liquid Velocity - inferred from the vapor velocity and the liquid level in the loop by a steady-state mass balance.

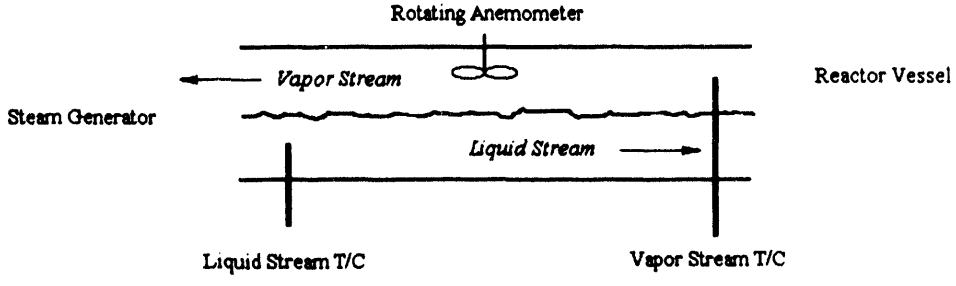


Figure 2. Diagram of Loop A Hot Leg Instrumentation

Results

Figures 3 and 4 illustrate typical measurements of primary (reactor) and secondary side (steam) pressure and reactor power. Steaming rates were changed in steps to produce approximately equal changes in secondary side pressure. The resulting change in the reactor heat input is illustrated in Figure 4. The reactor power is given as percent of nominal full power. The step changes in primary side pressure at approximately 7000 and 14,000 seconds were the result of control rod insertion. For these runs, control rod position was held constant after each insertion resulting in slight variations in primary side pressure as the steaming rate was varied. Minor adjustments in rod position at each power level can be used to reduce these variations if necessary. Steady state heat transfer rates, pressure, temperatures and velocities are obtained by averaging over a two to three hundred second time frame after the system has stabilized. Liquid and vapor stream temperatures as a function of the heat transfer rate are given in Figure 5 for a primary side pressure of 625.35 kPa (76 psig) and in Figure 6 for a primary side pressure of 652.93 kPa (80 psig). Data taken at other primary side pressures show the same trends.

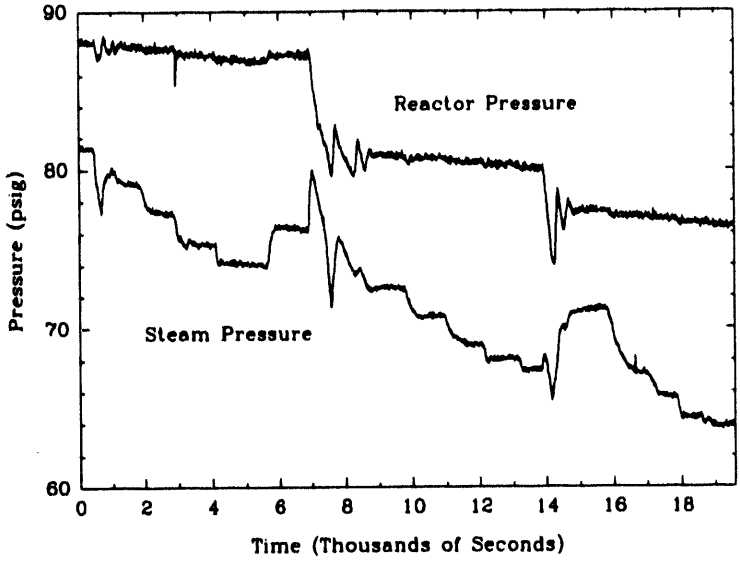


Figure 3: Primary and Secondary Side Pressure

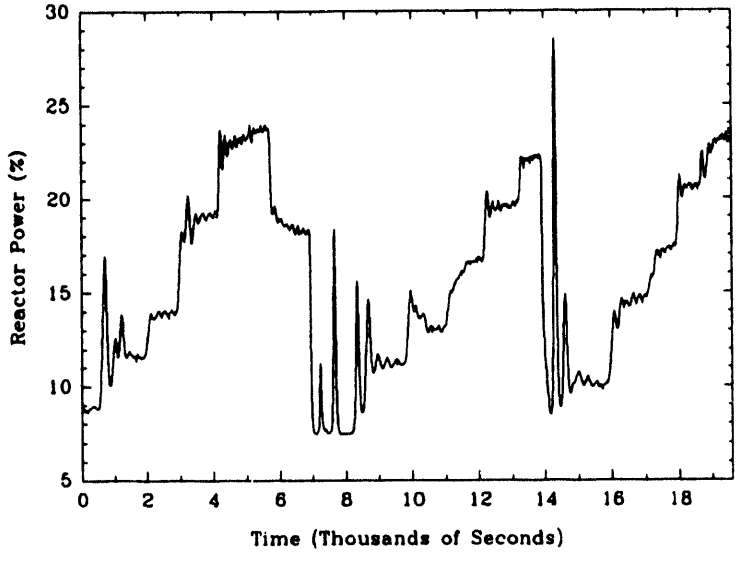


Figure 4: Reactor Power

The indicated saturation temperature is computed from the measured primary side pressure. The differences between the saturation temperature and the indicated vapor temperatures are due to the primary side pressure sensor being located in the pressurizer steam dome, some distance from the actual temperature measurement, and calibration uncertainties between the thermocouples and the pressure transducer. The data indicates convergence of the liquid and vapor temperatures to the primary side saturation temperature as heat transfer rates are increased. The vapor temperature is essentially the saturation temperature on the primary side. The slight downward trend in the vapor temperature is a result of the small changes in primary side pressure as a function of power level.

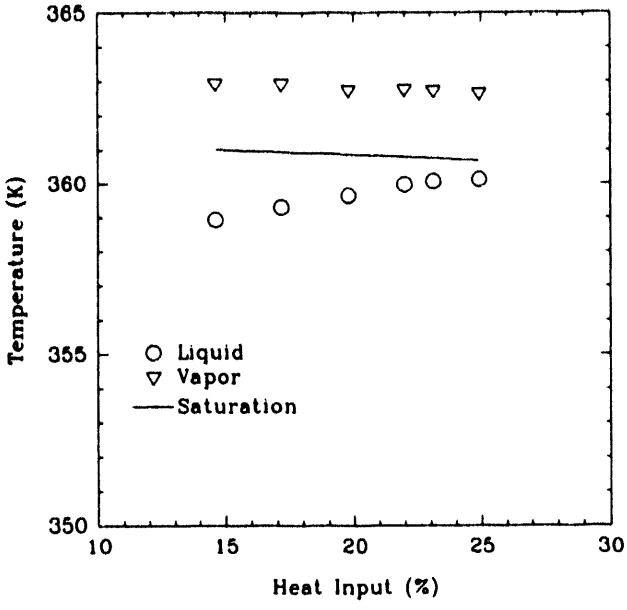


Figure 5: Liquid and Vapor Temperatures at 625.35 kPa (76 psig)

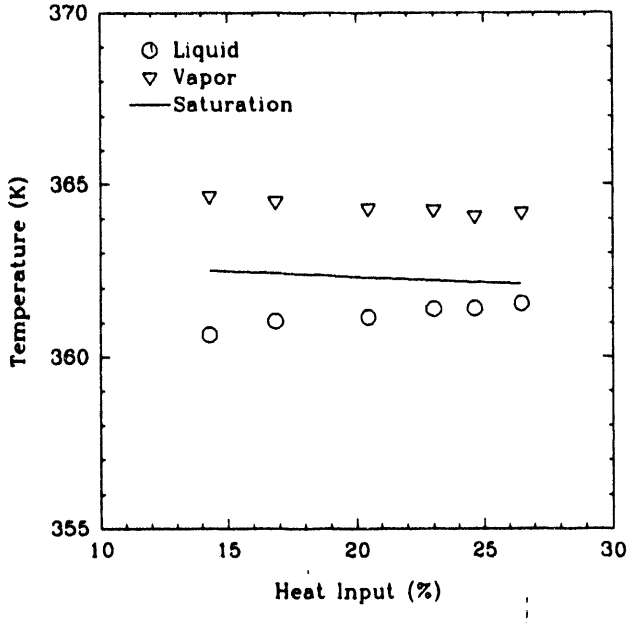


Figure 6: Liquid and Vapor Temperature at 652.93 kPa (80 psig)

A number of factors contribute to the behavior of the liquid temperature. At low heat transfer rates, the liquid and vapor flow rates are lower, the liquid film on the steam generator tube walls is thinner, there is less interfacial heat transfer between the liquid and vapor streams and a smaller primary to secondary side temperature differential is

required to drive the heat transfer across the steam generator tubes. Under these conditions, the liquid film more closely reflects the saturation conditions on the secondary side. These conditions are reversed as the heat transfer rates across the steam generators are increased.

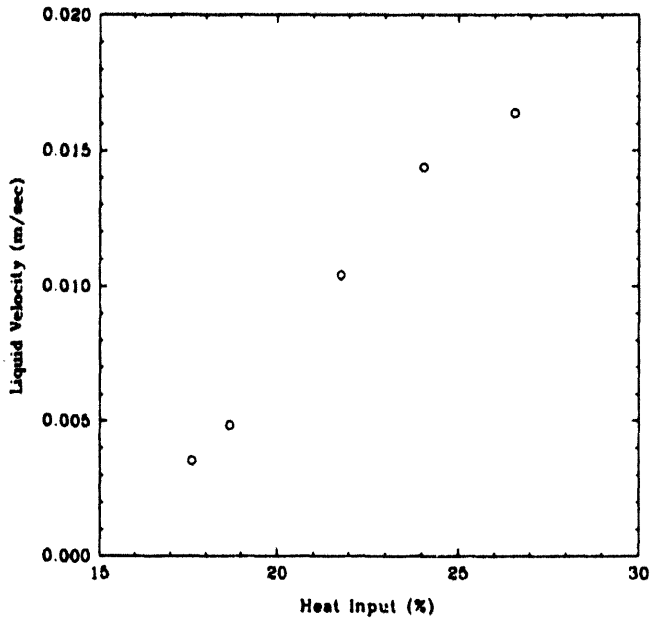


Figure 7: Liquid Velocity versus Heat Transfer Rate at 660 kPa

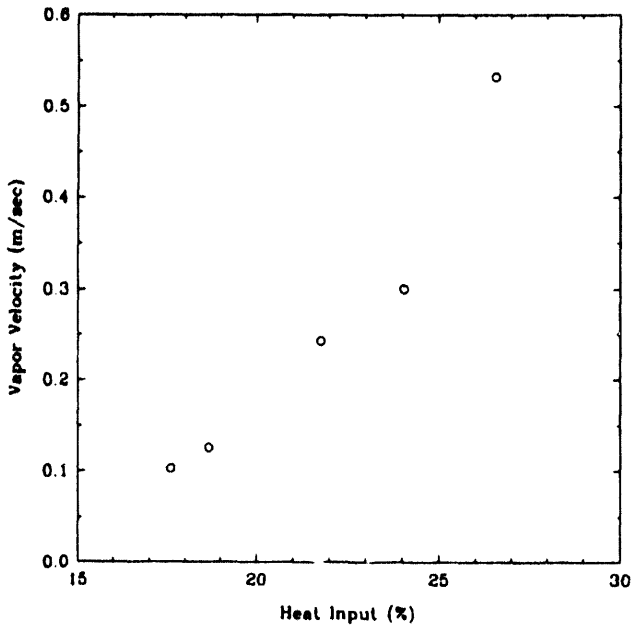


Figure 8: Vapor Velocity Versus Heat Transfer Rate at 660 kPa

Liquid and vapor velocities at 660 kPa (81 psig) are shown in Figures 7 and 8. As expected, the velocities increase with increasing heat transfer rates, though this is somewhat a function of the liquid level in the hot leg.
For the data shown here, the liquid level varied from approximately 0.32 to 0.95 cm (1/8 to 3/8 inches) below midloop. Again similar behavior is seen at other pressures. This is illustrated in Figure 9 by plotting the vapor mass flow rate as a function of primary side pressure and heat transfer rate.
Mass flow rate is the preferred variable as it automatically accounts for varying liquid levels and pressures. The increase in the mass flow rate with pressure is primarily due to the increasing density of the vapor phase.

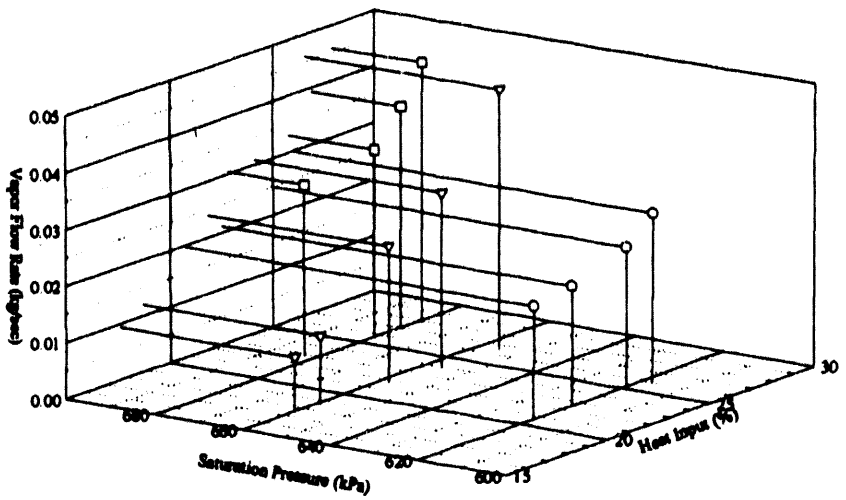


Figure 9: Vapor Mass Flow Rate versus Pressure and Heat Input

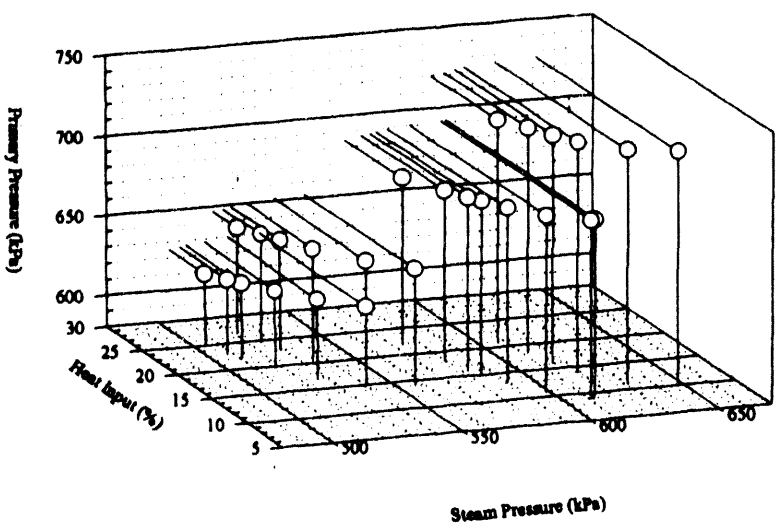


Figure 10: Primary Side Pressure versus Heat Transfer Rate and Steam Generator Pressure

Primary side pressure as a function of heat transfer rate and secondary side pressure is shown in Figure 10. The data show for a given primary side pressure, the increase in heat transfer rate with decreasing secondary side pressure. This is as would be expected. In addition, the secondary side pressure is seen to increase with increasing primary side pressure at a given heat transfer rate. In accident scenarios involving loss of heat sink while operating under midloop conditions, concerns arise over the maximum system pressure obtained prior to the establishment of reflux cooling. Heat generation rates are dictated by decay heat, and in the absence of loss of off site power, the secondary side pressure and steaming rate may be the only mechanism available for accident mitigation. This data can be used to provide insight into the steam generator operating pressure required to maintain primary side pressure below some set limit for a given heat input.

The data shown in Figure 10 may also be analyzed in terms of an Overall Heat Transfer Coefficient (UA) where we define UA as

$$UA \equiv \frac{\dot{Q}}{T_{sat}^{Primary} - T_{sat}^{Secondary}}.$$

The UA value is shown in Figure 11 as a function of primary side pressure and heat transfer rate. The heat transfer coefficient appears linear with the heat transfer rate, and other than an apparent systematic error in the low pressure results (619.15 kPa), independent of pressure.

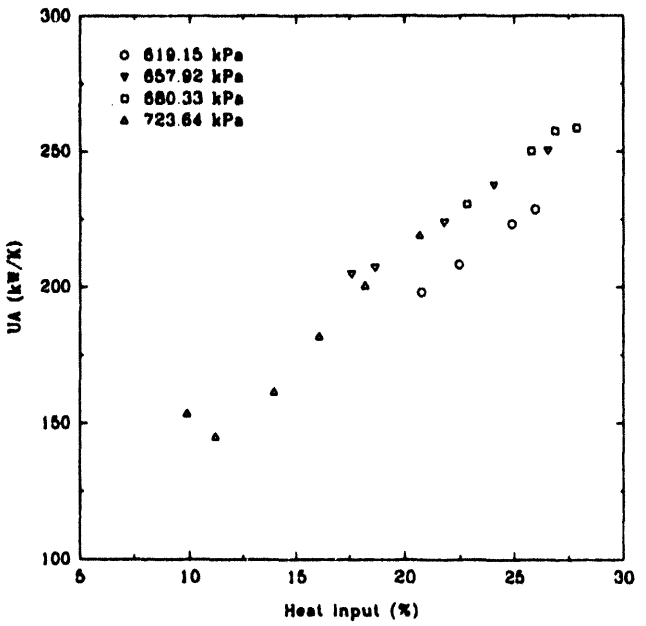


Figure 11: Overall Heat Transfer Coefficient

SUMMARY AND CONCLUSIONS

Reflux cooling under conditions associated with loss of forced circulation, mid-loop coolant levels and noncondensables in the primary coolant system is being studied on the NCSU Scaled PWR Facility. The Scaled PWR Facility is a Freon-11 based, 1/9 scale model of a two-loop Westinghouse Pressurized Water Reactor. The

first phase of this work has involved measurement of steady-state heat transfer rates, liquid and vapor velocities and liquid and vapor temperatures as a function of primary and secondary side pressures while operating under reflux cooling conditions in the absence of noncondensables. The results clearly show the strong coupling of heat transfer rate to the primary and secondary side saturation pressures and can provide benchmark data for modeling of the reflux cooling process in actual U-Tube steam generator configurations. The current work is being extended to measure the magnitude and time duration of the primary side pressure excursion associated with loss of heat sink as a function of noncondensable concentration.

REFERENCES

1) C. Calia and P. Griffith, "Modes of Circulation in an Inverted U-Tube Array with Condensation," HTD-Vol. 15, ASME, New York (1981)

2) S. Banerjee, J-S. Chang, R. Girard and V. S. Krishnan, "Reflux Condensation and Transition to Natural Condensation in a Vertical U-Tube," *Journal of Heat Transfer*, **105**, 719 (1983).

3) R. Girard and J. S. Chang, "Reflux Condensation Phenomena in Single Vertical Tubes," *Int. J. Heat Mass Transfer*, **35**, 2203 (1992).

4) M-H. Chun and J-W. Park, "Reflux Condensation Phenomena in Vertical U-Tubes With and Without Noncondensable Gases," 84-WA/HT-2, ASME, New York (1984).

5) M. Siddique, M. W. Golay and M. S. Kazimi, "Local Heat Transfer Coefficients for Forced-Convection Condensation of Steam in a Vertical Tube in the Presence of a Noncondensable Gas", *Nucl. Tech.*, 102, 386 (1993).

6) Y. A. Hassan and L. L. Raja, "Analysis of Experiments for Steam Condensation in the Presence of Noncondensable Gases Using the RELAP5/MOD3 Code," *Nucl. Tech.*, **104**, 76 (1993).

7) L. W. Ward, "Evaluation of the Loss of Residual Heat Removal Systems in Pressurized Water Reactors With U-Tube Steam Generators," *Nucl. Tech.*, **100**, 25 (1992).

8) D. E. Palmrose, E. D. Hughes, and G. W. Johnsen, "RCS Pressure Under Reduced Inventory Conditions Following a Loss of Residual Heat Removal," *AIChE Symposium Series, Heat Transfer 1992*, San Diego, California, Vol. **88**, No. 288, 267 (1992).

9) J. R. Caves, G. D. Miller, and B. W. Wehring, "NCSU Pressurized Water Reactor Physical Simulator," *IEEE Trans. Nucl. Sci.*, **36**, 1690 (1989).

10) M. Ishii and I. Kataoka, "Similarity Analysis and Scaling Criteria For LWR's Under Single-Phase and Two-Phase Natural Circulation," NUREG/CR-3267, March 1983.

CORE TO SURGE-LINE ENERGY TRANSPORT IN A SEVERE ACCIDENT SCENARIO

M. di Marzo, K. Almenas*, S. Gopalnarayanan
Mechanical Engineering Department
*Nuclear and Materials Engineering Department
University of Maryland
College Park, MD 20742

The analysis of loss of coolant accidents in a nuclear power plant, which progress to the stage where the core is uncovered, poses important safety related questions. One of these concerns the rate of energy transport to metal components of the primary system. An experimental program has been conducted at the University of Maryland test facility which quantifies the rate of energy transfer from an uncovered core in a B&W (once-through type steam generators) plant. SF_6 is used to simulate the natural circulation driving force of the high pressure steam expected at prototypical conditions. A time-dependent scaling methodology is developed to transpose experimental data to prototypical conditions. To achieve this transformation, a nominal fluid temperature increase rate of 1.0 °C/s is inferred from available TMI-2 event data. To bracket the range of potential prototypical transient scenarios, temperature ramps of 0.8 °C/s and 1.2 °C/s are also considered. Repeated tests, covering a range of test facility conditions, lead to estimated failure times at the surge line nozzle of 1.5 to 2 hours after initiation of the natural circulation phase of the transient.

1. Introduction

The study of severe nuclear power plant accidents has progressed from hypothetical scenarios, which were defined by imposed assumptions, to accident development sequences which maintain a physically coherent sequence of events. An example of this evolution is the Direct Containment Heating (DCH) issue. It arose by assuming that, during a core melt event, the pressure of the system would be maintained and a breach would be created at the vessel bottom. This sequence of events could produce a violent expulsion of the molten fuel mass which in turn could lead to its dispersal into the containment and an associated rapid transfer of mass and energy to the containment atmosphere. However, it is conceivable that the primary system could depressurize before a failure in the bottom section of the pressure vessel occurs. Such depressurization could be caused by structural failures (due to overheating) in the upper regions of the primary system brought about by natural circulation heat transport. A consensus exists in the technical community that the evaluation of the energy transfer occurring in the regions above a molten or overheated core is presently associated with substantial uncertainties [1,2]. There is a need to obtain experimental data for flow geometries and operating conditions simulating those above a degraded core. To be useful, such experiments require verifiable scaling procedures for transposing the data to prototypical scale and conditions.

Some experimental information, which address the conditions to be found in the primary system of a reactor, can be inferred from the TMI-2 accident. The relevant

information on natural circulation processes, that has been distilled from this event, remains relatively sparse. Of special importance in this respect is the metallurgical evaluation of two control rod lead-screws. These lead-screws extended from the top of the vessel dome to the upper plate of the core. An extensive metallurgical analysis has made it possible to infer the temperatures to which these lead-screws were exposed. The evidence presented by Vinjamuri et al. [3] implies that the lead-screws were exposed to a temperature of 390 °C (at the top) increasing to a temperature of up to 980 °C near the core.

A number of experimental and analytical studies relevant to this area are summarized by Denny [4]. The most significant series of experimental investigations has been conducted by Stewart [5,6] and co-workers on a 1/7 test facility at Westinghouse laboratories. The facility models 1/2 of the pressure vessel and near-by piping for a Westinghouse plant (U-tube type steam generators). An initial series of tests used water and SF_6 gas at atmospheric pressure. Subsequent series of tests employed SF_6 at moderate pressures (up to 27 bar). Subsequently, modifications were made to the facility in order to approximate the hot-leg flow geometry of a B&W plant (once-through type steam generators). The last series of experiments showed counter-current circulation in the hot leg in spite of its small cross-sectional area, however, the full report of the high pressure experimental results is not yet available.

On the analytical side, a number of studies which model the PWR core and hot leg flow geometries have been carried out using the current state-of-the-art thermal hydraulic codes. These include the RELAP5 [7,8], the SCADAP/RELAP5 [9], and the CORMLT [4] codes. The limitations of the codes are especially apparent in the modeling of the gas-gas counter-current flow. To achieve this, the models have to divide contiguous pipe segments into two independent flow channels. This requires a-priori assumptions regarding the cross-sectional flow area of the counter-currently flowing streams and eliminates mass and momentum interchange between them.

Scaling studies which strive to develop a methodology for transposing experimental data to prototypical core-uncovery transients have to confront several unique conditions. A principal one is that this event is time dependent and steady state conditions are not reached. Not all scaling studies take this into account. Thus, in a number of recent studies [5,6,7,8,9,10], the issue of energy and mass transport above an uncovered core have been considered by employing the classical quasi-steady-state scaling approach. This allows the derivation of time independent scaling invariants. Such an approach is justifiable for transients during which the system stays within a limited range of fluid conditions and for which the dominant time constants are considerably shorter than the transient duration. This is approximately the case for SB-LOCA transients where the core is being cooled by a liquid or a two-phase coolant. However, both of these criteria do not apply anymore once the core becomes uncovered. Such an event initiates a transient during which the temperature of the core and surrounding gases increases. This transient temperature rise does not approach steady state and is terminated either by a change in the boundary conditions (e.g. core re-flooding caused by the emergency core cooling) or by failure of the primary pressure boundary. While the transient is progressing, thermal equilibrium is approached only by the relatively thin internal metal structures. The heavier internal structures and especially the massive metal boundaries (that is the reactor vessel walls, the

hot leg and associated piping walls) will not reach thermal equilibrium. This can be readily verified by comparing thermal time constants for metal and fluid regions. More significantly, this characteristic was illustrated during the TMI-2 accident sequence: the available, though limited, measurements and post accident analysis of material specimens showed that in the thirty-five-minute period (during which natural circulation processes could develop), temperatures above the core rose continuously [3].

Under these circumstances scaling schemes which are based on the assumption of quasi-steady-state conditions can be misleading. In order to reproduce prototypical phenomena, both the scaling procedures (which are used to design a scaled experimental facility) and the experimental test program must recognize that energy transport above an uncovered core is a dynamic process which does not reach a steady state condition. This requirement is the basis of the University of Maryland at College Park (UMCP) experimental facility design and test program.

Several other relevant aspects should be noted. A number of previous scaling studies focus their attention on the fluid within the system and disregard the solid structures and their associated heat capacities by assuming steady or quasi-steady state heat conduction. The time dependency of solid structures is included in a "lumped parameter" fashion in a number of studies described in an overview of natural circulation provided by Wassel et al. [10] while No and Ishii [11] address the heat-up transient of the core region.

Finally, the temperatures above a degraded core can be quite high, therefore the effects of radiative energy transport must be considered. This effect cannot be reproduced in reduced temperature experimental facilities and must be inferred. At the high prototypical pressure and temperature conditions, steam will be largely opaque to thermal radiation and most regions within the primary system will be "optically thick". The Rosseland absorption coefficient [12] for steam at overall pressures exceeding 10 bars is in the order of 600 $(\text{bars-m})^{-1}$ which means that, for steam pressures ranging from 40 to 100 bars in prototypical conditions, the absorption coefficient is in the order of 2×10^4 $(\text{m})^{-1}$. If one assumes that an optical thickness of three characterizes an optically thick medium, then for the prototypical conditions, steam should be considered optically thick at depths of more than one millimeter.

2. Scaling rationale

The scaling of transient heating phenomena in the complex geometry of the B&W plant [13] is described for a configuration in which loop flow is completely interrupted. As shown in Fig 1, this is a condition where the lower portion of the steam generators primary and the cold legs up to the loop seals elevation are filled with liquid water. The secondary sides of the steam generators are empty. This condition is postulated under the "station blackout" scenario. This analysis, could be applied to both raised and lowered loop (e.g. Davis-Besse) configurations provided that similar liquid blockages are present in the cold leg loop seals.

The various components involved in this heating transient differ primarily in their geometric characteristics. For example, in the major pipes (the hot and cold legs), which

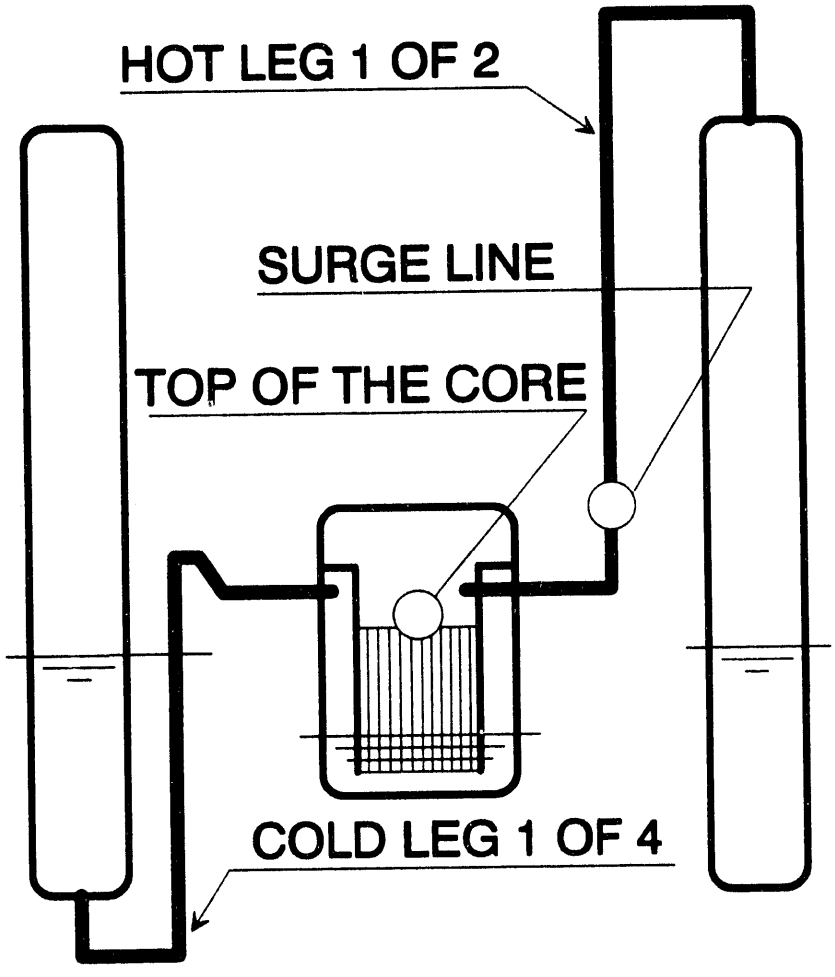


Figure 1 - Schematic representation of a B&W PWR primary system

have a high aspect ratio (L/D), heat is ransferred to the metal wall in a manner that can be conceptualized as a complex fin. On the other hand, the vessel is a compact structure where heat is transferred within geometries that can be characterized as enclosures. The pressure vessel includes substantial heat capacities associated primarily with the fuel elements and internal metal partitions.

The above assessment of the system thus identifies three types of components: a) the hot legs and the cold legs; b) the internal metal masses; and c) the vessel wall. The objective of this scaling effort is to generate a sound methodology which can be used to translate measurements obtained in a scaled model to prototypical conditions. A specific goal is to quantify the transient metal temperatures at potential failure locations and to infer time-to-failure information which can be compared with estimates for the lower vessel head failure. The result of this evaluation will determine the relevant DCH initiating scenario. The hot leg at the pressurizer surge line nozzle is identified as a potential failure location. Therefore, attention is focused on the hot legs and on the scaling of the transient thermal

behavior of metal at remote locations.

Hot legs scaling

The scaling of the complex, three dimensional hot leg geometry poses a difficult challenge. It will be shown that the time constants of convective energy transport in the fluid and of conductive energy transport in the metal have the same order of magnitude and must be considered simultaneously.

The conservation equations are cast into a non-dimensional form and integrated after applying appropriate boundary conditions to yield the various non-dimensional scaling parameters. The momentum equation makes use of a vectorial distribution of the gravitational field $\vec{\gamma}$. By using the Boussinesq approximation the relevant conservation statements are written as:

$$\frac{\partial \vec{u}}{\partial t} + \nabla\bullet(\vec{u}\vec{u} - \nu \nabla\vec{u}) = \beta \Delta T \vec{\gamma} g$$

$$\frac{\partial T}{\partial t} + \nabla\bullet(\vec{u}T - \alpha \nabla T) = 0 \qquad \frac{dT_m}{dt} = \alpha_m \nabla^2 T_m$$

(1,2,3)

The energy equation for the metal assumes a small Biot number for the metal wall. For the prototype, the wall does have a non-uniform temperature distribution. However, compared to the difference in temperature between the primary fluid and the containment temperature, the temperature drop across the wall is small. Therefore, the lumped capacity assumption is well within the approximations imposed by the scaling procedure. In order to non-dimensionalize these equations, it is necessary to identify the dominant time scale that should be used. A number of time scales can be readily identified: a) the momentum diffusion scale (D^2/ν); b) the fluid thermal diffusion scale (D^2/α); c) the metal thermal diffusion scale (W^2/α_m); and d) the axial transport scale (L/u_{nc}). The prototypical conditions span a wide range of temperatures, thus a large variation in the physical properties is observed. Estimates of the various time scales for the initial and representative transient prototypical conditions are provided in Table 1.

Table 1. Prototypical Time Scales [s]

	at 300 °C; 70 bars	at 1300 °C; 140 bars
Momentum diffusion (D^2/ν)	1.4×10^6	2.8×10^5
Thermal diffusion (D^2/α)	2.0×10^6	2.4×10^5
Metal thermal diffusion (W^2/α_m)	420	420
Axial transport ($L/[g\ \beta\ \Delta T\ D]^{1/2}$) for ΔT between 20 and 200 °C	24 - 8	67 - 20

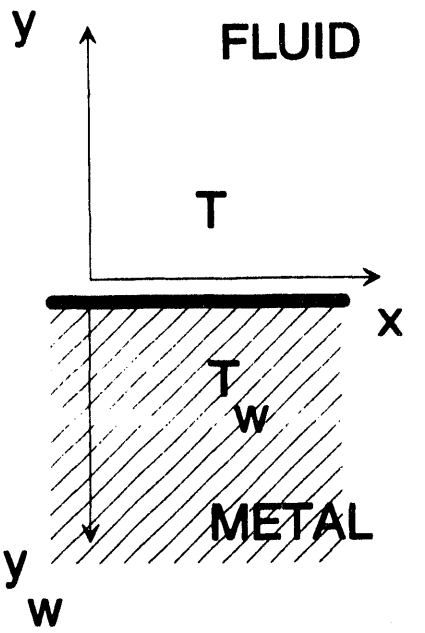


Figure 2 - Coordinate system

The axial transport process emerges as the dominant scale for the prototype because its time constant is significantly shorter than the others. The thermal diffusion time scale of the metal structures is also very important since major interest focuses on the metal thermal behavior. Figure 2 illustrates the coordinate system at the fluid-metal boundary. Based on the axial transport time constant and on the characteristic velocity for natural convection, the following non-dimensional variables are defined:

$$x^* = \frac{x}{L} \qquad y^* = \frac{y}{D} \qquad y_w^* = \frac{y_w}{W}$$

$$\vec{u}^* = \frac{\vec{u}}{\sqrt{g\beta\,\Delta T D}} \qquad t^* = \frac{t\sqrt{g\beta\,\Delta T D}}{L}$$

$$T^* = \frac{T - T_\infty}{\Delta T} \qquad V^* = \frac{V}{D^2 L}$$

$$S^* = \begin{cases} S/D^2 & (\textit{hot leg inlet cross-sectional area}) \\ S/DL & (\textit{fluid-metal interfacial area}) \end{cases}$$

(4,5,6,7,8,9,10,11,12)

By making use of the divergence theorem and by considering the proper reference area [Eqs. (11) and (12)], the momentum and energy equations are transformed as follows:

$$\int_{V*} \frac{\partial \vec{u}*}{\partial t*} dv* + \int_{S*} (\vec{u}*\vec{u}* - \frac{L/D}{\sqrt{Gr}} \nabla*\vec{u}*)\cdot\hat{n}\, ds* = - \int_{V*} L/D\, \vec{\gamma}\, dv*$$

$$- \int_{V*} \frac{\partial T*}{\partial t*} dv* = \int_{S*} (\vec{u}*T* - \frac{L/D}{Pr\sqrt{Gr}} \nabla*T*)\cdot\hat{n}\, ds*$$

$$\frac{dT_m*}{dt*} = \left[\frac{\rho c}{(\rho c)_m} \frac{D}{W}\right] \frac{L/D}{Pr\sqrt{Gr}} \left[\left(\frac{\partial T*}{\partial y*}\right)_{@wall} - \frac{h_e D}{k} T_m*\right]$$

(13,14,15)

Note that the metal energy equation is rearranged using the assumption of lumped heat capacity in the direction orthogonal to the wall. Therefore, it represents the local transient thermal behavior of the wall in the axial direction. This approximation is justified by the small value of the Biot numbers both inside and outside the structure for the prototype and the model (i.e. the maximum value of the Biot number, for the inner side of the wall in the prototype, is estimated at 0.18).

Equations (13), (14) and (15) are used to identify the following non-dimensional parameters:

$$\Pi_1 = \frac{L}{D} \qquad \Pi_2 = (Gr)^{-1/2} \qquad \Pi_3 = (Pr)^{-1}$$

$$\Pi_4 = \frac{\rho c}{(\rho c)_m} \frac{D}{W} \qquad \Pi_5 = \frac{h_e D}{k}$$

(16,17,18,19,20)

Two difficulties arise in this scaling task. The first is the wide range of temperatures traversed by the transient which requires careful consideration of the variation of physical properties. In order to estimate the resulting distortions, the values for the initial and final conditions will be determined and a geometrical average will be used to approximate the various non-dimensional parameters. The second difficulty is that the elevated temperatures of the prototype require the inclusion of the radiant heat transfer contribution. Under prototypical pressure of 70 to 140 bars, steam is opaque. Therefore, direct radiation between the metal structures is unlikely but radiation to and from the gas should be considered. In the range of temperature and pressures of concern, steam has an emissivity of about 0.4 [14]. For the purpose of deriving comparative indexes, the gas is approximated as a non-Kirchoff surface of emissivity 0.4 and absorptivity 1. This means that the portion of radiation transmitted to gas layers which are not adjacent to metal surfaces is absorbed within the gas itself. With this simplification, the relative magnitude of the radiation

Table 2. Prototypical and Model Physical Properties and Representative Dimensions

	Prototype	Model	P/M
Fluid	H_2O & H_2	SF_6	
System Pressure (MPa)	7.0 - 14	2.0	
System Temperature (°C)	300 - 1300	20 - 190	
Ambient Temperature (°C)	100	20	
Fluid Density (kg/m^3)	25	120	0.21
Fluid Viscosity (kg/m-s)	3.4×10^{-5}	2.0×10^{-5}	1.7
Fluid Thermal Conductivity (W/m K)	0.10	0.019	5.3
Fluid Specific Heat (J/kg K)	3.4×10^{3}	8.4×10^{2}	4.1
Fluid Thermal Expansion Coefficient (K^{-1})	1.7×10^{-3}	5.3×10^{-3}	0.32
Hot Leg Length (m)	21	1.6	13
Hot Leg Inside Diameter (m)	0.91	0.087	11
Hot Leg Wall Thickness (m)	0.070	0.014	5.0

contribution to the overall heat transfer coefficient is derived. By linearizing and normalizing the radiative contribution with respect to the convective heat transfer coefficient [15], one obtains:

$$h_{overall} = h_c \left(1 + \frac{4 \sigma T^3}{h_c \Omega} \right)$$

$$where \quad \Omega = \frac{1 - \varepsilon_{wall}}{\varepsilon_{wall}} + \frac{1}{\varepsilon_{steam}} \qquad (21,22)$$

The term in parenthesis on the right hand side of Eq. (21) will be referred to as the "radiation enhancement" and is identified as Σ_h. The subscript is added to stress the fact that the radiation enhancement is evaluated for an assumed value of the convective heat transfer coefficient. The evaluation of the convective heat transfer coefficient is difficult because the transient flow of steam in the hot legs is not known. This is the main motivation for experimental programs. Given appropriate experimental information from the scaled model, correlations, which provide reasonable predictions of the measured convective heat transfer

coefficients, can be identified [16]. The correlations can then be used to infer a convective heat transfer coefficient ratio between prototype and model as:

$$(h_c)_{P/M} = k_{P/M} \left(\frac{\beta \Delta T}{\nu \alpha} \right)^{0.282}_{P/M} D^{0.154}_{P/M}$$

(23)

For this particular problem, typical values of the radiation enhancement Σ_h range between 1.1 and 1.6 yielding a geometrical averaged value of about thirty percent. The radiation enhancement can be regarded as a correction to the Prandtl number [14] (parameter Π_3). For clarity, the two parameters will be kept separate since this will simplify the assessment of the scaling distortions.

For future reference, the various terms of the conservation equations are written in the following way:

$$\int_{V*} \frac{\partial \vec{u}*}{\partial t*} dv* + \int_{S*} (\vec{u}* \vec{u}* - \Pi_1 \Pi_2 \nabla* \vec{u}*) \cdot \hat{n} \, ds* = \int_{V*} \Pi_1 \vec{\gamma} \, dv*$$

$$- \int_{V*} \frac{\partial T*}{\partial t*} dv* = \int_{S*} (\vec{u}* T* - \Pi_1 \Pi_2 \Pi_3 \Sigma_h \nabla* T*) \cdot \hat{n} \, ds*$$

$$\frac{dT_m*}{dt*} + \Pi_1 \Pi_2 \Pi_3 \Pi_4 \left[\Pi_5 T_m* - \Sigma_h \left(\frac{\partial T*}{\partial y*} \right)_{@wall} \right] = 0$$

(24,25,26)

Careful consideration is given to the energy equation for the hot leg metal wall because the wall temperature is one of the quantities of interest in this transient. If one considers the general form of the solution for Eq. (26), subjected to a steady state initial condition, the following result can be obtained:

$$T_m* = e^{-t*/\tau} \left[\int_0^{t*} e^{z/\tau} f(T*) \, dz + C \right]$$

$$\text{where} \qquad \tau_{hot\,leg\,wall} = (\Pi_1 \Pi_2 \Pi_3 \Pi_4 \Pi_5)^{-1}$$

(27,28)

It is assumed that initially the prototype is at a near uniform temperature of about 300 °C and the scaled model is at ambient temperature. Core uncovery initiates the transient in the prototype while electrical heaters are turned on at a specified power in the scaled model. Based on the definitions of the non-dimensional variables, the model experimental data will be translated to prototypical conditions according to the following

relationships:

$$t_{prototype} = \left(\frac{L}{\sqrt{g\,\beta\,\Delta T D}}\right)_{P/M} t_{model}$$

$$(T_m - T_\infty)_{prototype} = (\Delta T)_{P/M} (T_m - T_\infty)_{model}$$

(29,30)

The traditional definition of the reference temperature difference, ΔT, based on a reference fluid and hot leg temperature cannot be used in this case since the heat-up is a transient event. Furthermore, the fraction of the energy deposited in each of the hot leg is relatively small (i.e., about 4 %). For the prototype this fraction is likely to be even smaller since the heat capacity of the core is far larger than the heat capacity of the test facility heaters. To circumvent this difficulty, a parameter, called the "temperature ramp ratio" is introduced to compare the prototype and test facility time dependent heat-up rates:

$$R = \left(\frac{\partial T}{\partial t}\right)_{P/M}$$

(31)

The temperature ramp ratio in effect quantifies the impact that core power exerts on the fluid rather then core power itself. This is preferable since, as it has been noted, the massive prototypical core heat capacity is not reproduced in the scaled facility. However, if tests are started from the same initial conditions, then the prototype-to-model ratio of the fluid heat capacities remain constant. Then the ratio of the prototype-to-model power transferred to the fluid can be replaced by the prototype-to-model ratio of the respective temperature ramps. That is the basis for the definition of the ramp ratio R.

The introduction of Eq. (31) in Eqs. (29) and (30) yields:

$$t_{prototype} = \left(\frac{L}{\sqrt{\beta D}}\right)^{2/3}_{P/M} R^{-1/3}\, t_{model}$$

$$(T - T_o)_{prototype} = \left(\frac{L}{\sqrt{\beta D}}\right)^{2/3}_{P/M} R^{2/3}\, (T - T_o)_{model}$$

(32,33)

With reference to Eqs. (17,24,25,26), the parameter Π_2 is the inverse of the square root of the Grashof number, namely:

$$(\Pi_2)_{P/M} = \left(\frac{\mu}{\rho}\right)_{P/M} \left(\frac{1}{\beta\, \Delta T D^3}\right)_{P/M} \qquad (34)$$

The right hand side of this parameter is dominated by the ratio of the diameter D (the model being smaller than the prototype). In order to compensate this influence, a working fluid which has a large viscosity-to-density ratio is required. An acceptable candidate is the non-toxic dense gas SF_6 which was also selected by Stewart for the Westinghouse facility [5,6]. Table 2 lists some of its properties in reference to steam at prototypical conditions and Table 3 summarizes the scaling distortions associated with the various terms of the governing equations [Eqs. (24,25,26)] as a function of the ramp ratio. As shown in Table 3, the distortion of most scaling parameters (that is the deviation of the prototype-to-model parameter ratio from the unity) grows as the ramp ratio increases. Physically, this implies that a large difference in the prototype-to-model heat-up rate of the carrier fluid exacerbates the differences in the viscous term and in the fluid-wall heat transfer term.

Scaled model

The UMCP integral test facility is a comprehensive scaled representation of a B&W PWR system. It models both once-through steam generators, the hot and cold legs, and the pressure vessel which incorporates an internal down-comer and reactor vessel vent valves. The facility has been used to investigate the integral system response of a wide range of accident conditions. For the current test program, the facility was modified according to the scaling approach previously outlined. Table 2 lists some of the representative dimensions of the facility in comparison with the prototype.

Table 3. Effect of Ramp Ratio on Average Distortions

Ramp Ratio	1.0	2.0	5.0	10
Time Ratio: $t_{P/M}$	3.6	2.9	2.1	1.7
Temperature Difference Ratio: $\Delta T_{P/M}$	3.6	5.8	11	17
Aspect Ratio: $\Pi_{1,\,P/M}$	1.2	1.2	1.2	1.2
Viscous Term Ratio: $(\Pi_1 \Pi_2)_{P/M}$	0.19	0.15	0.11	0.09
Fluid-Wall Heat Transfer: $(\Pi_1 \Pi_2 \Pi_3 \Sigma_h)_{P/M}$	0.20	0.16	0.11	0.09
Metal Wall Time Constant: $[(\Pi_1\Pi_2\Pi_3\Pi_4\Pi_5)^{-1}]_{P/M}$	1.1	1.4	1.9	2.4

A schematic of the flow geometry in the vicinity of the core is shown in Fig. 1. This

simplified figure omits a number of details, components not shown (but present in the experimental facility) include: a second hot leg, three additional cold legs, the upper head plate, the reactor vessel vent valves and the control rod guide tubes. The last three components represent significant massive metal structures located above the core. In the figure, the "top of the core" and "surge line" locations are identified since the specific objective of this paper is to quantify the energy transport between these two locations.

3. Results and discussion

The experimental bounds are set by the saturation conditions of the SF_6 which (in order to avoid condensation of the gas at ambient temperature) restricts the model operating pressure to slightly less than 2 MPa. The test duration is limited by the onset of SF_6 decomposition which becomes significant at temperatures in excess of 500 °C. The tests are terminated when the core heaters reach this limiting temperature. Within these bounds, the tests are conducted by powering-up the heaters from a steady state initial condition at ambient temperature. The pressure is maintained at about 2 MPa throughout the test and, when the maximum temperature set point is reached, the core heaters are automatically tripped. For this test series, the UMCP facility has been operated using heater power in the range between 20 and 40 kW.

A key parameter characterizing each transient is the temperature ramp which is measured at the top of the core. This location has been selected since it represents the highest bulk fluid temperature. In order to infer a temperature ramp ratio R, a prototypical temperature ramp must be postulated. The metallurgical analysis performed by Vinjamuri et al. [3] shows that the lead-screw rods located at the top of the TMI-2 core reached a temperature of about 1000 °C. The initial condition can be assumed to be about 300 °C and the duration of the natural circulation phase during the TMI-2 event is about 2100 seconds. This corresponds to a prototypical temperature ramp in the metal of 0.33 °C/s. This is the lower bound which could be assigned to prototypical temperature increase rates. Realistic rates are likely to be considerably higher. The lead-screws in question are separated from the hot core gasses by a metal guide tube. Their rate of temperature increase will therefore lag behind the actual fluid temperature. Since part of the TMI-2 core actually melted, local temperatures approaching 3000 °C must have been reached [17]. This is the basis to choose, for comparison purposes, a nominal prototypical fluid temperature ramp ratio of 1.0 °C/s at the top of the core. Appreciably higher sustained temperature increase rates cannot be justified by the available energy source and the heat capacities of the core and the immediate core region although, for brief periods of time (i.e., during intense zirconium oxidation), the prototypical temperature ramp could be steeper.

Figure 3 presents the fluid temperature increase for the model at the top of the core for three different core power tests. Note that each of the three traces represent multiple tests. The figure illustrates that the tests are repeatable and that temperature trajectories are well bounded. Figure 4 illustrates the measured temperature rise in the metal at the surge line nozzle location for the test facility.

The postulated prototypical temperature increase rate of 1 °C/s, results in ramp ratios of: 3.5, 4.5, and 6.3 for test facility heater powers of: 40, 30, and 20 kW respectively.

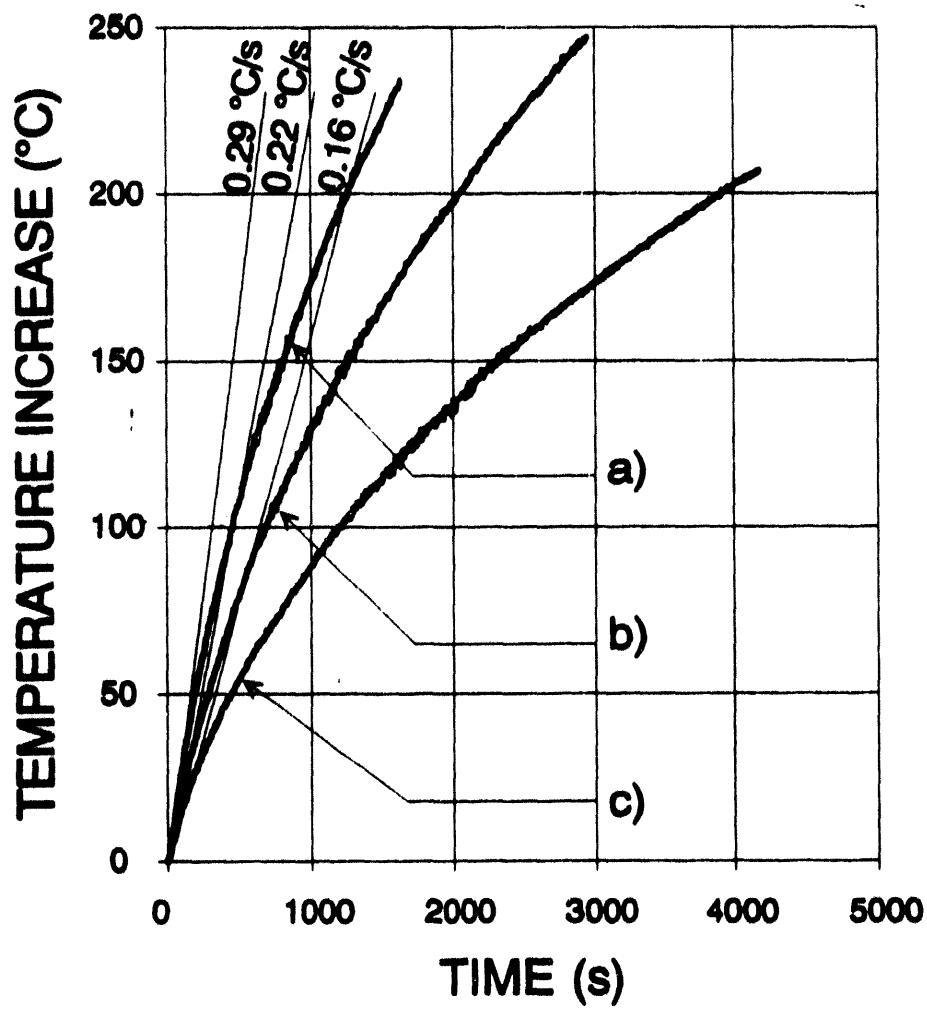


Figure 3 - Fluid temperature at the top of the core for the UMCP facility for various core powers (a: 40 kW; b: 30 kW; c: 20kW)

Use of these R values in Eqs. (32) and (33), generates the temperature-versus-time plots for the prototype shown in Figure 5. Note that these traces are evaluated independently from the three model transients conducted at different powers (i.e. with different ramp ratios). The fact that the three independent traces are almost coincident demonstrates the effectiveness of the scaling relationships.

Surge line failure can be expected to occur when the temperature of the hot leg surge line nozzle metal approaches 1300 °C, this requires a local temperature increase of about 1000 °C. Note that, for the R = 3.5 transient (conducted at 40 kW), this failure criterion is not reached. However, it can be inferred by extrapolation and the resulting value is consistent with the estimates obtained from the transients with R = 4.5 and R = 6.3 (i.e. 20 and 30 kW tests). If the distortions are to be contained within one order of magnitude, the transient with R = 6.3 should not be considered. This implies that only the 30 kW test

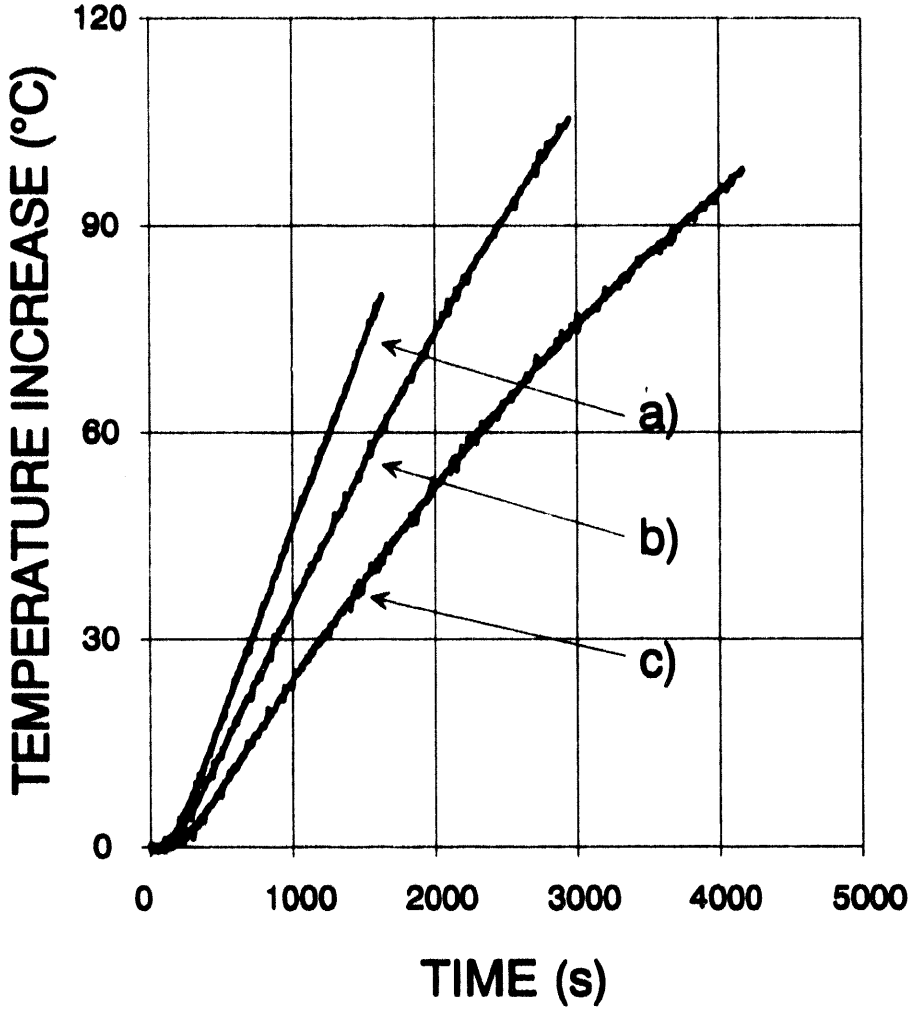


Figure 4 - Surge line metal temperature for the UMCP facility for various core powers (a: 40 kW; b: 30 kW; c: 20kW)

provides good simulation coverage (i.e., test duration) while keeping the distortions within acceptable bounds.

From Figure 5, the time-to-failure is estimated at 6000 s. The total error bar associated with the two estimates is ± 500 s and is due to the spread in the experimental data. Of course, this estimate depends on the postulated average fluid temperature increase rate of 1 °C/s for the prototype. While, on the basis of the TMI-2 event data, this is a plausible magnitude, other scenarios could lead to higher or lower rates of temperature increase. To extend these findings, the same procedure has been followed for a postulated prototypical ramp of 0.8 °C/s and 1.2 °C/s. The time-to-failure estimates for these cases are 7700 ± 700 s with a prototypical ramp of 0.8 °C/s and 5000 ± 300 s with a prototypical ramp of 1.2 °C/s.

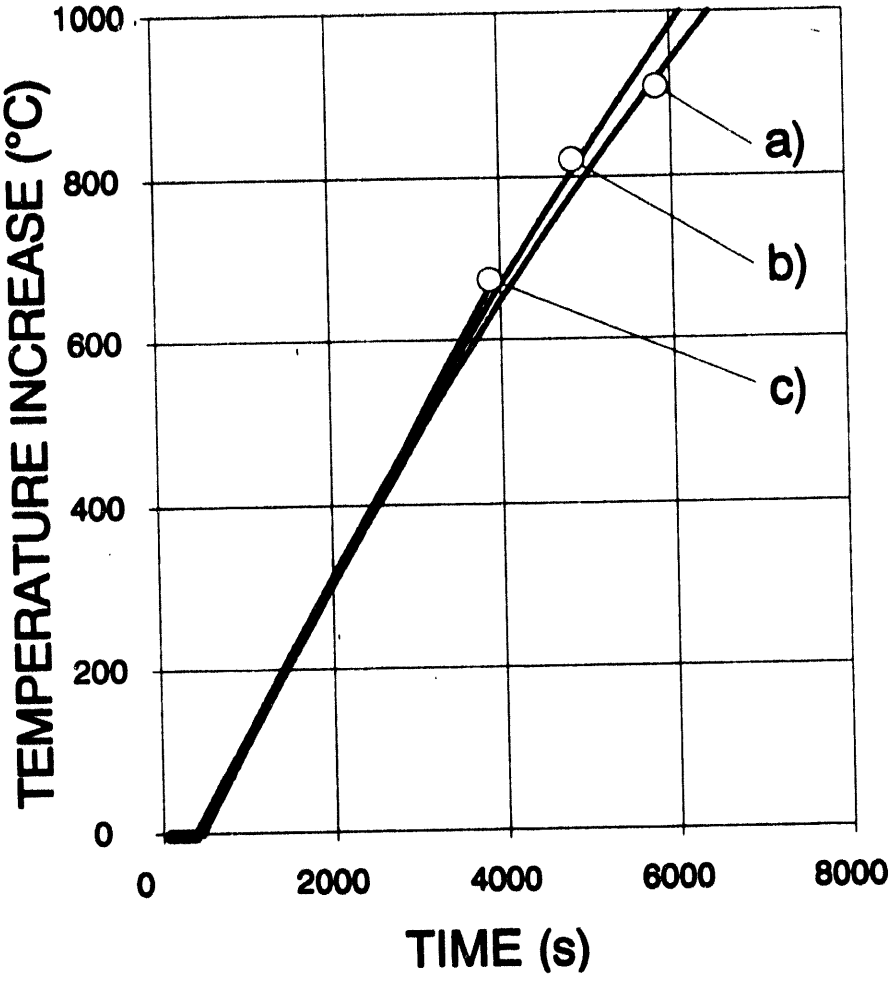


Figure 5 - Scaled prototype surge line metal temperature for a postulated prototypical fluid temperature ramp at the top of the core of 1 °C/s with various ramp ratios (a: R = 6.3; b: R = 4.5; c: R = 3.5)

These results are summarized in terms of the surge line nozzle failure probability P_f in Figure 6. It is shown that the time range for surge line nozzle failure is on the order of 1.5 to 2 hours after initiation of the natural circulation phase of the transient.

4. Conclusions

The time dependent non-dimensional conservation equations have been used to derive scaling relationships required to transpose experimental data obtained in test facility transients to prototypical conditions. A difficulty posed by transient heat-up events is that temperature differences change continuously and standard procedures used for non-dimensionalizing temperatures are inadequate. This issue is resolved by employing the "temperature ramp ratio" concept. This ramp ratio makes it possible to compare prototypical and test facility heat-up scenarios. The effect of thermal radiation has been

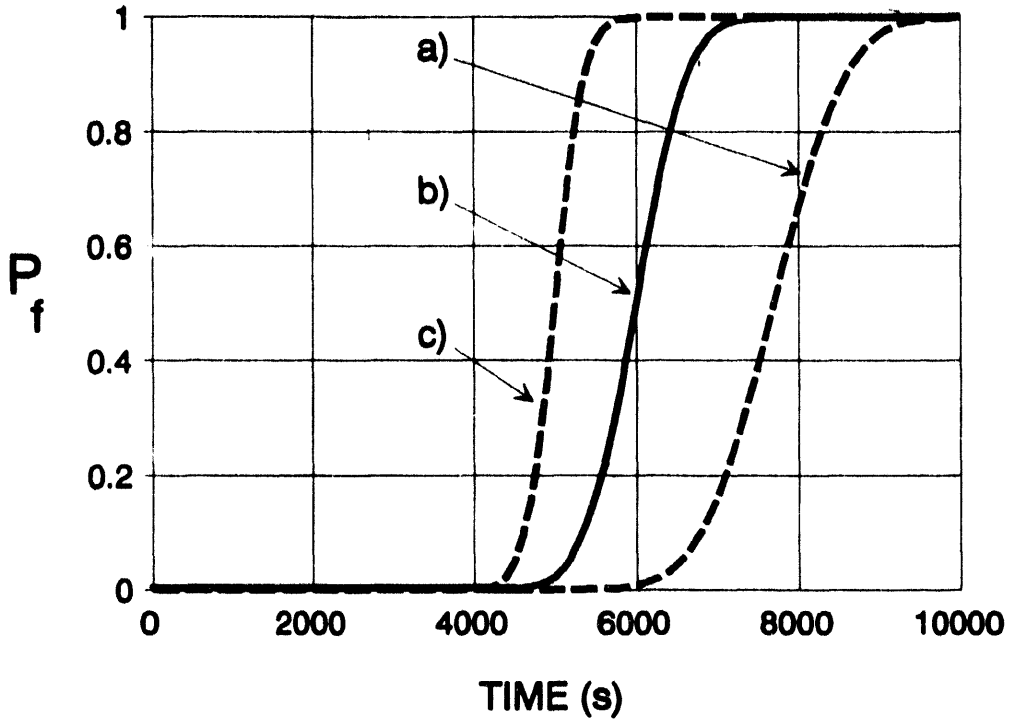


Figure 6 - Surge line nozzle failure probability for various prototypical fluid temperature ramps at the top of the core (a: 0.8 °C/s; b: 1.0 °C/s; c: 1.2 °C/s)

scaled and is included as an enhancement of the overall prototype heat transfer between the fluid ant the metal wall.

The scaling distortions for all the terms derived from the conservation equations are quantified for a range of ramp ratios consistent with the experimental data and with reasonable prototypical temperature ramps. This analysis is used to guide the choice of test facility operation and boundary conditions. It is shown that because of its low kinematic viscosity and relatively high density SF_6 is a suitable working fluid. The chosen matrix of experimental transients strives both to minimize scaling distortions and to provide a range of test conditions which are sufficiently broad so that a verification of the scaling methodology, through repeat tests using overlapping experimental conditions, becomes possible.

The series of experiments, conducted at the UMCP facility, provide transient data which are transposed to the prototypical scale to yield time-to-failure estimates at the hot leg surge line nozzle. With a postulated prototypical temperature increase rate of 1 °C/s (which is consistent with the TMI-2 transient observations), failure at the surge line nozzle is estimated to occur 1.5 to 2 hours after initiation of the natural circulation phase of the transient.

Acknowledgements

This study is supported by the U.S. Nuclear Regulatory Commission. The authors are indebted to Professors Gore, Griffith, Ostrach and Viskanta for their suggestions and advise.

Nomenclature

c	heat capacity
C	constant
D	hot leg inside diameter
g	gravitational acceleration
Gr	Grashof number: $g \beta \Delta T D^3 / \nu^2$
h	heat transfer coefficient
h_c	convective heat transfer coefficient
h_e	external convective heat transfer coefficient
k	thermal conductivity
L	hot leg length
$\hat{n}$	unit vector normal to the wall
P_f	surge line nozzle failure probability
Pr	Prandtl number: $\mu c / k$
R	temperature/time ramp ratio (Eq. 31)
S	surface
t	time
T	temperature
T_∞	external temperature
u_{nc}	natural convection characteristic velocity: $(g \beta \Delta T D)^{1/2}$
$\vec{u}$	velocity vector
V	volume
W	characteristic length of a metal structure
x	axial coordinate
y	fluid coordinate normal to the wall
y_w	metal coordinate normal to the wall
z	dummy variable
α	thermal diffusivity
β	thermal expansion coefficient
$\vec{\gamma}$	gravitational field vector distribution (Eq. 1)
ΔT	reference temperature difference
ϵ	emissivity
μ	viscosity
ν	kinematic viscosity
Π_i	non-dimensional parameter (Eqs. 16,17,18,19,20)
ρ	density
σ	Stefan-Boltzmann constant

Σ_h radiation enhancement
τ time constant
Ω radiation network resistance (Eq. 21)

Subscripts
m metal property
P/M prototype-to-model ratio
* non-dimensional property
o at transient initiation (Eq. 33)

References

[1] V. Stello, Integration plan for closure of severe accident issues, SECY-88-147 (1988).
[2] V. Stello, Revised severe accident research program plan, SECY-89-123 (1989).
[3] K. Vinjamuri, D.W. Akers and R.R. Hobbins, TMI-2 Leadscrew radionuclide deposition and characterization, EPRI-NP-4113-SR (1985)
[4] V.E. Denny, The role of natural circulation in severe accident analysis, NUREG/CR-0080, 2 (1986).
[5] W.A. Stewart, A.T. Pieczynski and V. Srinivas, Experiments on natural circulation in a PWR model for degraded core accidents, EPRI RP2177-5 (1990) .
[6] B.R. Sehgal, W.A. Stewart and W.T.Sha, Experiments on natural circulation during PWR severe accidents and their analysis, Int. European Nuc. Soc./ANS Meeting on Reactor Safety, Avignon, France (1988)
[7] D.J. Hanson et al., Depressurization as an accident management strategy to minimize the consequences of DCH, NUREG/CR-5447 (1990).
[8] D.J. Pafford, D.J. Hanson, V.X. Tung and S.V. Chmielewski, Natural circulation under severe accident conditions, NUREG/CP-0126, 2, (1992)
[9] P.D. Bayless, Analysis of natural circulation during a Surry station blackout using SCADAP/RELAP5, NUREG/CR-5214 (1988).
[10] A.T. Wassel, S.M. Ghiaasiann, V.E. Denny and R.M. Traci, "Modelling of natural circulation in reactor coolant systems, Fluid Physics Ind., FPI R88-05-04 (1988).
[11] H.C. No and M. Ishii, An analytical method for generating the scaling criteria of core uncovery and heatup processes, ANS Proc. HTC , 5, 303 (1991).
[12] C.L. Tien, Advances in Heat Transfer, (T.F. Irvine and J.P. Hartnett editors) Academic Press, 5, 253 (1968).
[13] Babcock & Wilcox, Steam, (1978)
[14] W.H. McAdams, Heat Transmission, McGraw-Hill (1933).
[15] E.M. Sparrow and R.D. Cess, Radiation Heat Transfer, Brooks/Cole (1970).
[16] B.Y. Gebhardt, Y. Jaluria, R. Mahajan and B. Sammakia, Buoyancy-Induced Flows and Transport, Hemisphere 14 (1988).
[17] R.R. Hobbins, J.M. Broughton and C.M. Allison, Understanding the TMI-2 accident: an overview, Proc. of the Int. ANS/ENS Topical Meeting on Thermal Reactor Safety, San Diego, (1986)

ASSESSMENT OF THE POTENTIAL FOR HPME DURING A STATION BLACKOUT IN THE SURRY AND ZION PWRS[a]

D. L. Knudson[b]
P. D. Bayless[b]
C. A. Dobbe[b]
F. Odar[c]

Idaho National Engineering Laboratory
Idaho Falls, ID 83415

ABSTRACT

The integrity of a PWR (pressurized water reactor) containment structure could be challenged by direct heating associated with a HPME (high pressure melt ejection) of core materials following reactor vessel lower head breach during certain severe accidents. Structural failure resulting from direct containment heating is a contributor to the risk of operating a PWR. *Intentional* RCS (reactor coolant system) depressurization, where operators latch pressurizer relief valves open, has been proposed as an accident management strategy to reduce those risks by mitigating the severity of the HPME. However, decay heat levels, valve capacities, and other plant-specific characteristics determine whether the required operator action will be effective. Without operator action, natural circulation flows could heat ex-vessel RCS pressure boundaries (surge line and hot leg piping, steam generator tubes, etc.) to the point of failure before failure of the lower head providing an *unintentional* mechanism for depressurization and HPME mitigation. This paper summarizes an assessment of RCS depressurization with respect to the potential for HPME during a station blackout in the Surry and Zion PWRs. The assessment included a detailed transient analysis using the SCDAP/RELAP5/MOD3 computer code and an evaluation of RCS depressurization-related probabilities primarily based on the code results.

---

a. Work supported by the U. S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, under DOE Idaho Field Office Contract DE-AC07-76ID01570.

b. Staff member at the Idaho National Engineering Laboratory.

c. Staff member at the U. S. Nuclear Regulatory Commission.

INTRODUCTION

The integrity of a PWR (pressurized water reactor) containment structure could be challenged by direct heating associated with a HPME (high pressure melt ejection) of core materials following reactor vessel lower head breach during certain severe accidents. A potential structural failure resulting from DCH (direct containment heating) is a contributor to the risk of operating a PWR.

Intentional RCS (reactor coolant system) depressurization, where plant operators latch pressurizer PORVs (power-operated relief valves) open, has been proposed as an accident management strategy to reduce the risks associated with potential containment failures by preventing or mitigating the severity of the HPME. However, decay heat levels, valve capacities, and other plant-specific characteristics determine whether the required operator action will lead to effective RCS depressurization. Analyses have been completed at the INEL (Idaho National Engineering Laboratory) that indicate intentional depressurization could be a viable method for mitigating HPME in the Surry PWR.[1] Subsequent analyses indicate that intentional depressurization could also be effective for many other PWRs.[2]

Without operator action, full loop, in-vessel, and hot leg countercurrent natural circulation flows could develop and redistribute core decay heat during severe reactor accidents.[3] Ex-vessel RCS pressure boundaries (surge line and hot leg piping, steam generator tubes, etc.) could be heated by the natural circulation of high temperature steam to the point of failure before failure of the lower head. Under those conditions, RCS depressurization through the ex-vessel pressure boundary breach could then occur without operator action. Thus, *unintentional* depressurization could provide an alternate way to minimize the potential for containment failure by preventing or mitigating the severity of the HPME.

An assessment of RCS depressurization with respect to the potential for HPME during a station blackout in the Surry an Zion PWRs was recently completed at the INEL.[4,5] This paper provides a summary of that work.

ASSESSMENT APPROACH

The assessment was limited to evaluation of a station blackout scenario because it is expected to cover the possible range of RCS responses during potential HPME events. The specific station blackout sequence selected for analysis is designated TMLB'. This sequence is initiated by the loss of off-site power. On-site AC (alternating current) power is also unavailable because the diesel generators fail to start or fail to supply power. Decay heat removal through the steam generators cannot be maintained in the long term because there is no AC power for the electrical pumps and the steam driven auxiliary feedwater pumps also fail to supply water.

When the TMLB' sequence begins, power is lost to the control rod drives and pumps. A reactor scram follows, with coastdown of the main feedwater pumps and RCPs (reactor coolant pumps). Feedwater is quickly reduced to zero as the main feedwater valves close. The turbine stop valves close and the pressure in the steam generators increases until the relief (or dump) valves open. Steam generator pressures are maintained between the opening and closing pressures of the relief valves thereafter. Water in the steam generator secondaries is completely vaporized by heat transfer from the RCS. However, heat transfer from the RCS is significantly reduced once water in the steam generator secondaries is depleted. Core decay energy then heats the RCS, resulting in system pressurization controlled by cycling pressurizer PORVs. The RCS pressure can also be influenced by RCP seal leaks, which could develop following the loss of

seal cooling water associated with the loss of all AC power. After the RCS saturates, a high pressure boiloff begins, ultimately leading to core uncovery and heatup. Without recovery of power or equipment, the transient can proceed to severe core damage and melting.

The assessment focused on the Surry and Zion PWRs in order to support an NRC Accident Management Program[6] and an NRC sponsored effort to resolve the DCH issue for PWRs.[5] Throughout this work, it was assumed that HPME would not occur if the RCS pressure could be reduced to 1.38 MPa or less before lower head failure. A two-part approach was used to complete the assessment including a detailed SCDAP/RELAP5/MOD3[7] analysis and an evaluation of RCS depressurization-related probabilities.

SCDAP/RELAP5/MOD3 Analysis

The objectives of the SCDAP/RELAP5/MOD3 analysis were to quantify the (a) time and location of the initial RCS pressure boundary failure, (b) associated RCS conditions at the time of initial pressure boundary failure, and (c) RCS conditions at the time of reactor vessel lower head failure. A specific modeling approach was required to meet those objectives.

SCDAP/RELAP5/MOD3 nodalization was included to allow development of full loop, in-vessel, and hot leg countercurrent natural circulation based on previous work.[3] Natural circulation flows were important in this assessment since they provide a mechanism for the potential generation of ex-vessel failures through redistribution of core decay heat.

Simple structural models of the lower head, surge line, hot leg piping, and steam generator tubes were included to track the potential for creep ruptures induced by the combined effects of elevated temperature and pressure. All structural models were based on nominal geometry without accounting for material defects or deterioration. Any predicted failure was appropriately recorded, although an associated RCS blowdown was not simulated. Instead, code calculations were extended to lower head failure without RCS depressurization in order to estimate the possible timing difference between all events.

SCDAP input was required to define certain parameters that control severe core damage progression. In general, best estimate parameters were selected where there were data or where the effects of the parameters were understood. For parameters with a high degree of uncertainty, values were selected to minimize the time to lower head failure. This approach provides the basis for a conservative evaluation of the potential for HPME since time is minimized for generation of an ex-vessel failure by natural circulation heating. The following describes input development for some of the more important parameters used in the calculations performed.

A temperature must be input to specify the cooling required to fragment core components during a quenching process. The expected range is from (T_{sat} + 100) K to 1273 K. A temperature of 1273 K was used in all calculations to minimize the cooling required to fragment. Early fragmentation and the associated core blockage could promote core heatup and molten pool formation, providing the potential for a relatively early failure of the lower head.

Debris formation during core degradation results in a flow restriction, leading to core heatup. An input was required to specify the extent of the restriction. Accordingly, the flow area through cohesive debris was set to 11% of the nominal flow area in all calculations. At values of 10% and less, SCDAP/RELAP5/MOD3 sets the flow area to zero. However, a flow area of zero corresponds to coplanar blockage, which has not been observed in limited test data. On that basis, 11% represents the maximum flow restriction

consistent with current understanding. By maximizing the flow restriction, core heatup and lower head failure should occur relatively early.

The ZrO_2 failure temperature controls when oxidized cladding will fail, provided that the oxide layer is less than the specified durable thickness. The failure temperature can vary between the melting points of Zr (2023 K) and ZrO_2 (2963 K). A value of 2400 K, which is near the lower end of the best estimate range, was used in all calculations.

Durable thickness is represented by the fraction of oxidation necessary for the cladding to withstand attack by molten Zr. Once the durable thickness is reached, the oxidized cladding will remain intact until the ZrO_2 is heated to the specified failure temperature (2400 K in this analysis). As a result, higher values tend to promote earlier relocation. On that basis, the ZrO_2 was assumed to be durable only if completely (100%) oxidized.

A thermal contact resistance must be input to characterize heat transfer between relocated core materials and the lower head vessel wall. Near-perfect (conduction-limited) contact might be possible if core materials are molten when they reach the lower head. However, considerable resistance could be postulated between particulate debris and the lower head. Because the parameter range is large, variable, and not easily quantified, the thermal contact resistance between relocated materials and the lower head was set to 0.0001 m^2-K/W in all calculations. This value should be small enough to approximate molten contact. In addition, application of the value for all other conditions is consistent with the effort to minimize the time to lower head failure.

Ballooning of the fuel rod cladding can occur if the internal pin pressure exceeds the external (RCS) pressure. Current code versions require an input to define the deformation that results in cladding failure due to ballooning. With the exception of one calculation, the deformation limit was set to 2%, corresponding to the best estimate value in cases where some oxidation occurs before the onset of ballooning. A rupture strain corresponding to a cladding deformation of 15% was assumed as a sensitivity parameter in one Surry calculation. According to the SCDAP code development staff, that value is near the upper limit of the average deformation that could be expected. A deformation of 15% provides a potential for larger in-core flow blockage, which could affect core heatup by reducing heat transfer to the natural circulation steam flow. In addition, core heatup could increase because the surface area available for oxidation increases with deformation.

If the cladding balloons and ruptures, inner cladding surfaces may be oxidized (along with outer cladding surfaces) as a result of exposure to high temperature steam. SCDAP requires input to define the threshold deformation for onset of this double-sided oxidation. Best estimate values are in the range of 2%. However, double-sided oxidation was assumed following cladding rupture at all rod locations with deformations of at least 1%, which is consistent with the effort to minimize the time to lower head failure.

Molten materials may pour from the core to the lower head in a coherent stream or the pour may be broken up as a result of interactions with in-vessel structures and water below the core. In general, breakup results in quenching the debris with a corresponding repressurization that results from associated vapor production. The quenched debris will then have to reheat before an effective lower head thermal attack can begin. On the other hand, heat transfer to the coolant is minimized and thermal attack on the lower head is maximized if the debris remains intact. Consistent with the effort to minimize the time to lower head failure, intact debris relocation (without debris/coolant heat transfer) was assumed in most of the calculations. Because debris breakup is a possibility and because debris/coolant heat transfer associated with breakup

could produce a repressurization affecting the HPME potential, debris breakup was an assumed sensitivity parameter in one Surry and one Zion calculation.

A series of six SCDAP/RELAP5/MOD3 calculations from accident initiation through the time of lower head failure were performed for each of the plants as described below.

Surry Calculations

In the Base Case, full loop, in-vessel, and hot leg countercurrent natural circulation flows were considered. Although hot leg countercurrent natural circulation is expected, uncertainties exist with respect to flow magnitude and the effectiveness of heat transfer to ex-vessel structures. Based on those uncertainties, hot leg countercurrent natural circulation was eliminated in Case 2. As a result, Case 2 represents a bounding calculation where ex-vessel heat transfer is minimized (which should reduce the time to lower head failure). Cases 3 through 6 were designed to account for full loop, in-vessel, and hot leg countercurrent natural circulation, along with the potential effects of RCP seal leakage.

Under normal operating conditions, high pressure systems supply cooling water flow to the seals to offset a design leak rate of approximately 3 gpm per RCP. However, the loss of all AC power results in a loss of seal cooling water. Without cooling water, leak rates increase as RCP seal temperatures increase. Leak rates of 21 gpm per RCP have been calculated for intact RCP seals subjected to normal RCS temperatures and pressures.[8]

Leak rates will be higher if one or more of the three seal stages in a Westinghouse RCP fail. The primary factors affecting seal behavior during a TMLB' sequence are high temperature survivability and the potential for hydraulic instability under two-phase flow conditions.[9] High temperature survivability involves the potential for O-ring degradation and blowout. Hydraulic instability is related to evidence suggesting that flashing could cause one or more of the seal stages to pop open. Unfortunately, the prediction of failure of any particular seal stage (which leads to a particular leak rate) is not straightforward. For that reason, a panel of experts was assembled to make a probabilistic determination of RCP leak rates in Westinghouse PWRs during a station blackout.[10] [The resulting expert opinions were used in a comprehensive PRA of the Surry PWR (and four other PWRs in the United States), as documented in NUREG-1150.[11]] For the 'old' O-ring materials assumed to be in both Surry and Zion RCPs, the panel concluded that the highest probability leak rate was 250 gpm per RCP, while the maximum leak rate (at a low probability) was 480 gpm per RCP.[10] (A leak rate of 480 gpm per RCP is consistent with failure of all three seal stages in a Westinghouse RCP.[8])

Based on results from the experts, a leak rate of 21 gpm per RCP was introduced at TMLB' initiation in Cases 3 through 6 to represent leakage associated with the loss of seal cooling. In Case 3, leakage was increased from 21 to 250 gpm at the time water in the RCP reached the saturation temperature to account for potential two-phase instabilities. In Case 4, the maximum leak rate of 480 gpm per RCP was introduced at the time of RCP saturation to provide information on the depressurization rate and its potential impact on HPME. Case 5 was identical to Case 3 except for the treatment of heat transfer from molten materials during relocation to the lower head. In Case 5, it was assumed that molten materials would break up during relocation to provide insights into the effects of repressurization due to debris/coolant heat transfer on the potential for HPME. Case 6 was identical to Case 4 except for the treatment of fuel cladding deformation. In Case 6, the limit on cladding deformation was increased from 2% to 15%.

Zion Calculations

The Zion Base Case was identical to the Surry Base Case in that full loop, in-vessel, and hot leg countercurrent natural circulation flows were considered. Cases 2 and 3 were designed to account for all modes of natural circulation along with the potential effects of RCP seal leakage. In Case 2, seal leaks of 21 gpm per RCP were introduced at TMLB' initiation and then increased to 250 gpm per RCP at the time saturation temperatures were reached. In Case 3, leaks were increased to the maximum rate of 480 gpm per RCP at the time of saturation. Case 4 was identical to the Base Case except that one of two pressurizer PORVs was assumed to stick open at the time core exit temperatures reached 922 K. Zion Case 5 was identical to Surry Case 5 in that breakup with debris/coolant heat transfer during molten relocation was assumed in both cases. And finally, Case 6 was identical to Case 2 except that a code modification was made to limit formation of flow blockages in the fuel assemblies on the core periphery. The code modification was prompted by the fact that core-wide blockages were predicted in many of the Zion calculations, including Case 2. Case 6 was needed because some rod-like geometry would be expected in regions adjacent to the relatively cool downcomer bypass and because the current version of SCDAP/RELAP5/MOD3 does not apply any azimuthal variation to a calculated blockage. The limit imposed through the code modification was based on the minimum area that appeared to be available for flow on the core periphery during the TMI-II accident.

Evaluation of RCS Depressurization-Related Probabilities

The objective of the second and final part of the assessment was to evaluate RCS depressurization-related probabilities. Two specific depressurization issues were considered including (1) a surge line/hot leg failure issue and (2) an RCS pressure at lower head failure issue. Those issues, which were derived from the accident progression event trees developed in NUREG-1150,[11] can be expressed as follows

1. What is the probability that the surge line or hot leg will fail and depressurize the RCS to a low pressure before lower head failure?

2. What are the probabilities of being at a low, intermediate, and high RCS pressure at the time of reactor vessel lower head failure given that an ex-vessel failure does not occur?

(Low, intermediate, and high RCS pressures were taken to be pressures below 1.38 MPa, pressures between 1.38 and 6.89 MPa, and pressures above 6.89 MPa, respectively.)

Probabilities for both RCS depressurization issues were quantified for (1) TMLB' sequences without RCP seal leaks (TMLB' sequences at full system pressure), (2) TMLB' sequences with seal leaks of 250 gpm per RCP, (3) TMLB' sequences with seal leaks of 480 gpm per RCP, and (4) TMLB' sequences with stuck-open/latched-open POPVs. The approach used to quantify the issue probabilities was closely patterned after the expert elicitation method followed in completion of NUREG-1150. In general, the issues were first decomposed (or separated) into parts that were easier to evaluate; endpoint probabilities were established for each part; a distribution was assumed between the end points; and the resulting distributions were recombined to arrive at a probability for the issue.

The use of SCDAP/RELAP5/MOD3 results to establish the endpoint probabilities was the key to this process. However, the endpoints were not simply derived from the calculated results. Instead, the results were used as a basis for further evaluation. In some cases, engineering judgments were made to assess the magnitude of potential uncertainties in the results. In other cases, potential uncertainties were addressed by

completing sensitivity calculations using SCDAP/RELAP5/MOD3. Code uncertainties that were specifically considered centered on those that could influence the potential for RCS depressurization; i.e., those that could affect the relative timing between lower head and ex-vessel failures.

The timing of ex-vessel failures is a function of accumulated creep rupture damage, which is a function of both temperature and pressure. Code-calculated temperatures and pressures were applied to predict the timing of all ex-vessel failures. Uncertainties in oxidation of the core, heat transfer in degraded core geometries, and heat transfer through hot leg countercurrent natural circulation could affect the temperature of steam circulating through the ex-vessel components. Uncertainties in heat transfer during molten relocation and following accumulator injection could affect the pressure. Variations in temperatures and pressures were estimated in an attempt to bound the potential uncertainties. The temperature and pressure variations were then used to calculate possible variations in the timing of ex-vessel failures.

The timing of lower head failure is primarily influenced by uncertainties affecting molten relocation. Currently, failure of the in-core crust through the bottom surface is the only relocation mechanism in SCDAP/RELAP5/MOD3. Uncertainties arise since other relocation possibilities exist including radial spreading of the in-core molten pool to a point of contact with the core former plates, side wall failure of the in-core crucible, and the spilling of molten materials over the top of the in-core crucible as a result of debris falling into the pool from above (i.e., a plunger effect). Engineering judgement was required to estimate possible variations in the timing of lower head failure.

The resulting variations in the timing of potential lower head and ex-vessel failures provided a basis for establishing endpoint probabilities. Distributions between the endpoints were assumed to be linear. Recombining the appropriate distributions was the final step in quantifying the issue probabilities. Complete details associated with this process are documented in NUREG/CR-5949 (Draft).[4]

SCDAP/RELAP5/MOD3 RESULTS

Results from all SCDAP/RELAP5/MOD3 calculations completed in the first part of the assessment are summarized for the Surry and Zion PWRs as follows.

Surry Results

Results listed in Table 1 reflect the predicted response of the Surry PWR. Base Case results indicate creep rupture failures in the surge line and hot leg piping will occur well before failure of the lower head. Without leaks, the RCS pressure is maintained by pressurizer PORV cycling as shown in Figure 1. During each valve cycle, energy is transferred from the core to the surge line and hot leg piping. Hot leg countercurrent natural circulation is established between PORV cycles, which also transfers core decay heat to the hot legs. However, the surge line is heated to a failure condition before the hot legs because it is relatively thin. Given that the steam generator tubes were assumed to be free of defects and deterioration, tube failures would not be expected because the tubes remain relatively cool as shown in Figure 2. Tube temperatures remain relatively cool because of heat transfer from the tubes to the secondary side steam and because the circulating RCS steam loses energy (to the hot leg piping) before reaching the steam generators. Previous studies indicate that the RCS pressure could be reduced from the PORV set point pressure to a value below 1.38 MPa before the predicted lower head failure through either a surge line or hot leg breach.[3]

Table 1. Summary of Surry SCDAP/RELAP5/MOD3 results (in minutes).[a]

Event	Case					
	Base	2	3	4	5	6
Core uncovery	176.7	177.3	189.3	167.7	189.3	167.7
First fuel clad failure	235.5	206.0	220.5	197.3	220.5	205.2
Surge line failure	237.5	215.5	337.2	>463.3	337.2	>396.7
First hot leg failure	258.3	234.3	334.8	>463.3	334.8	>396.7
First fuel melting	278.3	253.0	241.8	234.8	241.8	345.0
First core relocation	480.8	257.8	403.3	426.0	403.3	383.8
Lower head failure	482.0	260.1	405.7	433.0	479.6	389.8
RCS pressure at lower head failure (MPa)[b]	16.0	16.0	8.6	1.4	6.5	1.4

a. A greater-than sign (>) indicates that the event had not occurred by the end of the calculation at the indicated time.

b. Without credit for depressurization that could occur following potential ex-vessel failures.

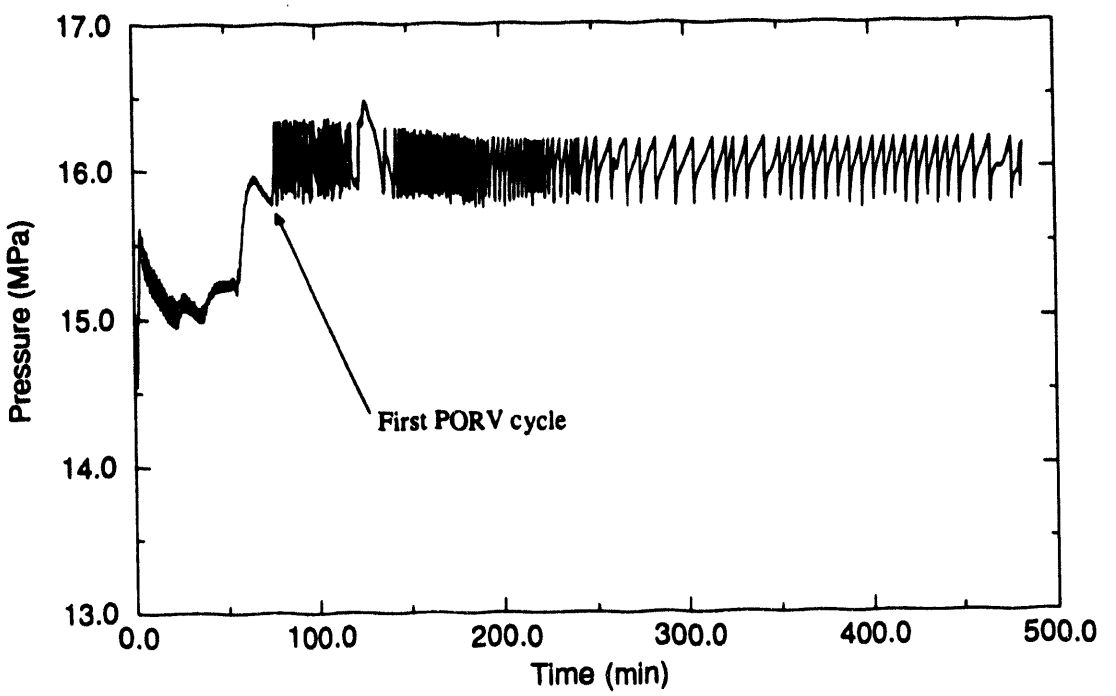


Figure 1. RCS pressure in the Surry Base Case.

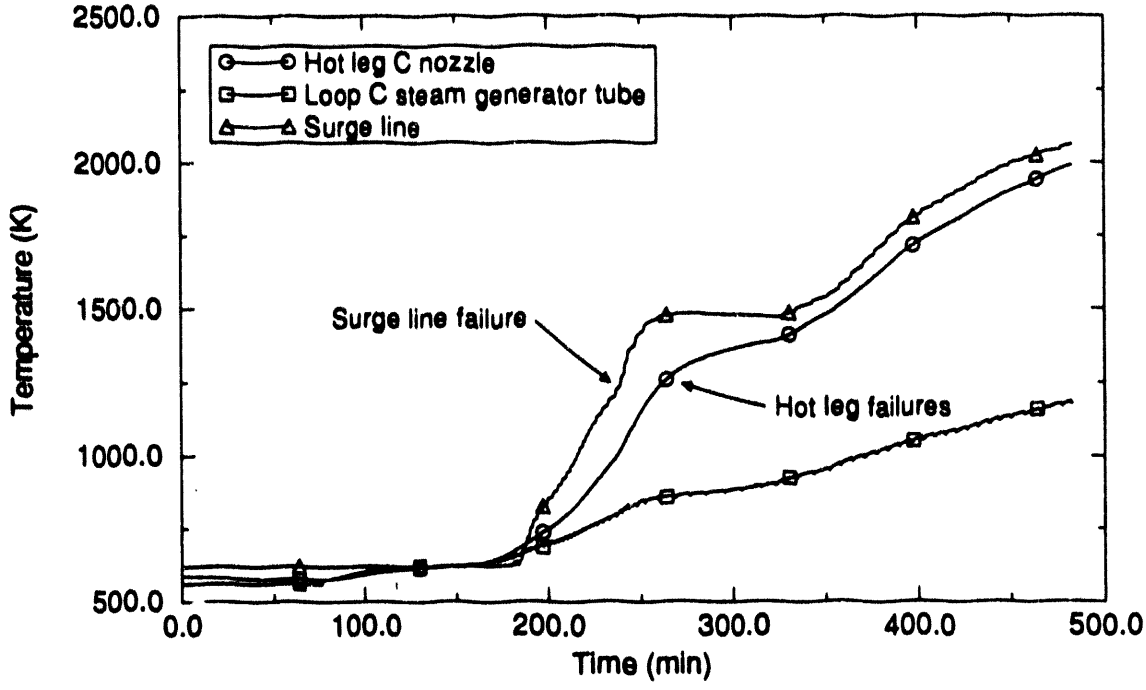


Figure 2. Volume-averaged structure temperatures in the Surry Base Case.

Case 2 results indicate that surge line and hot leg failures can be expected before failure of the lower head even if hot leg countercurrent natural circulation is not established (assuming the RCS is not depressurized by leaks). Hot leg countercurrent natural circulation provides an effective mechanism for the transfer of core decay heat to the ex-vessel piping. If that heat sink is eliminated, heatup of the core and in-vessel structures will accelerate with corresponding increases in steam temperatures. Under those conditions, however, the surge line and hot leg will also be exposed to higher temperatures during each PORV cycle, which led to surge line and hot leg creep ruptures before lower head failure. Without hot leg countercurrent natural circulation, steam generator tube failures would not occur since tube heating is minimal.

The RCS pressure is reduced below the pressurizer PORV set point by the seal leak rates considered in Cases 3 through 6. PORV cycling ends with that pressure reduction as shown for Case 5 in Figure 3. Although surge line heating decreases when PORV cycling ends, ex-vessel heating continues as a result of hot leg countercurrent flow. Results from Cases 3 and 5 indicate that both surge line and hot leg failures would occur before lower head failure if the RCS pressure is reduced below the pressurizer PORV set point by seal leaks of 250 gpm per RCP. Although the hot leg is relatively massive, it would be heated to a failure condition before the surge line because of the decrease in surge line heating and because the hot leg is exposed to the highest-temperature steam leaving the reactor vessel. RCS depressurization through either breach would occur before failure of the lower head. Given that the steam generator tubes are free of defects, the results indicate that failure of the tubes would not be expected with leaks of 250 gpm per RCP.

SCDAP/RELAP5/MOD3 results for Cases 4 and 6 indicate that a lower head failure would be the first breach of the RCS pressure boundary in the Surry PWR if RCP seals leak 480 gpm per pump. The onset of core damage is accelerated by the higher leak rate. However, the higher RCP leak rate also depressurizes the RCS to allow earlier accumulator injection, which can delay further core degradation. The most impor-

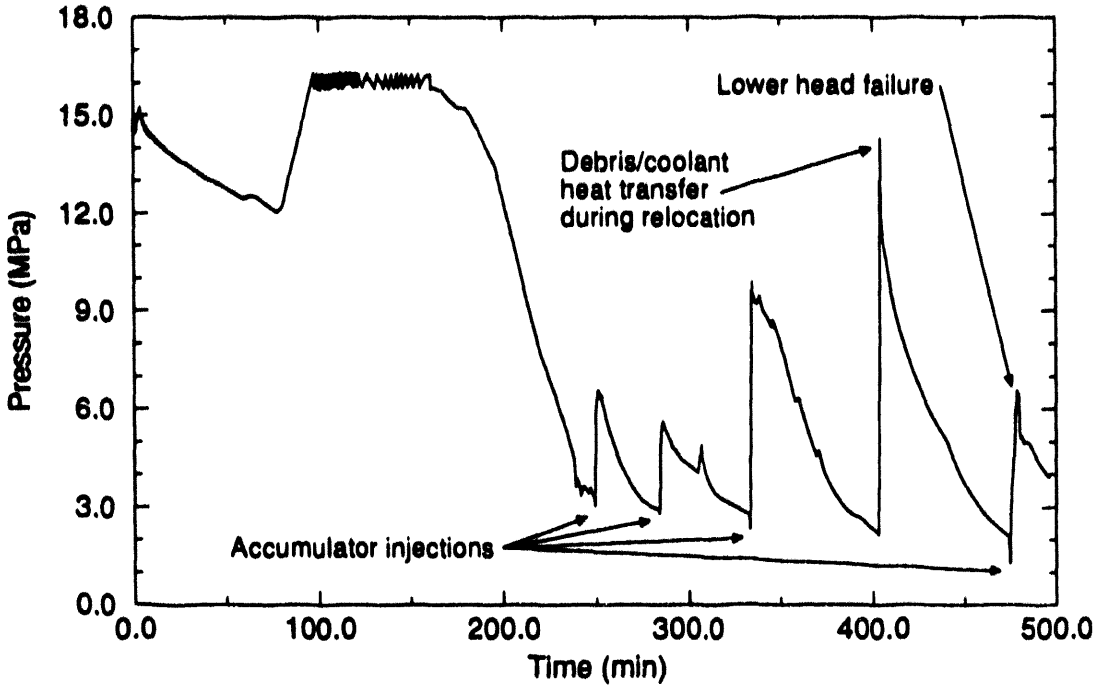


Figure 3. RCS pressure in Surry Case 5.

tant aspect associated with RCP seal leak rates, however, has to do with its effect on ex-vessel heating. The total core decay energy is split into the portion that is deposited in the vessel and ex-vessel structures by circulating steam and the portion that is dissipated through RCP seal leaks. The results indicate that seal leaks of 480 gpm per RCP dissipate a relatively large fraction of core decay energy leaving a relatively small fraction for ex-vessel heating. As indicated in Table 1, ex-vessel failures occur before lower head failure with seal leaks of 250 gpm per RCP while ex-vessel failures do not occur with leaks as high as 480 gpm per RCP.

Debris/coolant heat transfer during molten relocation from the core to the lower head can significantly delay lower head failure. Minimum and maximum debris/coolant heat transfer are the only options currently available in SCDAP/RELAP5/MOD3. With the minimum option, it is assumed that the debris relocates from the core to the lower head in a coherent stream without heat transfer, which results in a rapid lower head thermal attack. With the maximum option, it is assumed that the debris will breakup as a result of interactions with water (and structures) in the lower plenum and lower head. The code then calculates a complete quench of the debris, up to the limit imposed by the amount of coolant available. A large RCS repressurization can result during quench as indicated in Figure 3; however, lower head thermal attack is delayed until the debris reheats. Case 3 and 5 results indicate that the delay in lower head failure could be more than 1 h in the Surry PWR.

Changes in deformation associated with ballooning of the fuel rod cladding can significantly change core damage progression and the time to lower head failure. The core flow resistance in Case 6 was relatively high with a ballooning deformation limit of 15%. As a result, the core was reflooded from the top down by an accumulator injection that was forced through the core bypass. A boiloff was then required before the core could reach molten temperatures. The accumulators were essentially emptied during the

reflood, which eliminated the possibility of effective cooling during the subsequent reheating. A relatively large relocation of approximately 44370 kg of molten UO_2 occurred as a result. With deformation limit of 2% in Case 4, periodic accumulator injection provided only partial cooling of the core hot spots. However, the partial cooling occurred over a prolonged period and was sufficient to delay relocation, which consisted of about 12940 kg of molten UO_2. The delay in relocation produced a corresponding delay in lower head failure of 43.2 minutes (compared to the higher deformation case).

Zion Results

Results listed in Table 2 reflect the predicted response of the Zion PWR. The Zion Base Case results are similar to the Surry Base Case results in that surge line and hot leg failures were predicted before failure of the lower head. That similarity is due to the fact that ex-vessel heating was found to be approximately equal in the two plants. Ex-vessel heating is approximately equal since the plants have the same core power per loop with comparable heat sinks (the hot leg and steam generator geometries are similar and the steam generator relief valve set point pressures are the same). As a result, surge line and hot leg failures occurred at about the same time in Surry and Zion as indicated by the Base Case results in Tables 1 and 2, respectively. However, lower head failure in the Zion PWR was relatively early because Zion has a higher decay power density. Nevertheless, Table 2 results indicate a substantial margin between ex-vessel and vessel failures in spite of the relatively early lower head failure.

Table 2. Summary of Zion SCDAP/RELAP5/MOD3 results (in minutes).[a]

	Case					
Event	Base	2	3	4	5	6
Core uncovery	185.7	184.8	173.0	185.7	184.8	184.8
First fuel clad failure	227.5	213.0	200.2	221.8	213.0	213.0
Surge line failure	235.3	>333.3	>333.3	>258.3	>333.3	>333.3
First hot leg failure	258.0	>333.3	>333.3	>258.3	>333.3	>333.3
First fuel melting	287.8	239.3	241.3	245.5	239.3	239.7
First core relocation	319.7	298.0	309.7	245.5	298.0	316.3
Lower head failure	323.2	302.8	317.8	254.3	326.3	321.5
RCS pressure at lower head failure (MPa)[b]	16.0	3.7	2.1	2.7	9.0	3.3

a. A greater-than sign (>) indicates that the event had not occurred by the end of the calculation at the indicated time.

b. Without credit for depressurization that could occur following potential ex-vessel failures.

SCDAP/RELAP5/MOD3 results for Cases 2, 5, and 6 indicate that a lower head failure would be the first breach of the RCS pressure boundary in the Zion PWR if each RCP seal leaks 250 gpm. Thick crusts

were formed across the bottom of the core in those cases. The associated flow blockage was sufficient to prevent effective core penetration and cooling by injected accumulator water. (Cooling by accumulator water was enhanced to a degree by limiting crust formation on the core periphery in Case 6. An 18.7 minute delay in lower head failure resulted. However, a lower head failure was still the first breach of the RCS pressure boundary.) Without effective penetration and cooling by accumulator water, RCS repressurization following injection was minimal as shown in Figure 4. Relative to the Surry calculations, the lack of RCS repressurization reduced ex-vessel creep rupture damage. In addition, ineffective core cooling combined with a relatively high decay power density led to early molten relocation and lower head failure before ex-vessel failures in the Zion PWR.

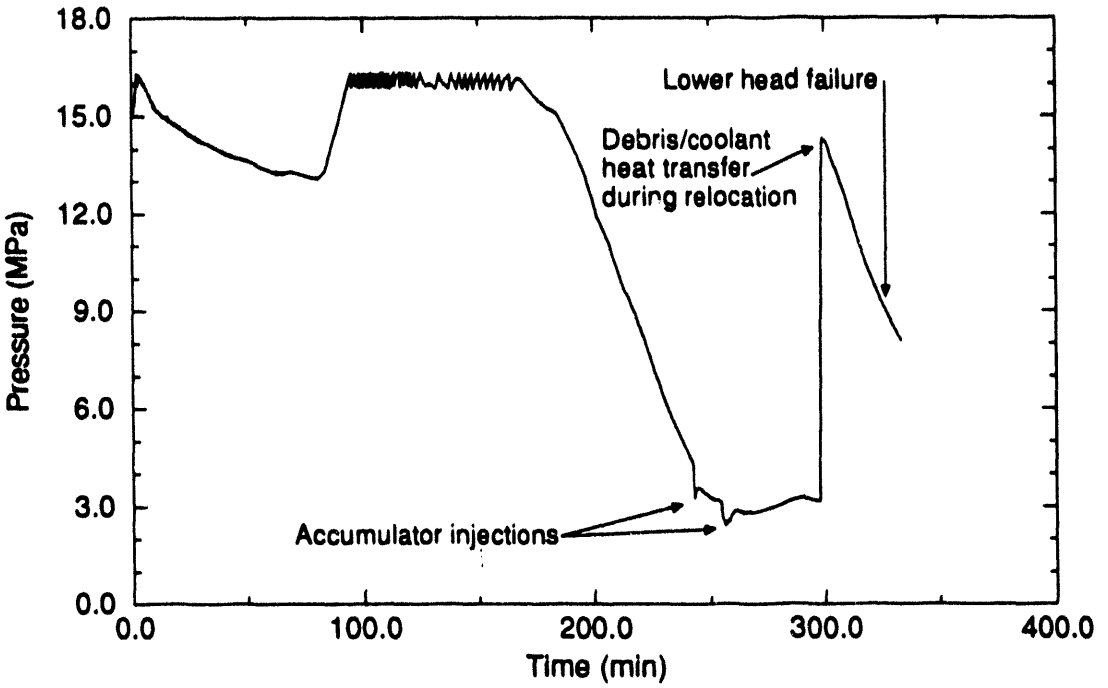
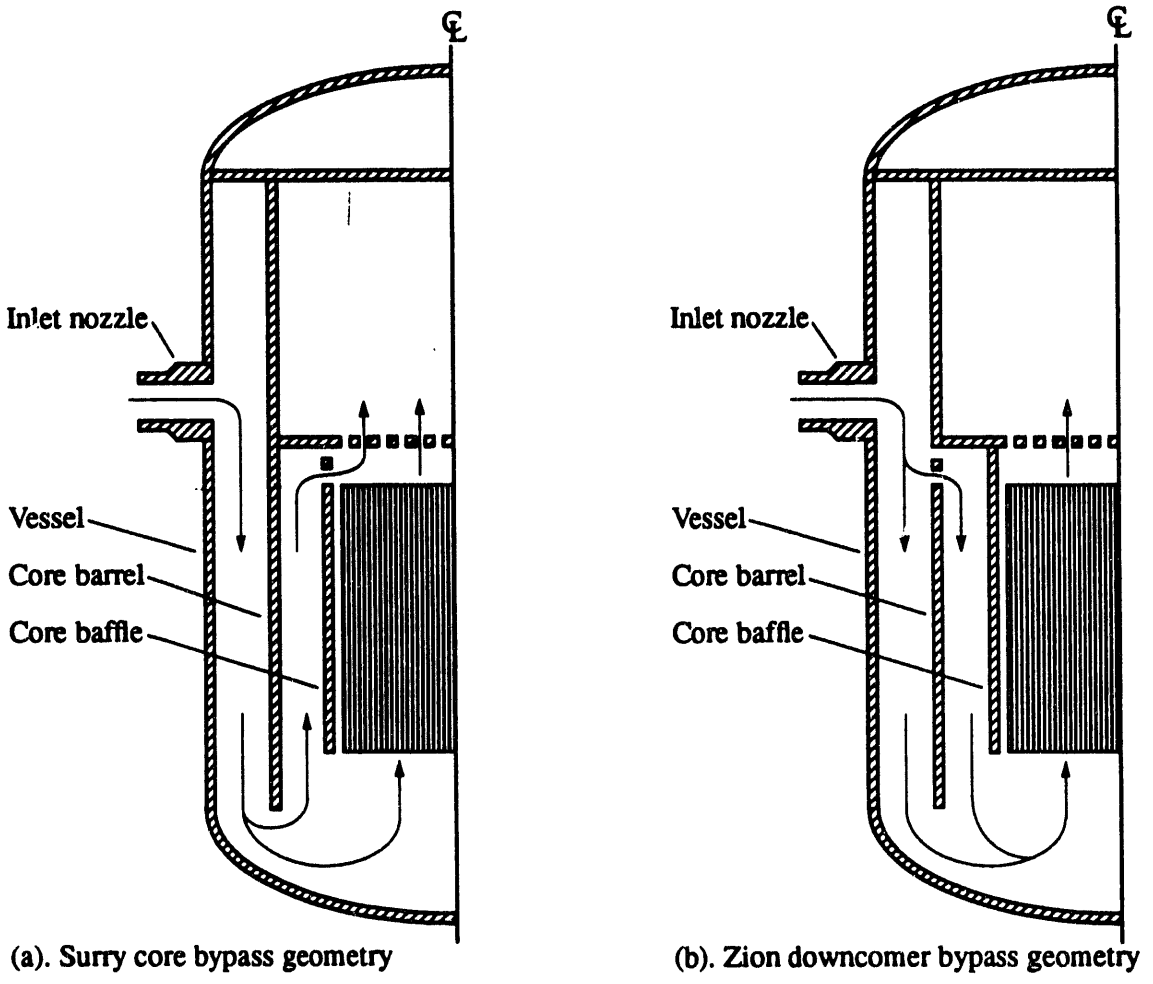


Figure 4. RCS pressure in Zion Case 5.

The previously discussed Surry results are distinctly different. Specifically, the first RCS pressure boundary breach in Surry was predicted to be an ex-vessel failure if each RCP seal leaks 250 gpm. A limited investigation was performed to determine why the Surry and Zion results differed. The core decay power density and the bypass geometry of the Zion PWR appear to be the most important factors. A sensitivity calculation was completed where the Zion decay power density was scaled back to the Surry PWR level. The results indicated that lower head failure in Zion could be delayed 67.2 minutes through that power reduction.

The bypass geometry determines the direction of flow in the region between the core barrel and core baffle. In Surry (and some other Westinghouse PWRs), holes in the top of the core baffle plates just below the upper core plate result in a core bypass flow as shown in Figure 5. Most of the flow goes upward through the fuel assemblies while a fraction bypasses the core through the baffle plate holes. In Zion (and



(a). Surry core bypass geometry

(b). Zion downcomer bypass geometry

Figure 5. Normal flow patterns for Surry core bypass and Zion downcomer bypass geometries.

some other Westinghouse PWRs), holes in the core barrel just below the upper core plate result in a downcomer bypass flow, also shown in the figure. Most of the flow goes through the downcomer annulus while a fraction bypasses the downcomer through the core barrel holes.

The difference between core bypass and downcomer bypass flow geometries in insignificant under normal operating conditions. However, the bypass flow geometry can influence in-vessel natural circulation and core degradation during severe reactor accidents. In-vessel natural circulation occurs when the hottest steam in the center part of the core rises into the upper plenum. Heat transfer to upper plenum structures cools the steam. The cooler steam tends to sink along the outer edges of the upper plenum and the core where it is reheated to complete the circulation cell. The core bypass geometry provides a relatively cool return flow path for the steam. In addition, the core baffle plates direct (at least) a portion of the natural circulation flow to the bottom of the core. Since natural circulation flow in the area between the core barrel and baffle is precluded in plants with a downcomer bypass geometry, return flow must progress downward through the outer-most fuel assemblies. Most of that flow will begin to rise due to heating before reaching the bottom of the assemblies, resulting in a semi-stagnant zone in the lower portions of the core.

The bypass geometry is also important with respect to the progression of core degradation. Specifically, a core bypass geometry provides an alternate flow path for accumulator water. Accumulator water is injected into the cold legs and flows into the lower head. Depending on the extent of core blockage, some amount of injected water will be forced into the core bypass. In cases with extensive core blockage (i.e., Surry Case 6), accumulator water can fill the core bypass and spill into the top of the core through the holes in the core baffle plates. Core cooling is limited to accumulator reflooding from the bottom in plants with downcomer bypass geometries. Cooling by accumulator water is relatively ineffective if blockage forms at the bottom of the core, as predicted in Zion Cases 2, 5, and 6. A sensitivity calculation was completed where the Zion bypass flow geometry was changed to match the core bypass geometry of the Surry PWR. The results indicated that failure of the Zion reactor vessel lower head could be delayed 72.2 minutes by the bypass geometry change.

The lower head failure delays associated with changes in decay power density and bypass geometries provided additional time for accumulating creep rupture damage in the Zion ex-vessel structures. However, when considered separately, the delays did not provide sufficient time to reach ex-vessel failures. Additional calculations could be performed to evaluate the combined effects of the Surry decay power density and core bypass geometry with respect to RCS pressure boundary failures in the Zion PWR. The results from such a calculation could be useful in assessing the importance of decay power density and bypass geometry in the current Zion SCDAP/RELAP5/MOD3 results.

SCDAP/RELAP5/MOD3 results for Case 3 indicate that a lower head failure will be the first breach of the RCS pressure boundary in the Zion PWR if each RCP seal leaks 480 gpm. In that case, the total core decay energy is split into a portion deposited in the vessel and ex-vessel structures by circulating steam and a portion dissipated through RCP seal leaks. As in the Surry calculations, the results indicate that the fraction associated with ex-vessel heating is too small to induce an ex-vessel failure before failure of the lower head.

Debris/coolant heat transfer during molten relocation can significantly delay failure of the lower head. Without heat transfer, hot debris can begin a thermal attack as soon as it reaches the lower head. A large RCS repressurization can result if the debris is quenched during relocation as indicated in Figure 4. However, lower head thermal attack is delayed while the debris reheats. Case 2 and 5 results from Table 2 indicate that the delay in lower head failure could be approximately 23.5 minutes in the Zion PWR. Compared to Surry, the delay due to debris/coolant heat transfer is relatively small because the decay power density is higher in the Zion PWR.

Results for Case 4 listed in Table 2 indicate that a lower head failure will be the first breach of the RCS pressure boundary if one of the pressurizer PORVs sticks open at the time core exit temperatures reach 922 K. The RCS pressure was reduced to the initial accumulator pressure approximately 33.5 minutes after the PORV opened. By that time, however, a relatively thick core-wide crust had formed at an elevation of about 1 m above the bottom of the fuel assemblies. Only two relatively small accumulator injections were predicted. The injections were limited by the restriction to steam flow created by the core-wide crust. And with a downcomer bypass geometry, there was no other path for venting excess steam. As a result, only partial cooling of the lower part of the core occurred while the regions above the crust heated to a molten condition with subsequent relocation into the lower head. Flow through the open PORV did produce some surge line heating during this process. However, some of the core decay energy was also dissipated by hot leg countercurrent natural circulation in the non-pressurizer loops. Consequently, the combination of PORV flow and natural circulation heating did not induce ex-vessel failures before failure of the lower head in this case.

RCS DEPRESSURIZATION-RELATED PROBABILITIES

Probabilities for both RCS depressurization issues were developed for four different scenarios: (1) TMLB' sequences without RCP seal leaks (TMLB' sequences at full system pressure), (2) TMLB' sequences with seal leaks of 250 gpm per RCP, (3) TMLB' sequences with seal leaks of 480 gpm per RCP, and (4) TMLB' sequences with either stuck-open or latched-open PORVs. Therefore, the following probabilities are conditional on the occurrence of the specified scenarios.

Surry Depressurization Probabilities

Probabilities for Scenarios 1 through 3 were primarily based on SCDAP/RELAP5/MOD3 results for the Surry PWR as calculated in the first part of this assessment. Specifically, Scenario 1 was based on results from the Base Case and Case 2, Scenario 2 was based on results from Cases 3 and 5, and Scenario 3 was based on results from Cases 4 and 6. A SCDAP/RELAP5/MOD3 analysis of intentional depressurization of the Surry PWR[2] was used to establish probabilities for Scenario 4. However, none of the code results were used directly. Instead, sensitivity calculations were performed and engineering judgment was applied to evaluate the effects of potential uncertainties as previously discussed.

Surge Line/Hot Leg Failure Issue

An example of the process used to address potential uncertainties and quantify probabilities for the surge line/hot leg failure issue can be described relative to Figure 6. Cumulative distributions for RCS depressurization (through an ex-vessel failure) and lower head failure for Surry Scenario 2 are shown in the figure as a function of the calculated time of lower head failure. The distributions were based on calculated results and potential uncertainties in those results. Specifically, RCS depressurization is a function of the ex-vessel pressures and temperatures that drive creep rupture. Engineering judgement was applied to estimate possible variations in the calculated pressures and temperatures. The estimated variations in pressure and temperature were then used in sensitivity calculations to determine a range of possible ex-vessel failure times. Probabilities were assigned to the failure range to establish the illustrated distribution. Uncertainties in the calculated lower head failure time included the effects of debris/coolant heat transfer as well as the potential for alternate relocation mechanisms that are not currently treated by SCDAP/RELAP5/MOD3. As indicated in the figure, the resulting distributions have only a small region of overlap. Therefore, a high probability for RCS depressurization before lower head failure is estimated in this scenario.

Probabilities for all scenarios in the surge line/hot leg failure issue in the Surry PWR were developed similarly. The results are listed in Table 3. As indicated in the table, a probability of 0.98 was assigned to Scenario 1. In that case, the RCS pressure is maintained at the PORV set point through continuous valve cycling. Steam flow associated with the PORV cycling heated the surge line at high pressure. Calculated results indicated that creep rupture failure of the surge line would occur well ahead of lower head failure. After accounting for uncertainties in the results, it was concluded that there was a small fraction of the time where lower head failure could have occurred before RCS depressurization through the surge line breach. That uncertainty is reflected in the listed probability.

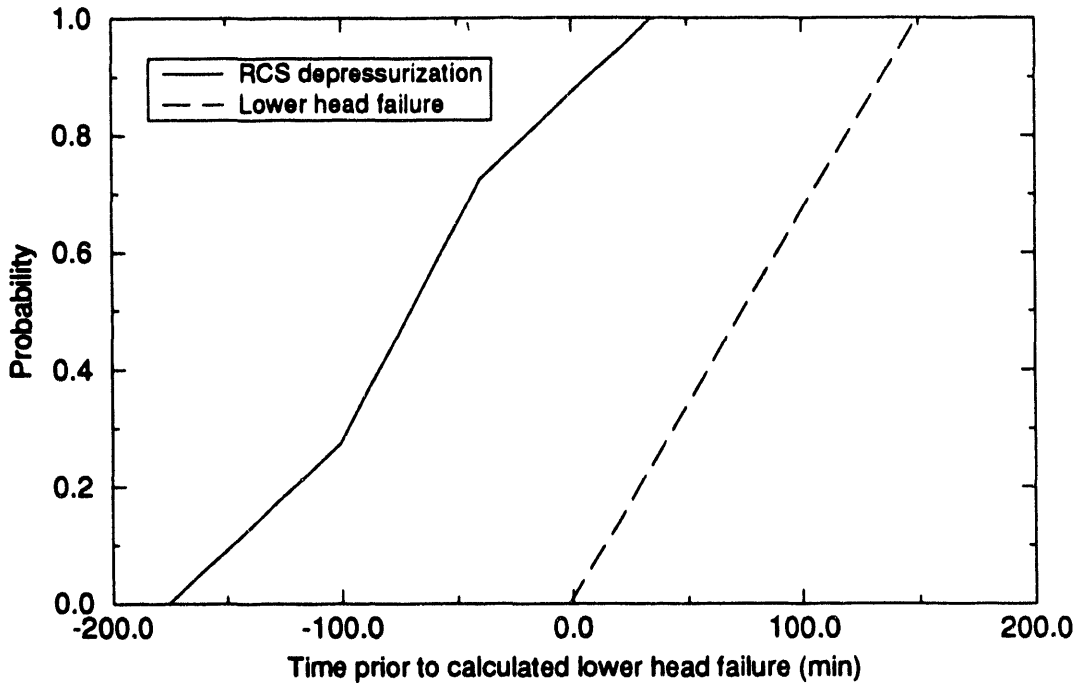


Figure 6. Probability of the surge line/hot leg failure issue given the occurrence of TMLB' sequences with seal leaks of 250 gpm per RCP in the Surry PWR.

Table 3. Probabilities for a surge line or hot leg failure with RCS depressurization to 1.38 MPa (or less) before lower head failure given the occurrence of the specified scenarios in the Surry PWR.

Scenario	Probability
1. TMLB' sequences without RCP seal leaks	0.98
2. TMLB' sequences with seal leaks of 250 gpm per RCP	0.98
3. TMLB' sequences with seal leaks of 480 gpm per RCP	0.0
4. TMLB' sequences with stuck-open/latched-open PORVs	1.0

Surge line heating was similar in TMLB' sequences with either stuck-open or latched-open PORVs. In that case, however, flow through the surge line was continuous, which significantly reduced the RCS pressure. By the time high surge line temperatures were reached (and before there was any potential for lower head failure), the RCS pressure was near the containment pressure. Because creep rupture is a function of both temperature and pressure and because the pressure was low, surge line failure occurred relatively late in the transient. After uncertainties were considered, however, it was concluded that there was only a very small fraction of the time where the lower head could have failed before the surge line. The fraction was small enough to justify a probability of 1.0 as listed in Table 3.

It should be recognized that the PORVs could be latched open or could stick open at virtually any time during a TMLB' sequence. In this assessment, however, it was assumed that probabilities for the surge line/ hot leg failure issue would not be significantly altered by the PORV opening time. Furthermore, probabilities for both latched-open and stuck-open conditions were assumed to be equivalent. Those assumptions were developed as follows.

SCDAP/RELAP5/MOD3 results for implementation of the late depressurization strategy indicate that the surge line would fail before failure of the lower head if plant operators latch the PORVs open at the time core exit temperatures reach 922 K.[2] Results from previous analyses indicated the same result if the PORVs are latched open at the relatively early time of steam generator dryout.[1] Based on current understanding and the available calculations, there is no reason to expect any difference in results applicable to this issue if any other earlier times were selected. In other words, the PORVs could be latched open before the time core exit temperatures reach 922 K without impacting the probability given in Table 3.

If the PORVs are latched open at some time after core exit temperatures reach 922 K, RCS pressure control through PORV cycling would be extended. Results from the Base Case indicate that PORV cycling subjects the surge line to heating at high pressure. If the heating is allowed to continue (i.e., if it is not interrupted by latching the PORVs open), surge line failure would occur more than 240 minutes ahead of lower head failure. If the PORVs are latched open before surge line failure (i.e., before sufficient heating at high pressure has transpired), some creep rupture damage will be accumulated. The subsequent RCS pressure reduction would result in cladding ruptures and the injection of accumulator water. High temperature steam from the subsequent boiloff and the energy associated with oxidation of the inner surfaces of the ruptured cladding would be deposited in the surge line. Surge line failure, as a result of the heating associated with boiloff and oxidation, would be expected well ahead of lower head failure as a result. That expectation is based on the fact that some surge line creep damage will have accumulated and the fact that the surge line response to the subsequent boiloff would not be substantially different than the response associated with late depressurization (where the surge line failed before the lower head). Therefore, based on current understanding and the available calculations, the probability given in Table 3 would not be significantly altered by the time at which the PORVs are latched open.

Similar reasoning applies to the time at which the PORVs could stick open. In fact, there is no basis to differentiate between a latched-open condition and a stuck-open condition, given that the operators could latch the PORVs open at any time. Therefore, the probabilities for both latched-open and stuck-open conditions were assumed to be equivalent.

In Scenarios 2 and 3, the total core decay energy was split between heat that was transferred to the hot leg piping by countercurrent natural circulation and the energy dissipated through the RCP seal leaks. With seal leaks of 250 gpm per RCP, countercurrent natural circulation was sufficient to heat the hot legs to a failure condition before lower head failure. After accounting for uncertainties in the calculated results, it was concluded that there was a small fraction of the time where lower head failure could have occurred before RCS depressurization through the hot leg breach (as indicated by the overlap of distributions shown in Figure 6). On that basis, a probability of 0.98 was assigned. When the seal leaks were increased to 480 gpm per RCP, however, hot leg heating was reduced because a larger fraction of the decay energy was lost through the RCP seal leaks. Specifically, hot leg (and surge line) temperatures associated with seal leaks of 480 gpm per RCP were significantly cooler than the corresponding temperatures for seal leaks of 250 gpm per RCP. As a result, the hot legs were not heated to a failure condition before lower head failure. Uncertainties in hot leg heating and the lower head failure time were not large enough to alter that result. Therefore, a probability of 0.0 was assigned to Scenario 3 as indicated in Table 3.

RCS Pressure at Lower Head Failure Issue

An example of the process used to address potential uncertainties and quantify probabilities for the RCS pressure at lower head failure issue can be described relative to Figure 7. Specifically, the uncertainty band for lower head failure was overlaid onto the RCS pressure response of Surry Case 5. (Note that an extrapolation of the RCS pressure was required in this case as indicated by the dashed line. Since core relocation occurred at approximately 402 minutes and since the accumulators emptied at about 480 minutes, the extrapolation did not have to account for a potential repressurization. Therefore, the extrapolated pressure decay could be estimated based on rates of calculated decay.) Based on the horizontal lines at the low and high pressure break points, it is clear that a lower head failure could have occurred at high, intermediate, or low RCS pressure in this case. It was assumed that the probabilities for failure at high, intermediate, and low RCS pressures were directly proportional to the fraction of the estimated failure band that corresponded to each pressure range.

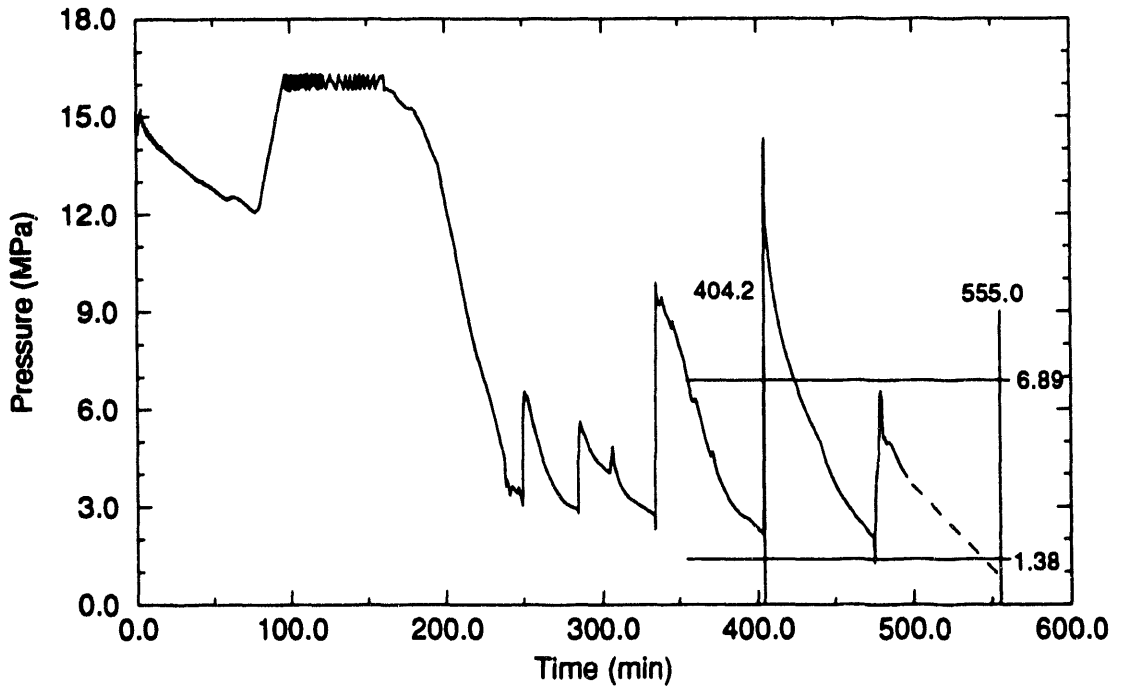


Figure 7. Pressure used to quantify RCS pressure at lower head failure issue probabilities in Surry Case 5.

Probabilities for all scenarios in the RCS pressure at lower head failure issue for the Surry PWR were developed similarly. The results are listed in Table 4. As indicated, probabilities are given without credit for RCS depressurization following any potential ex-vessel piping failure because the RCS pressure response associated with ex-vessel failures was addressed in the surge line/hot leg failure issue.

For Scenario 1, the RCS pressure was controlled through the time of lower head failure by continuous PORV cycling between the opening and closing set points of 16.2 and 15.7 MPa, respectively. Without credit for ex-vessel failures, the RCS pressure at lower head failure would obviously be in the high pres-

Table 4. Probabilities for being at low, intermediate, and high RCS pressure at the time of lower head failure given the occurrence of the specified scenarios without ex-vessel failures in the Surry PWR.

Scenario	Probability, at lower head failure, for		
	High RCS pressure (> 6.89 MPa)	Intermediate RCS pressure (1.38 - 6.89 MPa)	Low RCS pressure (< 1.38 MPa)
1. TMLB' sequences without RCP seal leaks	1.0	0.0	0.0
2. TMLB' sequences with seal leaks of 250 gpm per RCP	0.21	0.75	0.04
3. TMLB' sequences with seal leaks of 480 gpm per RCP	0.13	0.40	0.47
4. TMLB' sequences with stuck-open/ latched-open PORVs	0.0	0.0	1.0

sure range, and probabilities were assigned as appropriate. Those results were reversed by the continuous flow associated with TMLB' sequences with either stuck-open or latched-open PORVs. Specifically, it was concluded that continuous flow through the Surry PORVs was sufficient to depressurize the RCS to 1.38 MPa (or less) well ahead of the time of lower head failure. Uncertainties in the failure time and the potential for repressurization (through accumulator injection and/or debris/coolant heat transfer) were considered before assigning a probability of 1.0 to the low pressure range.

As previously discussed, the PORVs could be latched open or they could stick open at virtually any time during a TMLB' sequence. However, the time at which the PORVs are opened is of little consequence with respect to this issue as follows. The RCS would depressurize to 1.38 MPa (or less) through the PORVs if the valves were opened at any time before failure of the in-core crust. That was verified by SCDAP/RELAP5 calculations for the PORV opening times associated with implementation of both early and late depressurization strategies in the Surry PWR.[1,2] Results from the RCP seal leak cases indicate that accumulator injections can cool the in-core crust and effectively delay molten relocation in Surry. Therefore, if the PORVs were opened relatively early, the RCS would be depressurized. If the PORVs were opened near the time of crust failure, accumulator injections would cool the in-core crust, which would delay crust failure and molten relocation. After the accumulator water was boiled away (and vented through the open PORVs), crust heatup and failure would be expected at low RCS pressure.

If the PORVs were opened at the time of crust failure, accumulator injections may or may not effectively cool molten materials as they relocate to the lower head. As a result, lower head failure could occur at a high RCS pressure. However, the probabilities of the operator latching the PORVs open and the PORVs sticking open within this small time window were assumed to be negligible. This assumption was based on the idea that if an operator were going to open the PORVs to depressurize, that action would take place well ahead of any molten relocation. In other words, if the operator decided to depressurize, a reasonable amount of time would be allotted to do so. The conditions that would cause the PORVs to stick open are primarily associated with operation of the valves at temperatures above design conditions. The PORVs would see many cycles at elevated temperatures before the time of crust failure. If the PORVs were going

to stick open as a result of the adverse conditions, it would seem most likely for that failure to occur during one of the many cycles long before failure of the crust. Therefore, the time at which the PORVs are opened would not significantly impact the probabilities listed in Table 4 because the probability of the PORVs opening at the time of crust failure was assumed to be small.

Seal leaks of 250 and 480 gpm per RCP were sufficient to reduce the Surry RCS pressure well below the PORV set point to pressures that allowed accumulator injection. An RCS repressurization followed each injection due to vaporization of water during core cooling. A period of time elapsed between the injections while the excess vapor was discharged through RCP seal leaks. RCS repressurization was also calculated during relocation to the lower head as a result of heat transfer between the molten debris and coolant. Those mechanisms for repressurization provided the potential for intermediate and high pressures in Scenarios 2 and 3 (as illustrated in Figure 7).

For seal leaks of 250 gpm per RCP, lower head failures could have occurred at high, intermediate, and low RCS pressures 21%, 75%, and 4% of the time, respectively. Assuming that the probabilities are proportional to the fraction of each lower head failure period that corresponded to the specified pressure ranges, probabilities of 0.21, 0.75, and 0.04 were assigned to the high, intermediate, and low pressure ranges, respectively, as indicated in Table 4. Probabilities of 0.13, 0.40, and 0.47 were estimated for high, intermediate, and low pressure ranges, respectively, for seal leaks of 480 gpm per RCP.

Zion Depressurization Probabilities

Probabilities were primarily based on SCDAP/RELAP5/MOD3 results for the Zion PWR as calculated in the first part of this assessment. Specifically, Scenario 1 was based on results from the Base Case, Scenario 2 was based on results from Cases 2, 5, and 6, Scenario 3 was based on results from Case 3, and Scenario 4 was based on results from Case 4.

Surge Line/Hot Leg Failure Issue

Resulting probabilities for the surge line/hot leg failure issue in the Zion PWR are listed in Table 5. As indicated in the table, a probability of 1.0 was assigned to Scenario 1. In that case, natural circulation of steam and steam flow through cycling PORVs led to surge line and hot leg failures well before lower head failure. After accounting for uncertainties in the calculated results, it was concluded that a surge line or hot leg failure could have depressurized the RCS before failure of the lower head.

Table 5. Probabilities for a surge line or hot leg failure with RCS depressurization to 1.38 MPa (or less) before lower head failure given the occurrence of the specified scenarios in the Zion PWR.

Scenario	Probability
1. TMLB' sequences without RCP seal leaks	1.0
2. TMLB' sequences with seal leaks of 250 gpm per RCP	0.02
3. TMLB' sequences with seal leaks of 480 gpm per RCP	0.0
4. TMLB' sequences with a stuck-open/latched-open PORV	0.0

Ex-vessel failures were not calculated before lower head failures in cases representing Scenarios 2, 3, and 4. After accounting for uncertainties in the code results, it was concluded that there was only a low probability for being at or below 1.38 MPa at the time of lower head failure as a result of accident-induced ex-vessel failures. For that reason, surge line/hot leg failure issue probabilities of 0.02, 0.0, and 0.0 were assigned to Scenarios 2, 3, and 4, respectively.

RCS Pressure at Lower Head Failure Issue

Resulting probabilities for the RCS pressure at lower head failure issue in the Zion PWR are listed in Table 6. Without credit for ex-vessel failures, the RCS pressure would be in the high pressure range at the time of lower head failure in Scenario 1. Therefore, a probability of 1.0 was assigned as indicated in the table.

Table 6. Probabilities for being at low, intermediate, and high RCS pressure at the time of lower head failure given the occurrence of the specified scenarios without ex-vessel failures in the Zion PWR.

Scenario	Probability, at lower head failure, for		
	High RCS pressure (> 6.89 MPa)	Intermediate RCS pressure (1.38 - 6.89 MPa)	Low RCS pressure (< 1.38 MPa)
1. TMLB' sequences without RCP seal leaks	1.0	0.0	0.0
2. TMLB' sequences with seal leaks of 250 gpm per RCP	0.32	0.68	0.0
3. TMLB' sequences with seal leaks of 480 gpm per RCP	0.50	0.50	0.0
4. TMLB' sequences with a stuck-open/ latched-open PORV	0.28	0.72	0.0

RCP seal leaks and a stuck-open/latched-open PORV were sufficient to reduce the RCS pressure in the Zion PWR to the initial accumulator pressure of approximately 4.2 MPa. However, core-wide crusts were predicted in each of the cases (representing Scenarios 2, 3, and 4). The early formation of the core-wide crusts was attributed to the relatively high decay power density in the Zion PWR. Those core-wide crusts in combination with a downcomer bypass geometry led to protracted periods of small accumulator injections followed by slow depressurization through seal leaks or the open PORV. As a result, the RCS pressure would be expected to be in the high and intermediate pressure ranges at the time of lower head failure as indicated by the corresponding probabilities given in Table 6.

CONCLUSIONS

There is a low probability for HPME in the Surry PWR during station blackout accidents based on current SCDAP/RELAP5/MOD3 calculations and an assessment of the potential uncertainties in the associated results. Specifically, four separate station blackout scenarios were considered including (1) TMLB' sequences without RCP seal leaks (TMLB' sequences at full system pressure), (2) TMLB' sequences with seal leaks of 250 gpm per RCP, (3) TMLB' sequences with seal leaks of 480 gpm per RCP, and (4) TMLB' sequences with stuck-open/latched-open PORVs. In Scenarios 1, 2, and 4, natural circulation and flow through the PORVs led to surge line and/or hot leg failures before failure of the lower head. After accounting for uncertainties in the calculated results, it was concluded that RCS pressure reduction below 1.38 MPa would occur through the ex-vessel breach before lower head failure with a high probability. Specifically, probabilities for a surge line or hot leg failure with RCS depressurization below 1.38 MPa before lower head failure were assigned values of 0.98, 0.98, and 1.0, given the occurrence of Scenarios 1, 2, and 4, respectively.

In Surry Scenario 3, an ex-vessel failure was not calculated before lower head failure. For that reason, the probability of a surge line or hot leg failure with RCS depressurization below 1.38 MPa before lower head failure was assigned a value of 0.0. However, the probability of being at or below 1.38 MPa at the time of lower head failure without an ex-vessel failure was estimated to be 0.47. In addition, the probability of seal leaks as large as 480 gpm per RCP is very small.[10] In other words, the results associated with Scenario 3 would be relatively unlikely. Therefore, there is a low probability for HPME in the Surry PWR based on these considerations for Scenario 3 and the surge line/hot leg failure issue probabilities for Scenarios 1, 2, and 4.

There is a low probability for HPME in the Zion PWR during station blackout accidents that progress at without RCS leaks (i.e., Scenario 1). Specifically, SCDAP/RELAP5/MOD3 results for the Zion Base Case indicate that surge line and hot leg failures will depressurize the RCS to 1.38 MPa (or less) well before failure of the lower head. After code uncertainties were considered, it was concluded that the probability for such depressurization was essentially 1.0.

A probability for HPME in the Zion PWR exists for station blackout accidents that progress at reduced RCS pressures due to RCP seal leaks, stuck-open/latched-open PORVs, etc. Specifically, the first breach of the RCS pressure boundary was calculated to be a lower head failure in Scenarios 2, 3, and 4. After code uncertainties were considered, surge line/hot leg failure issue probabilities of 0.02, 0.0 and 0.0 were assigned to Scenarios 2, 3, and 4, respectively. In each case, however, the assumed leak was sufficient to reduce the RCS pressure significantly below the PORV set point range of 15.7 to 16.2 MPa. In fact, calculated pressures at the time of lower head failure were in the range of 2 to 4 MPa with the exception of a limiting calculation for debris/coolant heat transfer (see Table 2). However, a probability for HPME in reduced pressure scenarios exists based on the previously specified criteria of being at or below 1.38 MPa at the time of lower head failure. The potential for containment failure as a result of DCH associated with melt ejection in those scenarios was considered by the DCH Working Group.[5]

The potential for RCS depressurization in the Surry and Zion PWRs was not affected by steam generator tube failures. RCS depressurization to the secondary relief valve set point pressure of approximately 7.1 MPa could occur given failure of one or more steam generator tubes. However, tube failures were not predicted in any of the calculations performed because the tubes remain relatively cool as a result of heat transfer (from the tubes) to the secondary side steam and because the circulating RCS steam loses energy (to the hot leg piping) before reaching the steam generators. It is important to note that steam generator

tubes were assumed to be free of defects and deterioration in all calculations. Therefore, this conclusion should not be extended to operating PWRs since some degradation that could potentially affect tube integrity accumulates over plant life. Furthermore, the analysis of any potential tube degradation was outside the scope of this assessment.

This assessment was based on detailed SCDAP/RELAP5/MOD3 analyses to determine the RCS response of the Surry and Zion PWRs during a severe reactor accident. Therefore, the conclusions of this assessment are specific to the Surry and Zion PWRs. Although an evaluation of the applicability of the results to other plants was outside the scope of this program, some of the factors that would have to be considered include pressurizer PORV capacity; decay heat level; accumulator capacity and initial pressure; steam generator size, type, and initial liquid inventory; and hot leg, surge line, and reactor vessel geometries. Those factors are considered important because they could influence the core damage progression and the natural circulation of steam throughout the plant, which would affect the timing of RCS pressure boundary failures. A plant-specific understanding of those factors and their influence on transient behavior would be required to extend the results to other PWRs.

REFERENCES

1. D. J. Hanson et al., *Depressurization as an Accident Management Strategy to Minimize the Consequences of Direct Containment Heating*, NUREG/CR-5447, EGG-2574, October 1990.
2. D. A. Brownson, L. N. Haney, and N. D. Chien, *Intentional Depressurization Accident Management Strategy for Pressurized Water Reactors*, NUREG/CR-5937, EGG-2688, April 1993.
3. P. D. Bayless, *Analyses of Natural Circulation During a Surry Station Blackout Using SCDAP/RELAP5*, NUREG/CR-5214, EGG-2547, October 1988.
4. D. L. Knudson and C. A. Dobbe, *Assessment of the Potential for High Pressure Melt Ejection Resulting from a Surry Station Blackout Transient*, NUREG/CR-5949 (Draft), EGG-2689, May 1993.
5. DCH Working Group, *Integrated Report on DCH Issue Resolution for PWRs*, NUREG/CR-6109 (Draft), SAND93-2078, August 1993.
6. S. E. Dingman, *Risk Assessment for the Intentional Depressurization Strategy in PWRs*, NUREG/CR-6092 (Draft), SAND93-1737, July 1993.
7. C. M. Allison et al., *SCDAP/RELAP5/MOD3 Code Manual*, NUREG/CR-5273 (Draft), EGG-2555, Revision 2, Volumes 1-4, September 1991.
8. T. Boardman et al., *Leak Rate Analysis of the Westinghouse Reactor Coolant Pump*, NUREG/CR-4294, 85-ETEC-DRF-1714, July 1985.
9. C. J. Ruger et al., *Technical Findings Related to Generic Issue 23: Reactor Coolant Pump Seal Failure*, NUREG/CR-4948, BNL-NUREG-52144, March 1989.
10. T. A. Wheeler et al., *Analysis of Core Damage Frequency From Internal Events: Expert Judgement Elicitation*, NUREG/CR-4550, SAND86-2084, Volume 2, April 1989.
11. United States Nuclear Regulatory Commission, *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*, NUREG-1150, December 1990.

NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights. The views expressed in this report are not necessarily those of the United States Nuclear Regulatory Commission.

PEER REVIEW OF RELAP5/MOD3 DOCUMENTATION

Summarized by W. G. Craddick

Oak Ridge National Laboratory

Abstract

A peer review was performed on a portion of the documentation of the RELAP5/MOD3 computer code. The review was performed in two phases. The first phase was a review of Volume III, *Developmental Assessment Problems*, and Volume IV, *Models and Correlations*. The reviewers for this phase were Dr. Peter Griffith, Dr. Yassin Hassan, Dr. Gerald S. Lellouche, Dr. Marino di Marzo and Mr. Mark Wendel. The reviewers recommended a number of improvements, including using a frozen version of the code for assessment guided by a validation plan, better discussion of discrepancies between the code and experimental data, and better justification for flow regime maps and extension of models beyond their data base. The second phase was a review of Volume VI, *Quality Assurance of Numerical Techniques in RELAP5/MOD3*. The reviewers for the second phase were Mr. Mark Wendel and Dr. Paul T. Williams. Recommendations included correction of numerous grammatical and typographical errors and better justification for the use of Lax's Equivalence Theorem.

A peer review was performed on a portion of the documentation of the RELAP5/MOD3 computer code[1]. The review was performed in two phases. The first phase was a review of Volume III, *Developmental Assessment Problems*, and Volume IV, *Models and Correlations*. The reviewers for this phase were Dr. Peter Griffith, Dr. Yassin Hassan, Dr. Gerald S. Lellouche, Dr. Marino di Marzo and Mr. Mark Wendel. The second phase was a review of Volume VI, *Quality Assurance of Numerical Techniques in RELAP5/MOD3*. The reviewers for the second phase were Mr. Mark Wendel and Dr. Paul T. Williams. Both phases used the NRC's "Charter for Evaluation of RES Code Documentation" as a guide for the reviews. Some additional review criteria for each phase were added by NRC staff to address concerns specific to these volumes.

The additional criteria added by NRC Staff for the review of Volumes III and IV were those contained in Section 4.4.3 of NUREG-1230, *Compendium of ECCS Research for Realistic LOCA Analysis*[2]. This section describes criteria for documentation in order to support the code scaling, applicability and uncertainty (CSAU) evaluation process. The portions of the NRC's "Charter for Evaluation of RES Code Documentation" which apply to Volumes III and IV are a subset of the criteria given in Section 4.4.3. Therefore, the criteria from NUREG-1230 can be used to provide a concise but comprehensive list of the review criteria for this phase.

The requirements for code assessment reports (i.e., Volume III: *Developmental Assessment Problems*) are set forth in Section 4.4.3.2 of NUREG-1230 which states that it is necessary for the reports:

1. To assess code capability and quantify its accuracy to calculate various parameters of interest such as: cladding temperature, inlet and outlet flows for various components, pressure drops, liquid inventory distribution, temperature distributions, etc.,
2. To determine whether or not the calculated results are due to compensating errors,
3. To assess whether or not the calculated results are self-consistent and present a cohesive set of information that is technically rational and acceptable,
4. To assess whether or not the timing of events calculated by a code are in agreement with experimental data, and
5. To explain any unexpected or at first glance, strange result calculated by the code. This is particularly important when experimental measurements are not available to give credence to calculated results. In such cases, rational technical explanations will go a long way towards generating credibility and confidence in the code.

Futhermore, whenever there is a disagreement between calculated results and experimental data it is necessary:

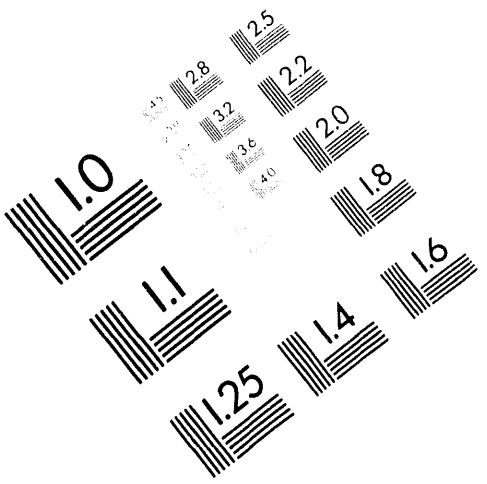
6. To identify and explain the cause of the discrepancy, that is, to identify and discuss the deficiency in the code (or if necessary, to discuss the inaccuracy of experimental measurements),
7. To address the question of how important the code deficiency is to overall results, that is, to parameters and issues of interest,
8. To explain why this code deficiency may not have an important effect on the particular scenario, or
9. To discuss what changes should be made to code models and correlations in order to obtain better agreement should the discrepancy, that is, the code deficiency, have a significant impact on overall results.

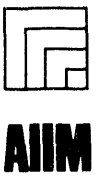
With respect to code input model and sensitivity studies (if performed), it is necessary for code assessment reports:

10. To provide a nodalization diagram along with a discussion of the nodalization rationale,
11. To specify and discuss the boundary and initial conditions as well as the operational conditions for the calculation,
12. To discuss modifications to the input model (nodalization, boundary, initial and/or operational conditions) resulting from sensitivity studies (if conducted),
13. To present and discuss results of sensitivity studies (if performed) on closure relations or other parameters, and
14. To provide guidelines for performing similar analyses.

The requirements for a QA document (i.e., Volume IV: *Models and Correlations*) are set forth in Section 4.4.3.1 which states that the document must:

1. Provide information on:
   - a: Its original source
   - b: Its data base
   - c: Its accuracy
   - d: Its applicability to NPP conditions

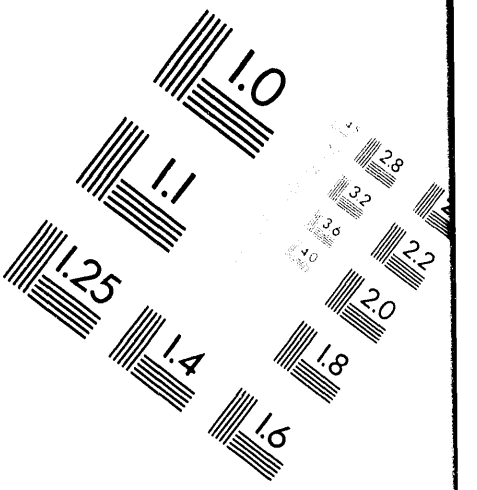


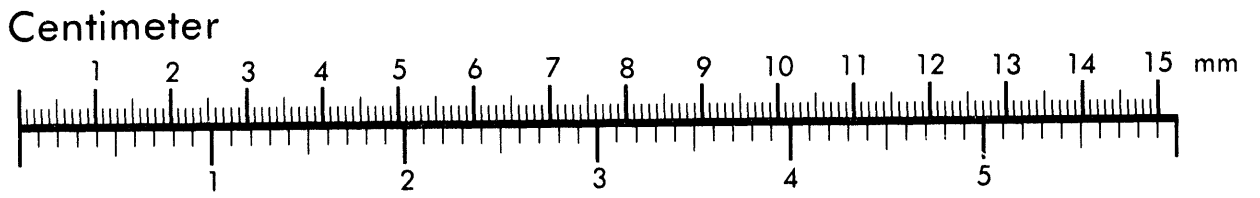


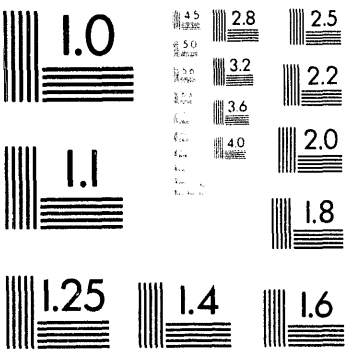
Association for Information and Image Management

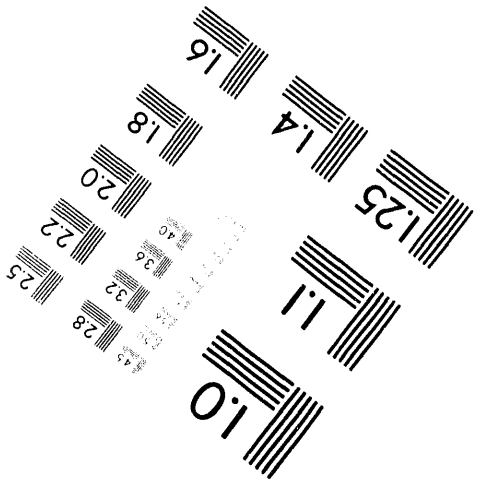
1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910

301/587-8202

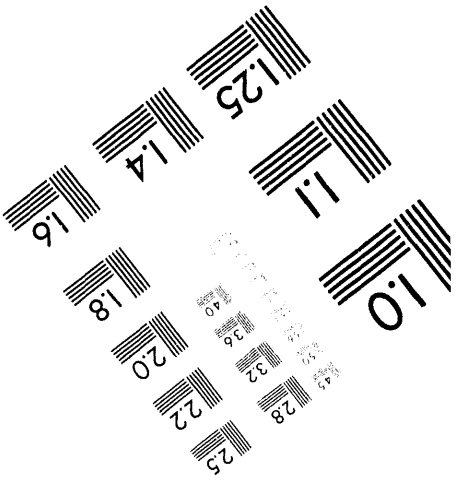








MANUFACTURED TO AIIM STANDARDS
BY APPLIED IMAGE, INC.



6 of 7

2. Provide an assessment of effects, if it is used outside its data base,
3. Describe how it is implemented in the code, that is how it is coded,
4. Describe any modification required to overcome computational difficulties, and
5. Provide an assessment of effects due to implementation (item 3) and/or due to modifications (item 4) on code overall applicability and accuracy.

Each of the five reviewers for Phase 1 prepared an independent report, and these reports were compiled and summarized by W. G. Craddick, D. G. Morris and M. Olszewski of ORNL. A letter report[3] containing the summary plus the full text of each reviewer's report was prepared and provided to the NRC in July, 1992.

While not unanimous in this regard, most of the reviewers felt that Volume III was well written and organized. However, the document has several significant deficiencies when compared to the criteria for acceptance defined in NUREG-1230 for documentation to be used to support the CSAU evaluation process. Modifications in several key areas would be required before the document could meet those criteria. A summary of the reviewer's major recommendations is provided below:

1. All code assessment activities should be performed with a frozen version of the code.
2. A validation plan should be completed. This plan would set forth the logical framework for testing the code. This would lead to a comprehensive set of assessment cases which would demonstrate comprehensive adequacy.
3. Where code results do not match experimental data, more discussion should be offered that details the reasons for the discrepancy. Identified code deficiencies should be evaluated and their impact on the code results assessed.
4. The description of code limitations should be expanded and scaling effects should be addressed.
5. Whenever code features are disabled, the impact on accuracy and code applicability should be discussed.
6. Guidelines for users for performing similar analyses should be included in the report, particularly where difficulties are encountered with code models.

The reviewers' reactions to Volume IV varied from strongly positive (Griffith) to rather negative (Lellouche). The majority felt that the description of what was in the code was fairly clear and understandable, through there is room for improvement. Certainly correction of numerous typographical errors is needed. There were definite differences in the reviewers' reactions to limitations in the description of the applicability and justification of the codes' models and correlations some judging these to be clear deficiencies in the documentation and others more inclined to attribute them to limitations in the code itself or in our knowledge of the physical phenomena. A summary of the reviewers' major recommendations is provided below:

1. Adopt a consistent set of symbols and nomenclature throughout the volume.
2. Provide additional supporting references, justification and explanation for flow regime maps, for applications of correlations and models beyond their original data bases and for modifications made in implementing correlations and models.
3. Provide an explanation for the limits placed on variables and coefficients, particularly in Chapter 4, Section 1.

4. Enhance the readability of Chapters 6 and 7, either by better defining the FORTRAN used or by adopting an alternate presentation strategy.

As was the case for the Phase 1 review, Phase 2 was based on both the NRC's "Charter for Evaluation of RES Code Documentation" plus additional criteria provided by the NRC staff. As before, only a portion of the RES Charter is applicable to Volume VI. Extracting the applicable items produces the following criteria.

1. Is there a description of the capabilities, range of applicability and limitations of the code?
2. Is the numerical solution scheme described? Is time and space averaging described?
3. An executive summary should be supplied which includes objectives, scope, methodology used, conclusions and recommendations.
4. The abstract should contain a brief description of the contents of the document and the sponsoring and performing agencies. Results, conclusions and recommendations should not be included in the abstract.
5. Is the documentation well written, well organized and understandable?
6. Present and discuss results of sensitivity studies on closure relations or other parameters.
7. Address the question of how important the code deficiency is to the overall results, that is, to parameters and issues of interest.

The supplemental criteria provided by the NRC staff address validation of the numerical techniques used in the code and are given below.

1. Volume VI is a self-contained account of the numerical techniques in RELAP5/MOD3.
2. Volume VI establishes the domain of applicability of those numerical techniques by a theoretical nodalization and time step analysis that determines ranges of values of Δx and Δt that lie within the region of stability, convergence, and accuracy for the numerical techniques and correlations used in the code.
3. By combining analytical and computed results, Volume VI meets the regulatory objective to provide RELAP5 documentation sufficiently detailed that the domain of applicability of the numerical techniques and necessary user procedures are both well-defined. That would also provide increased confidence in the ability to distinguish between model deficiencies and deficiencies in numerical techniques.

Wendel reviewed the documentation against the RES Charter criteria and Williams reviewed the documentation against the supplemental criteria. Craddick and Morris compiled and summarized the reviews from Wendel and Williams into a letter report[4] provided to NRC in May, 1993. The major conclusions reached in the review of Volume VI are:

1. Generally speaking, while all criteria are addressed, specific areas require revision and elaboration to meet documentation requirements.
2. Specifically, Chapters 4 and 5 do not meet the requirement of being "sufficiently detailed," and there is insufficient linkage between the theoretical studies presented in Chapter 4 and the computational experiments presented in Chapter 5.

3. Although Volume VI is organized in a logical fashion, significant problems exist with regard to readability due to awkward sentence structure, grammatical and typographical errors, and nomenclature inconsistency.
4. Formalized standards and procedures are rapidly evolving throughout the technical community for software quality assurance. If the term quality assurance is used in this formal sense, Volume VI does not address software quality assurance, despite the appearance of this term in the title of the volume.

Some additional explanation of the second conclusion with respect to the document being insufficiently detailed is warranted. Toward that end, the following four paragraphs are quoted from Williams' review.

Chapter 4 of Volume VI presents a theoretical linear stability analysis for the semi-implicit and nearly-implicit algorithms. The analysis relies upon *Lax's Equivalence Theorem* to provide the fundamental linkage between *well-posedness, consistency, stability,* and *convergence*. This theorem states that given a *properly-posed* linear initial-value problem and corresponding linear finite-difference approximation to it that satisfies the *consistency* condition, *stability* is the necessary and sufficient condition for *convergence*. In other words, in order to prove convergence for a numerical algorithm, it is necessary and sufficient to prove that the parent initial-value problem is well-posed and that the finite difference approximation is consistent and stable. *Well-posedness* requires that solutions to the continuum initial-value problem are unique and continuous functions of the initial data, specifically the initial and boundary conditions. *Consistency* requires that the individual finite-difference approximations converge in some sense to their corresponding continuum partial derivatives in the limit of Δx and $\Delta t \rightarrow 0$. *Stability*, a property solely of the finite-difference approximations used in the algorithm, requires that there should be a bounded limit to the extent to which any component of the initial data can be amplified by the numerical algorithm as it marches through time. *Physical instabilities* are characterized by solutions which have bounded limits, but *numerical instabilities* are unbounded.

Two fundamental issues must be addressed when applying *Lax's Equivalence Theorem* to algorithms for two-phase flow. The first issue is that the Equivalence Theorem has been rigorously proven for *linear* differential and difference operators only. The application of the theorem to nonlinear systems, such as the two-phase conservation law system, represents an extension (albeit commonly made in the computational fluid dynamics literature without justification) beyond its original range of applicability. Such an extension should be justified. This issue is not adequately addressed in Volume VI.

The second issue involves the lack of *well-posedness* of the two-phase conservation law system employed in RELAP5. Quoting from Ransom and Hicks,[5]

> **For some time it has been known that many of the two-phase flow models lead to ill-posed Cauchy problems because they have complex characteristics values. A necessary condition (at least in the linear case) for the Cauchy problem to be well-posed is that it be stable in the sense of von Neumann. For systems of partial differential equations of first order, stability in the sense of von Neumann is essentially equivalent to the condition that the model be hyperbolic (all real characteristics values and complete set of characteristic vectors.)**

This issue is addressed in Chapter 4 but could be expanded with additional background material. The main thrust of Chapter 4 is the theoretical development of conditions for the time-step Δt and nodalization Δx which will ensure that the stated stability condition, Eq. (4.11)$\rightarrow \| U^{n+1} \| \leq \| U^n \|$, is met. Since the theoretical treatment, apparently previously unpublished, given in Chapter 4 represents an extension of an analysis reported in the archival literature by Stewart,[6] the detailed comments in Sect. 3.3 of this review suggest a greater rigor and completeness in the presentation of proofs for any new theorems.

Based on the conclusions condensed from Wendel's and Williams' reviews, the set of recommendations summarized below was identified:

1. Include more detailed information in Chapters 4 and 5; specifically, (i) address two theoretic issues when applying Lax's Equivalence Theorem to algorithms for two-phase flow, (ii) provide a linkage between Chapters 4 and 5, and (iii) include geometry, and boundary and initial conditions (or at least a brief summary and appropriate reference) for the computational experiments in Chapter 5.
2. Adopt a consistent nomenclature throughout the volume.
3. Enhance the readability of the volume by correcting numerous grammatical and typographical errors and revising awkward sentence structure.
4. Consideration should be given to retitling the volume or including sections to address the formal requirements of quality assurance.

In conclusion, it is worth noting that the charters for all of these reviews included specific instructions that the review was to be of the documentation only, and not the code itself. This should be kept in mind when considering any of these recommendations. A finding that insufficient justification was presented for any particular model or feature of the code does not necessarily mean that such justification does not exist, but only that we did not find that justification in these volumes.

References

1. K. E. Carlson, et al., "RELAP5/MOD3 Code Manual," Volumes I-IV (DRAFT), NUREG/CR-5535, EGG-2596, Idaho National Engineering Laboratory, June 1990.

2. "Compendium of ECCS Research for Realistic LOCA Analysis," NUREG-1230 R4, Division of System Research, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, December 1988.

3. W. G. Craddick, D. G. Morris, and M. Olszewski, *Peer Review of Documentation for RELAP5/MOD3, Volume III: Development Assessment Problems and Volume IV: Models and Correlations*, ORNL letter report ORNL/NRC/LTR-92/20, July 1992.

4. P. T. Williams, M. W. Wendel, D. G. Morris, and W. G. Craddick, *Peer Review of Documentation for RELAP5/MOD3, Volume VI: Quality Assurance of Numerical Techniques in RELAP5/MOD3*, ORNL letter report ORNL/NRC/LTR-93/10, May 1993.

5. V. H. Ransom and D. L. Hicks, "Hyperbolic Two-Pressure Models for Two-Phase Flow," *Journal of Computational Physics*, Vol. 53, 1984, pp. 124-151.

6. H. B. Stewart, "Stability of Two-Phase Flow Calculation Using Two-Fluid Models," *Journal of Computational Physics*, Vol. 33, 1979, pp. 259-270.

BENCHMARK ANALYSES WITH RELAP5 FOR USNRC SIMULATORS

John D. Burtt and Robert P. Martin
Idaho National Engineering Laboratory
EG&G Idaho Inc.
P. O. Box 1625
Idaho Falls, ID 83415

Larry Bell
USNRC Technical Training Center
Osborne Office Center, Suite 200
Chattanooga, TN 37411

ABSTRACT

The U. S. Nuclear Regulatory Commission adopted the Kemeny Commission recommendations that all nuclear plants have a plant specific simulator for operator training. In support of this requirement a project was initiated to examine the capabilities of the current generation of simulators using advanced thermal hydraulic systems codes such as RELAP5 and TRAC-B. As part of the project, RELAP5 models of Pressurized Water Reactor simulators at the U. S. Nuclear Regulatory Commission's Technical Training Center have been developed and sets of transients performed for comparison with simulator predictions.

One such model was for the Washington Nuclear Project Unit 1 Simulator. Thermal-hydraulic analyses of five hypothetical accident scenarios were performed with the RELAP5/MOD3 computer code, then the same scenarios performed on the simulator, prior to a scheduled upgrade with S3 Technology's RETACT simulator code. The five transients performed were: (1) Loss of AC power, (2) Small Break Loss of Coolant Accident with Loss of AC power, (3) Stuck open Pressurizer Safety Valve, (4) Main Steamline Break with Steam Generator Tube Rupture, and (5) Loss of main Feedwater with Delayed Scram.

Comparison of code and simulator data was performed by reviewing each transient with a team of plant analysts and experienced reactor operators. The initial findings show that both the simulator and system codes' modeling need improvement. The conclusion drawn from this preliminary study is that simulator benchmarking is and should be a dynamic, iterative process with benefits for both simulator engineers and plant analysts.

This work is supported by the U. S. Nuclear Regulatory Commission under DOE Idaho Operations Office Contract DE-AC07-76IDO1570

1.0 INTRODUCTION

One of the lessons learned from the accident at Three Mile Island was the recognition of the need for effective reactor operator training. The President's Commission on the Accident at Three Mile Island (the Kemeny Commission) recommended that all plants have access to a plant-specific simulator for operator training. The simulators would have to have the capability to model plant operation as well as transients in an environment closely resembling the actual plant control room. The current generation of simulators have been unable to model many important transients or have produced incorrect responses.

In 1988 the U. S. Nuclear Regulatory Commission (USNRC) initiated a project to study the capabilities of the current generation of simulators, as well as the improved capabilities of the next generation. The platforms selected for the study were the simulators in use at the USNRC's Technical Training Center (TTC), located in Chattanooga, TN. The TTC currently has four in-house simulators, one from each US reactor vendor: Black Fox (General Electric BWR/6), WNP-1 (Babcock & Wilcox PWR), SNUPPS (Westinghouse PWR), and Calvert Cliffs (Combustion Engineering PWR). In addition, the Shoreham BWR/4 simulator is scheduled for installation in early 1994. These simulators are used to train USNRC personnel in reactor theory, operation and transient response.

The benchmarking project involves the development of computer models of each TTC simulator using an advanced thermal-hydraulic systems code. The models are then used to perform a series of transients, selected to test the capabilities of the model and simulator. The results of the transient are then compared with the results of the transient series run on the target TTC simulator. Comparison will be performed both before and after scheduled simulator upgrades.

This paper will present and discuss the preliminary results from transients performed for the Babcock & Wilcox (B&W) PWR WNP-1, using RELAP5/MOD3 and the TTC simulator.

1.1 The Simulator

The Washington Nuclear Project Unit 1 (WNP-1) simulator was installed at the TTC in 1988. The simulator consists of an Encore 32/9780 computer connected via Interpose Link to an Encore 32/55. The 32/9780 computer is a dual processor, high performance computer system (10 MFlop) that utilizes the latest real-time operating system and current technology peripherals. The computer is equipped with 8 Mbytes of main memory, two 858 MByte disk drives, and Ethernet (for communicating with the computers on the other TTC simulators. All the plant models and instructor station host software are executed on the 32/9780. A Macintosh-based instructors station is connected to the 32/9780 via Ethernet using TCP/IP protocol. Plant computer and SPDS simulation systems software is executed in the 32/55. The simulator's software executive system, developed by the TTC staff, runs under the control of Encore MPX operating system, version 3.5. The WNP-1 simulator has been recently upgraded to use S3 Technology's RETACT simulation Program.

The simulation software was developed by Singer-Link, Inc. Since the function of the simulator is to assist in training, the software has been designed to perform real-time simulation of plant systems. Development of this software for real-time performance on the then (198X) current state-of-the-art workstations required that some phenomenological models be simplified to facilitate that level of performance. It is the error introduced by these simplifications that presently concerns the USNRC. The USNRC is also interested in how well the simulators predict severe accident scenarios. Since the original intent of the simulation software was for training operators for likely operational transients, little previous work has gone towards understanding the degree to which current simulation codes predict more severe transient phenomena, such as loss-of-coolant accidents (LOCAs) and anticipated transients without scram (ATWS) events.

1.2 The RELAP5 Code

The RELAP5/MOD3 systems code [Carlson, et al. 1990] has been designed to perform best estimate, thermal-hydraulic transient calculations of nuclear power plants. RELAP5 was developed at the Idaho National Engineering Laboratory. It has been used by the international nuclear community for a decade to simulate transients in all types of commercial and non-commercial reactors. The transients include operational transients, anticipated transients, and design basis accidents. RELAP5/MOD3 was released in February 1990 and is the result of extensive development and assessment by several members of the International Code Assessment Program. The major improvements in the code over its previous versions are discussed in [Carlson, et al. 1990]. It incorporates advanced phenomenological models describing the physical activity in these plants. However, many of the models have been derived empirically and, therefore, have an inherent degree of uncertainty. Extensive developmental assessment has been performed challenging these models and they have been "fine tuned" to an acceptable level of performance, as defined by the USNRC.

2.0 SIMULATOR CODE ASSESSMENT

The common procedure for assessing large, best estimate thermal-hydraulic systems codes involves performing calculations that simulate separate effects or integral test facility experiments. This simulator benchmark study is unique because the baseline for code assessment is a best estimate systems code rather than an experiment. The strength that legitimizes code assessment baselined against experimental data is the assumption that the experimental data is absolute truth. Using a systems code as a baseline for assessing another systems code weakens that foundation. Therefore, to legitimize the assessment of a systems code, a procedure must be developed that qualifies results sufficiently to insure a true assessment. Such a procedure should be applied whenever there is uncertainty associated with the baseline, such as from faulty instrumentation in an integral test facility. An extrapolation of this idea would also make this procedure applicable to "blind" code assessments. With the computer code baseline, personal modeling philosophies and the degree of numerical sensitivity are influences that can affect the level of uncertainty in the baseline. [D'Auria, et al.] and others have specifically examined this problem.

For this study, an integral system has been examined. Code assessment of integral systems is a unique challenge because of the interactions between different systems and phenomena. Therefore, a procedure for assessing a systems code using another systems code as a baseline might be

different than if a separate effects experiment were being modeled. Below, a method is proposed to assess a systems code vs. another systems code. This is the method that has been applied to this study.

1) Codes are studied to understand inherent limits and uncertainties.

2) Detailed models for the simulator and the systems code are developed from technical specifications.

3) A robust set of abnormal transients are performed on both platforms.

4) Results from both transient calculations are compared to identify discrepancies.

5) Discrepancies are distinguished by the occurring phenomenological events.

6) The corresponding phenomenological models are then compared for completeness and weaknesses are identified. In certain cases, where this distinction is more difficult, further study may be required to understand the limits and uncertainties of the relevant model.

7) If possible, improvements are made to the simulator, best-estimate code and/or input model and steps 4-6 are repeated.

3.0 RESULTS

Preliminary assessment of the B&W PWR WNP-1 simulator has been performed using the above method. The RELAP5/MOD3 systems code was used as the baseline for this task. This section is divided to address how the above method has been applied to this problem.

3.1 Limits and Uncertainties of Systems Codes

RELAP5 has evolved through many years of development and developmental assessment. Since RELAP5 has been designed for best-estimate thermal-hydraulic analysis of nuclear power systems, these assessment studies have been baselined against a wide range of separate effects and integral test facility experiments. The general conclusions from these studies is that the code provides a good prediction of the expected response of a nuclear power plant for an extensive number of operational and abnormal transients. The code has been assessed for severe accidents, such as large and small break LOCAs, ATWS, and component failures. While uncertainty exists in the application of the empirically derived constitutive models and where many phenomenological models interact, the code is regarded as a state-of-the-art analysis tool.

The simulators have also had much assessment [e.g. Roppel and Black, 1982]. The general conclusions from these studies is that the simulator responds well to operational transients, but performance degrades for more severe accidents, such as LOCAs, steam line ruptures, and failed pressurizer relief valve transients, which push the simulator models to their design limits. Since

much of the physical phenomena are characterized by empirical curve fits and other methods (to facilitate quick computational processing), error tends to be more significant near the limits of applicibility of such relations. Specific problems observed with simulators include non-conservation of mass, momentum and energy, non-physical two-phase flow results, inaccurate state properties near the critical point, lack of coupling between related phenomena, etc.

Actual limits and uncertainties can be determined through a heuristic analysis that involves comparing calculational results against experimental data. Much of this has been done in the above mentioned references.

3.2 Simulator and Best Estimate Code Input Models

Simulator models for specific plants are often an integral part of the software. Unlike RELAP5, where a model is a distinct entity from the code, simulator models are "hardwired" into the simulator code to enhance execution speed and detail of unique phenomena. Simulator models must be extremely detailed to simulate a realistic control room setting relevant to training reactor operators.

RELAP5 and TRAC-B models are built from a basic set of thermal-hydraulic components, reactor kinetics options, and control elements. Together, a model of a nuclear system can be built with fine detail, assuming design detail is available. Best estimate code input models do not have the detail that simulator models typically have because of constraints on computer CPU, numerical methods, and because typical application of these models does not require such detail.

3.3 The WNP-1 Model

The WNP-1 comparison model was developed using RELAP5/MOD3 computer code. The RELAP5 WNP-1 model, shown in Figures 1 and 2, included all the major components [Martin, 1991]. Specific features modeled include all major primary system coolant flow paths, secondary system main feedwater downstream of the main feedwater valves, and secondary main steam paths upstream of the turbine stop valves. Modeling also included the emergency core cooling and auxiliary feedwater systems on the primary and secondary sides, respectively. An explicit model of the B&W integrated control system (ICS) was not modelled, but many control systems, such as the reactor protection system and the engineered safety features actuation system, were modelled. The model used 190 control volumes, 197 junctions, and 195 heat structures to simulate the WNP-1 nuclear steam supply system.

Five transient scenarios were analyzed with the RELAP5 model and the WNP-1 simulator. The five transients were:

1. Loss of ac Power (loss of off-site power with a diesel generator failure).
2. Small break LOCA (1000 gpm initially) with loss of ac power.
3. Failed open Pressurizer Safety Relief Valve.
4. Double ended Main Steam Line break with a steam generator tube rupture.
5. Loss of feedwater pumps with a delayed scram.

The five transients were all run from a 98% nominal power (3684.8 MWt), full flow (75.5 Mlb/hr) condition. The transients were chosen to include minimum operator interaction so as to limit interference with the phenomenological models from unrelated influences.

3.4 Comparison between RELAP5 and WNP-1 Simulator

A preliminary comparison of the data obtained from RELAP5 and the pre-upgrade WNP-1 simulator was performed by reviewing each transient with a team of experienced plant analysts and reactor operators. The initial result was an understanding that a "right or wrong" judgement was not going to be possible. The reason was that the reviewers concluded that both simulator and code models needed improvement.

The results of the first two transients, loss of ac power and small break LOCA with loss of ac power, had similar results in the simulator calculations. RELAP5 showed both transients dominated by natural circulation and heat removal through the steam generators. As seen in Figure 3, the simulator did not calculate any natural circulation, as evidenced by the lack of any hot and cold leg temperature differential. This was a serious defect in the pre-upgrade simulator software. In addition, the simulator's "rule of thumb" break size (1% break equals 200 gpm) proved wrong by an order of magnitude.

The RELAP5 model also proved in error at times. Figure 4 presents a comparison of reactor power taken from scenario 5: loss of feedwater pumps with delayed scram. The rampdown of power experienced by the simulator is a result of the plant's ICS load following feature, which will automatically reduce power as feedwater diminishes. The RELAP5 model had no load following capability in its control systems, thus the power stayed high. This difference meant that there was significantly more stored energy in the RELAP5 model during this transient than in the simulator. The increase in stored energy had a major impact on the remainder of the transient, leading to inaccurate results. In this case the RELAP5 model needs to be improved.

Finally, there were anomalies in the comparisons that had no straight forward explanation. Figure 5 shows a comparison of pressure in the broken steam generator in scenario 4: double ended main steam line break with steam generator tube rupture. The analysts expected a pressure reduction similar to the RELAP5 results. The simulator pressure curve showed an unexpected repressurization for approximately 15 seconds. While the general consensus was that the simulator was in error, the reason for the error was not immediately known. Problems like this need to be accurately explained to prevent carry-over problems to other transient analyses. Parametric studies using both the RELAP5 model and the simulator will be performed to identify the problem.

4.0 CONCLUSIONS

The conclusion drawn from this preliminary study is that the task of benchmarking plant specific simulators against the best-estimate thermal-hydraulic codes will not be a simple comparison task. What will be required is a dynamic, iterative process that will demand flexibility between plant analysts and simulator engineers. A validated code model will have to be compared with simulator results and the data analyzed. Changes to both models should be expected and the process repeated as required. Such a process will benefit both analysts and engineers and produce a high level of operator and analyst training.

5.0 REFERENCES

Kemeny Commission, Report of the president's Commission on the Accident at three Mile Island, Washington DC, October 1979.

Carlson, K. E. et. al., "RELAP5/MOD3 Code Manual Volume IV: Models and Correlations", NUREG/CR-5535, June 1990.

Carlson, K. E. et. al., "RELAP5/MOD3 Code Manual Volume III:, Developmental Assessment Problems", NUREG/CR-5535, June 1990.

D'Auria, F and Galassi, G. M., "Comparative Analysis of Accident Management Procedures in LOBI and SPES Facilities, Proceedings from NURETH-5, Salt Lake City, UT, September 1992.

Black, R. L. and Roppel, V. R., "Performance Analysis of WPPSS WNP-1 Simulator", B&W Nuclear Power Generation Division, January 1982.

Martin, R. P., "RELAP5 Thermal-Hydraulic Analysis of the WNP-1 Pressurized Water Reactor," NUREG/CR-5663, EGG-2633, March 1991.

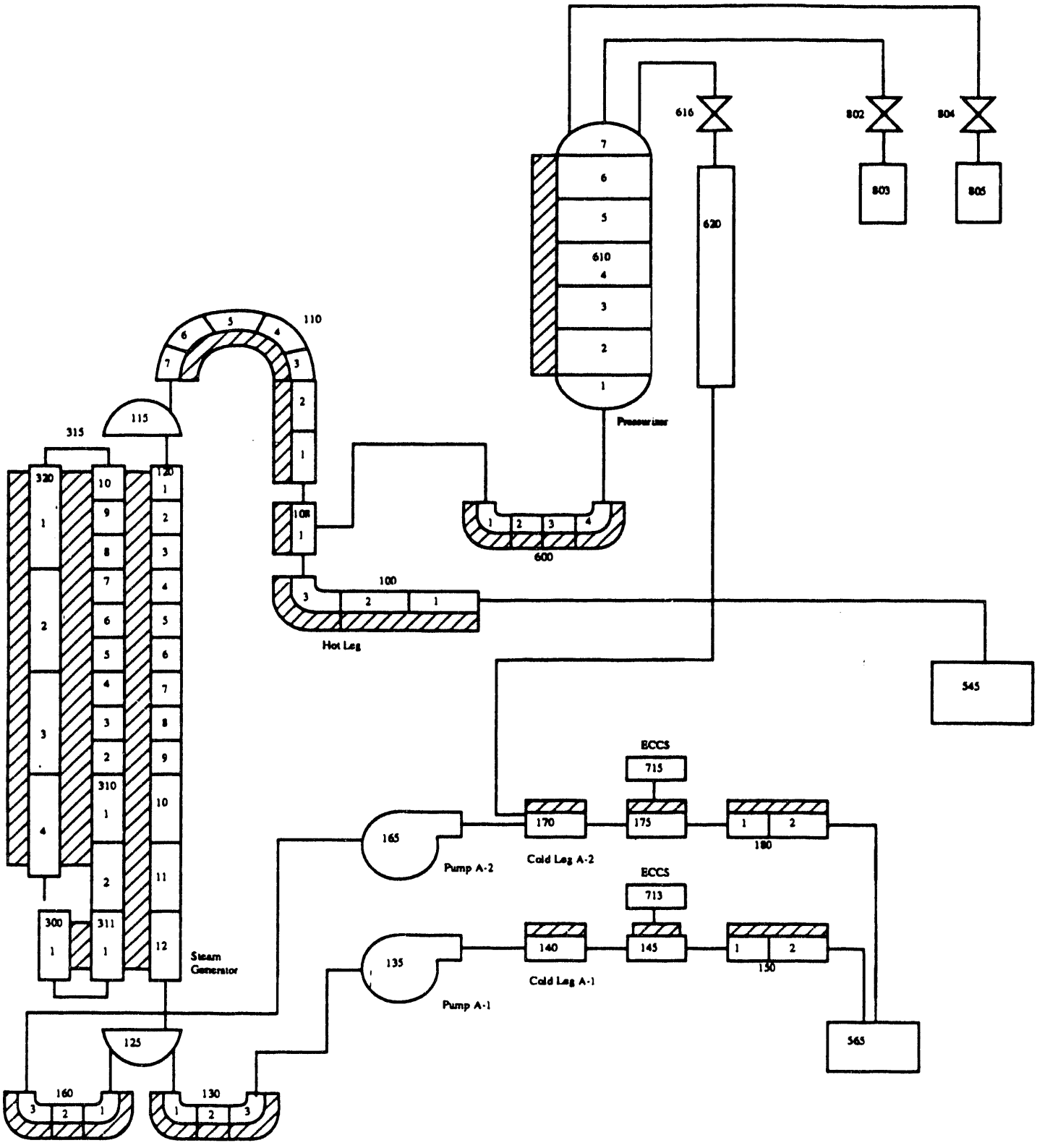


Figure 1. Nodalization of WNP1 primary coolant loop A

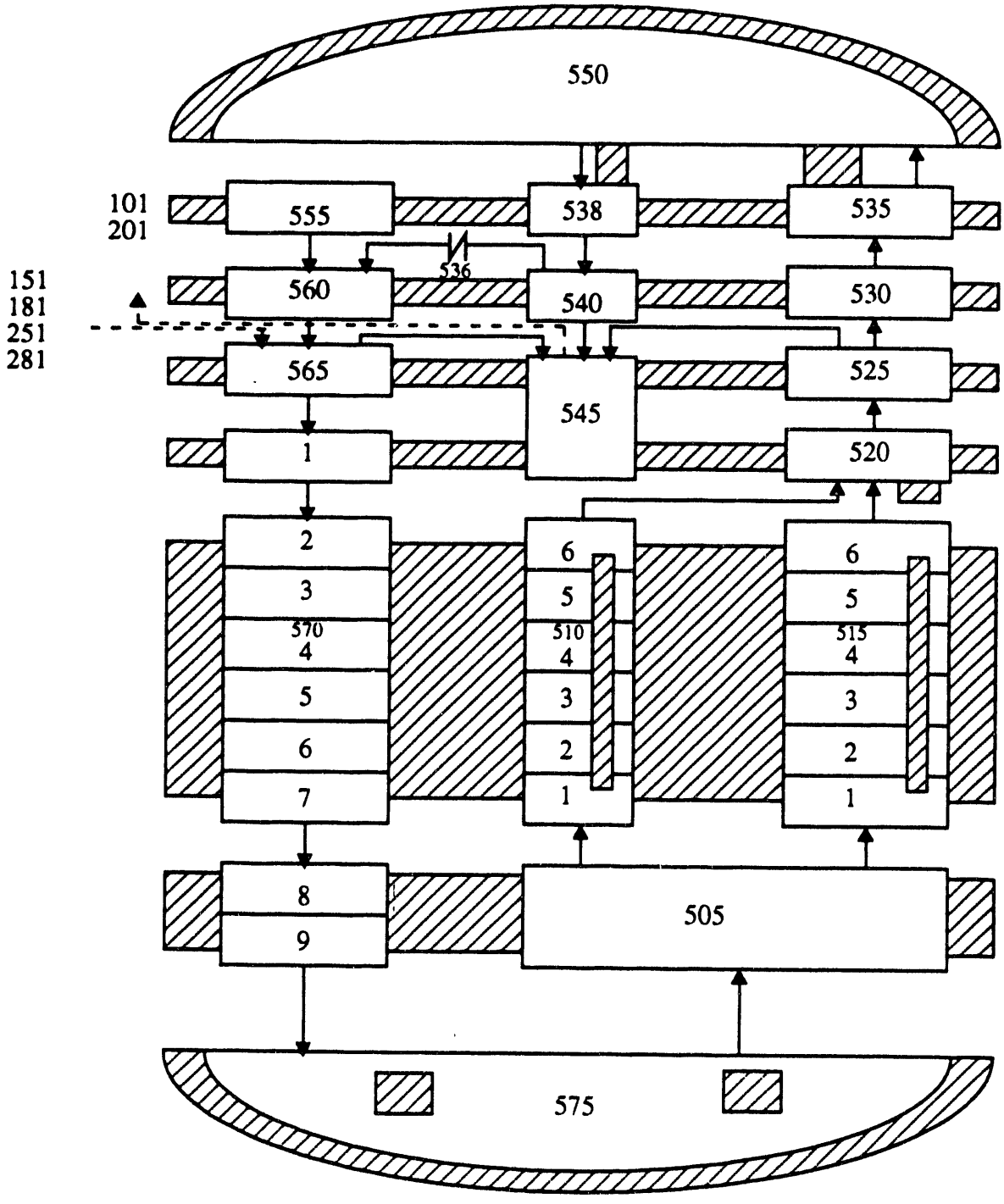


Figure 2. Nodalization of WNP1 Reactor Vessel

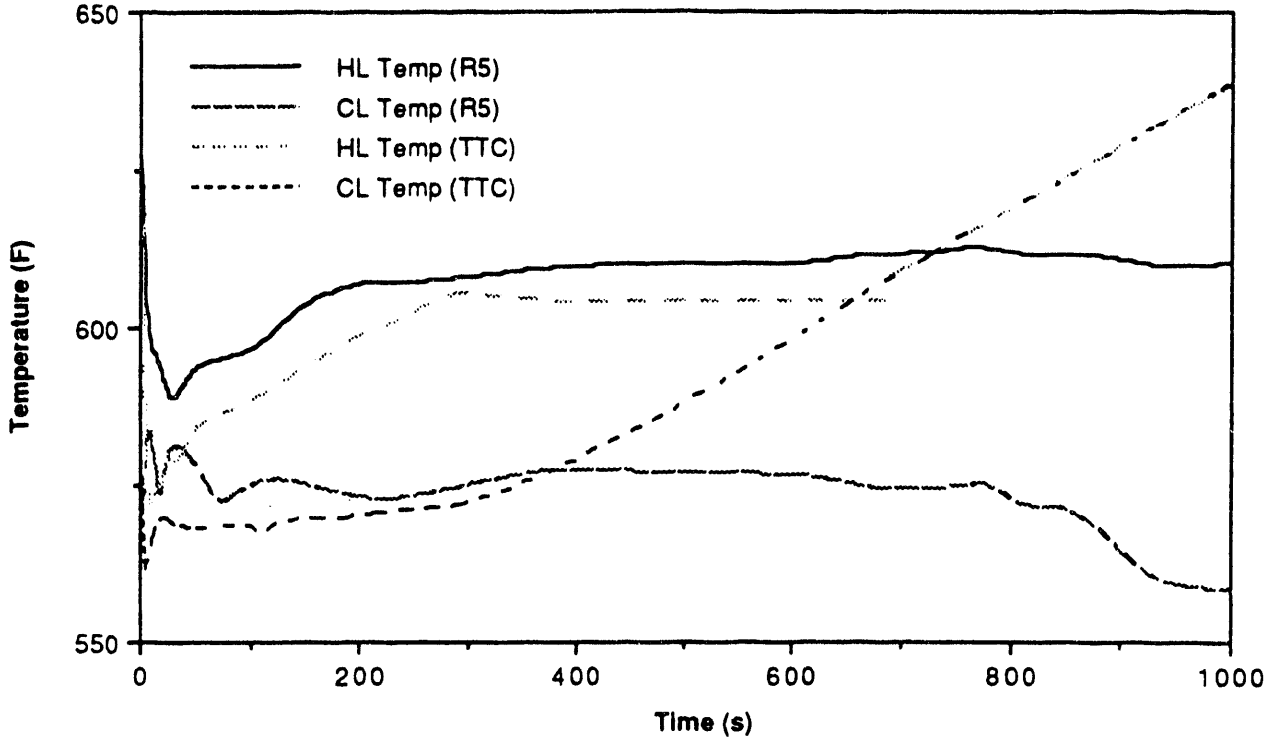


Figure 3. Primary hot and cold leg temperatures for station blackout/LOCA from RELAP5 and simulation.

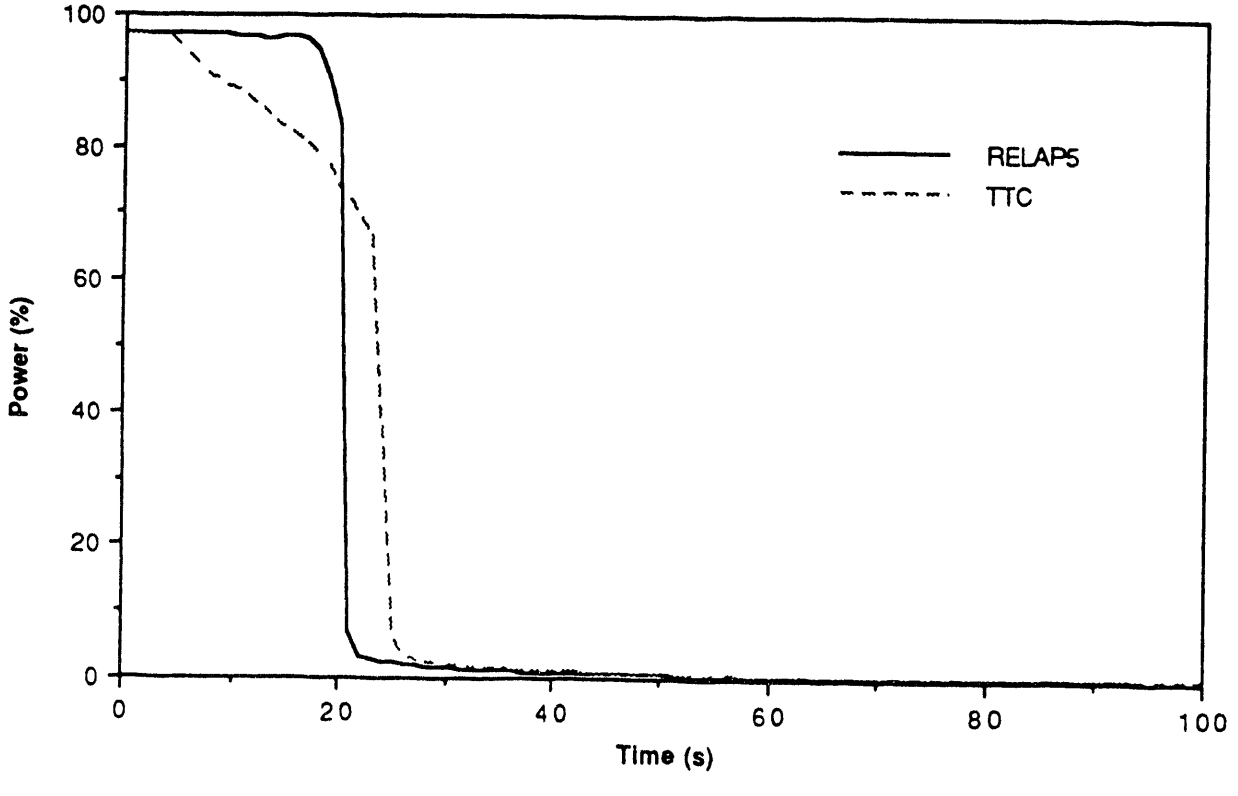


Figure 4. Reactor power for ATWS from RELAP5 and simulation

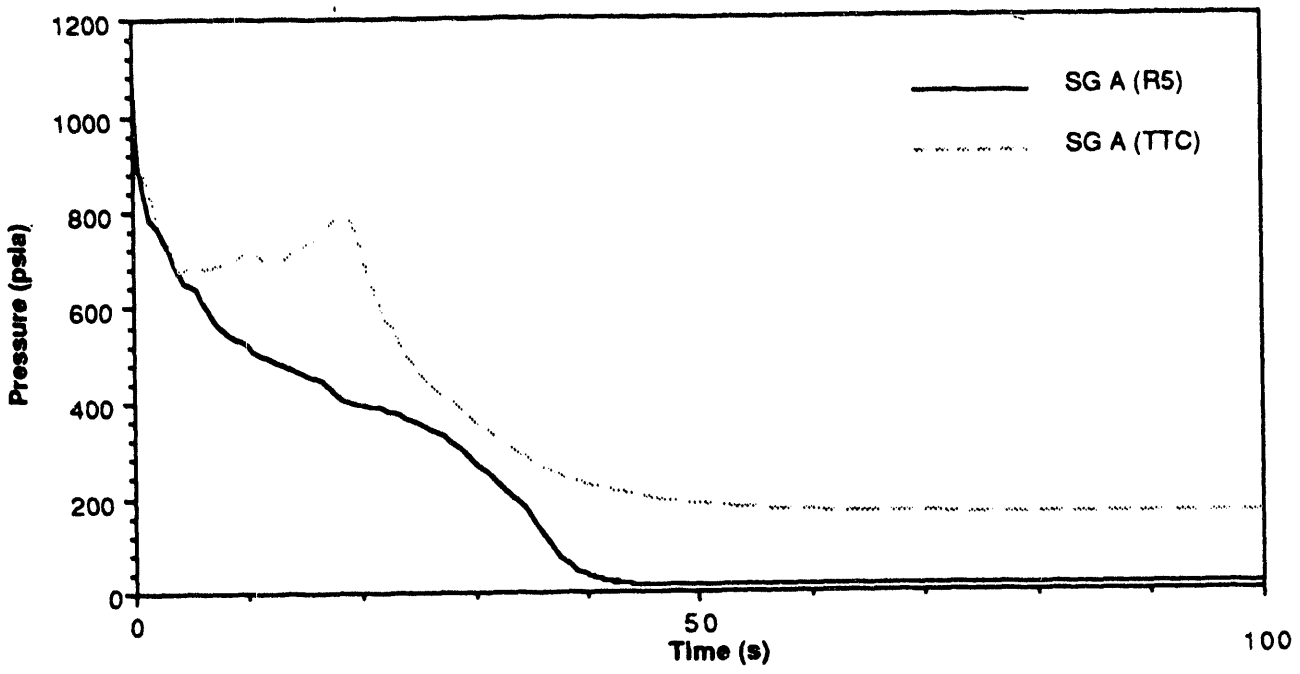


Figure 5. Steam generator pressure from a main steam line break from RELAP5 and simulator

Depressurization As An Accident Management Strategy to Minimize Direct Containment Heating*

D. A. Brownson[b]
F. Odar[c]

Idaho National Engineering Laboratory
EG&G Idaho, Inc.
Idaho Falls, ID 83415

Abstract

In a previous investigation of the Surry nuclear power station, it was concluded that intentional depressurization of the reactor coolant system could prevent or mitigate the effects of direct containment heating during a TMLB' station blackout transient. By applying appropriate scaling factors, the results of the Surry analysis were extended to other U.S. pressurized water reactors (PWRs) in order to evaluate their capability to successfully employ the intentional depressurization strategy. This extension resulted in the categorization of four PWR groups. A representative from each PWR group was then chosen for evaluation. The phenomenological behavior, equipment reliability, and operational performance of these PWRs during the intentional depressurization strategy was considered. These evaluations were then used to provide an indication of the capability of the remaining members of each PWR group to employ the intentional depressurization strategy.

Introduction

During certain accident sequences, the potential exists for ejection of molten corium from a high pressure reactor coolant system (RCS) and for dispersal of this corium into the containment atmosphere causing direct containment heating (DCH). High pressure melt ejections (HPME) account for 13% of the core damage frequency in the NUREG-1150 risk study of the Surry nuclear power plant (NPP).[1] Accident management strategies have been identified that have the potential to either prevent or mitigate the high

---

* Work supported by the U. S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, under DOE Idaho Field Office Contract DE-AC07-76ID01570.

[b] Staff member at the Idaho National Engineering Laboratory.

[c] Staff member at the U.S. Nuclear Regulatory Commission.

pressure severe accident sequences that could result in DCH. Examples of preventative strategies for the TMLB' station blackout scenario include (a) feed and bleed of the steam generators using normal or alternate feedwater injection methods or water sources, and (b) feed and bleed of the RCS using normal or alternate high pressure injection methods or sources of water. Strategies for mitigating DCH have also been identified in the event that preventative strategies are not effective. These strategies are generally aimed at minimizing the RCS-to-containment pressure differential at the time of reactor vessel lower head failure to reduce the driving force for HPME. One method of accomplishing these strategies is through intentional RCS depressurization prior to lower head failure.

Intentional depressurization of the RCS requires the operator to latch open the power operated relief valves (PORVs) at some point during the transient. The TMLB' station blackout transient was selected for analysis because station blackout contributes 95% to HPME occurrences in the Surry NUREG-1150 analysis. Two depressurization strategies were considered for the Surry NPP in earlier analyses (NUREG/CR-5447).[2] These were early depressurization - latching the PORVs open at the time of steam generator dryout, and late depressurization - latching the PORVs open at the time of a core exit thermocouple reading of 922 K (1200°F). A temperature of 922 K ensures that the core is in the process of uncovering and that fuel damage is imminent. Results indicate that late depressurization permitted more time for the operator to restore ac power or obtain the firewater or other water sources (and also led to less core damage during the depressurization process). Late depressurization was therefore the preferred intentional depressurization strategy over early depressurization in NUREG/CR-5447.

An approach was developed in Reference 3 for extending the Surry late depressurization results of NUREG/CR-5447 to other pressurized water reactors (PWRs). Based upon this approach, the PWRs in the U.S. with PORVs were categorized into four groups according to their perceived capability to employ the intentional depressurization strategy. PWRs without PORVs were not considered because the intentional depressurization strategy is dependent upon a plant having PORVs. The capability of a plant to depressurize was calculated based upon the ratio of PORV relief capacity to the plant's RCS volume. This ratio provides an indication as to how quickly mass and energy can be removed from the RCS in order to lower its pressure. If this ratio is then normalized to Surry, an indication of how quickly the RCS can be depressurized relative to Surry (a known quantity) can be obtained. The equation used for calculating the PORV ratio is as follows:

$$R_1 = \frac{(G_{PORV}/V_{RCS})_{PWR}}{(G_{PORV}/V_{RCS})_{Surry}}$$

where: G_{PORV} = PORV mass flow rate of study PWR and Surry
V_{RCS} = RCS volume of study PWR and Surry

The categorization of the U.S. PWRs is shown in Figure 1. As shown in this figure, the four PWR groups defined are: (1) Westinghouse Group 1 - PWRs with an intentional depressurization capability greater than Surry's; (2) Westinghouse Group 2 - PWRs with an intentional depressurization capability less than Surry's; (3) Combustion Engineering Group; and (4) Babcock & Wilcox Group.

A representative PWR of each of these groups was chosen for a systematic evaluation of its capability to employ intentional depressurization during a TMLB' station blackout sequence. The four PWRs chosen for evaluations were the Westinghouse Surry NPP, the Westinghouse Sequoyah NPP, the Combustion Engineering (CE) Calvert Cliffs NPP, and the Babcock & Wilcox (B&W) Oconee NPP. The Surry NPP was re-evaluated to take advantage of improvements to the SCDAP/RELAP5 code since the release of NUREG/CR-5447. Each of these PWRs were chosen because the values of the parameters which are important to the success of the intentional depressurization strategy are either representative or most limiting of the PWR's in their group. The phenomenological behavior, equipment reliability, and operational performance of intentional depressurization for each PWR was investigated to determine its potential to reduce RCS pressure to a sufficiently low value where DCH would be mitigated. These analyses are documented in Reference 4.

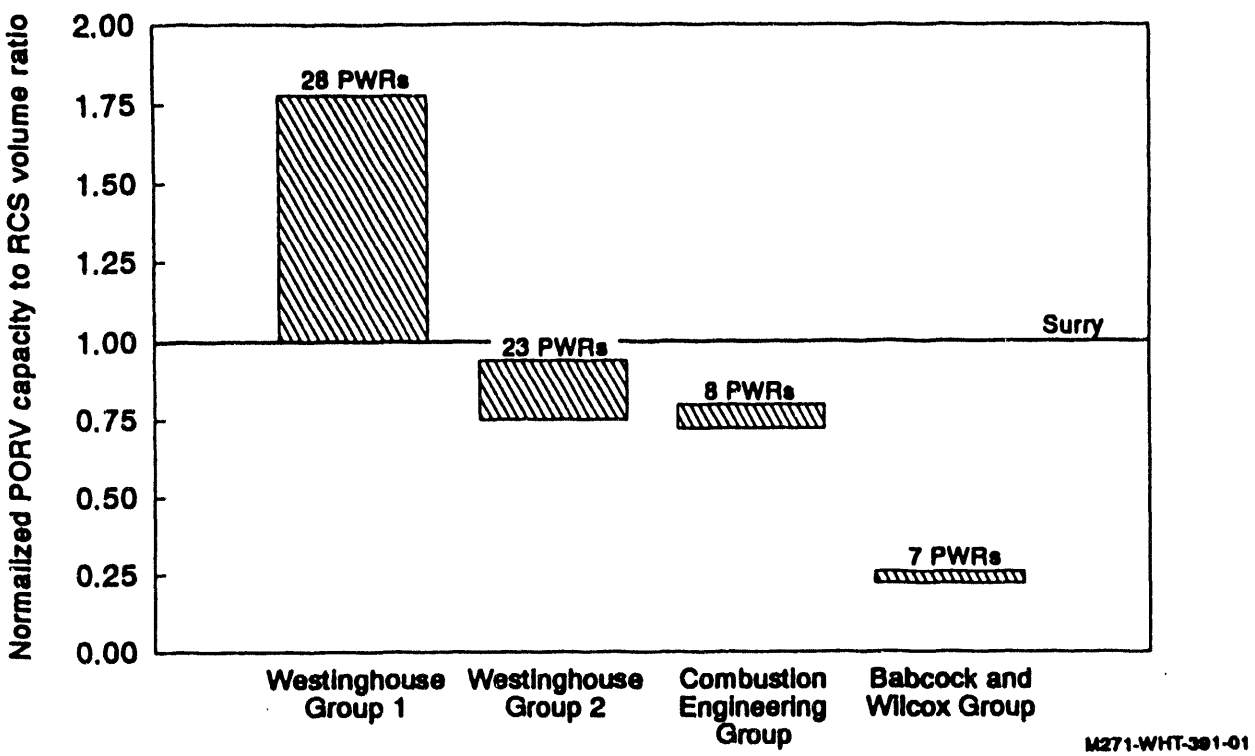


Figure 1. Grouping of PWRs based on their perceived capability to employ the intentional depressurization strategy.

According to NUREG-1150, an RCS-to-containment pressure difference of 1.38 MPa can be considered the cutoff pressure for the prevention or mitigation of the effects of DCH. Although values as high as 5.8 MPa have been put forth as the DCH cutoff pressure, the value reported in NUREG-1150 was used for the basis of this report's conclusions.

SCDAP/RELAP5/MOD3 Code and Model Descriptions

The phenomenological behavior of the selected PWRs were evaluated using the SCDAP/RELAP5/MOD3 computer code package.[5] SCDAP/RELAP5/MOD3 is a light water reactor transient analysis computer code that can be used to simulate a wide variety of system transients of interest to light water reactor safety, but it is specifically designed to calculate the behavior of the RCS during severe accidents. The reactor core, RCS, secondary system including feedwater and steam/turbine trains, and system controls can be simulated. The code models are designed to permit simulation of severe accidents up to the point of reactor vessel failure.

The SCDAP/RELAP/MOD3 models used in these analyses simulated the reactor vessel, the piping in all primary coolant loops, the pressurizer, steam generators, and selected parts of the secondary systems. Three parallel flow channels were modeled in the reactor vessel from the lower plenum through the core to the upper reactor vessel head. If the appropriate conditions exist, this arrangement will allow development of in-vessel natural circulation. External surfaces of the reactor vessel were assumed to be adiabatic. The three core channels were selected so that similarly powered fuel assemblies would be grouped together. This grouping was based on the equilibrium cycle assembly power sharing of the selected PWRs. Fuel rods, control rods, and empty guide tubes were simulated for each core channel. Input is required to define certain parameters that control severe core damage progression. In general, best estimate parameter values were selected to provide a best estimate to the time of lower head failure.

Both fluid volumes and heat structures were included to represent the primary coolant loop piping, the pressurizer and associated surge line, and steam generators. The accumulators were the only emergency core cooling system that required simulation because it is only system operational during a station blackout transient. The steam generator main feedwater system and associated piping are needed to establish steady-state conditions prior to transient initiation. Auxiliary feedwater systems were not modeled because they are not operational in this scenario. The external surfaces of all heat structures were assumed to be adiabatic.

A single valve was used to represent all PORVs connected to the pressurizer. The valve was appropriately sized to represent the total PORV capacity of the NPP. Similarly, a single valve was used to represent all safety relief valves. It was assumed that there was sufficient support equipment capacity to allow operation of the valves throughout the transient.

An axisymmetric mesh was used to represent the reactor vessel lower head to determine the time to lower head failure. The outer mesh intervals were used to simulate the lower head vessel wall and the internal mesh intervals initially represent the primary coolant filling the lower head. During core relocation, the coolant can boiloff, be displaced by debris, or both. Convection and radiation heat transfer were modeled at all interfaces between the coolant and debris. In addition, convective and radiative heat transfer were modeled along the vessel wall at all nodes that are not submerged by debris. The external surface of the lower head was assumed to be adiabatic.

Intentional Depressurization Analyses

This section will discuss the evaluation of the four PWRs selected. Three areas were evaluated to determine a PWR's capability to employ the intentional depressurization strategy. These were (1) phenomenological behavior, (2) equipment reliability, and (3) operational performance.

As stated in the previous section, the phenomenological behavior of each NPP was made using the severe accident code package SCDAP/RELAP5/MOD3. The TMLB' station blackout transient was selected for evaluation is defined as a loss of offsite and onsite ac power and the loss of steam driven auxiliary feedwater. The only source of water addition is the accumulators.

A total of six SCDAP/RELAP5/MOD3 analyses were performed; one each for Surry and Sequoyah, and two each for Calvert Cliffs and Oconee. Multiple calculations were necessary for Calvert Cliffs and Oconee to adequately bound the uncertainties during core relocation and lower head attack. A summary of each of the six analyses is presented in the following sections.

The second area of evaluation was equipment reliability. The primary focus of this evaluation was the PORV(s). The likelihood of their availability and failure throughout the transient was investigated. The results of these investigations indicate that there is insufficient capacity of the PORV support systems to allow PORV operation for the duration of the transient. Operation of the PORV(s) may require service air, dc battery power, or both. As long as ten hours may be required for PORV availability. None of the systems evaluated could support PORV operation for this duration.

The likelihood of PORV failure during the transient is believed to be high. However, because no data exists for PORV operation under the extreme conditions that would exist during a severe accident, it cannot be stated with certainty whether the valves will fail in an open or closed position. Failure in an open position should not impact calculation results. However, failure in a closed position may result in HPME.

Also of interest is the likelihood of ex-vessel piping failures. Creep rupture analyses of the hot leg and surge line piping were performed, although their effects were not accounted for in the calculation results. The purpose of these evaluations was to determine the possibility of RCS depressurization

through their failure sufficiently prior to lower head failure to prevent DCH. The SCDAP/RELAP5/MOD3 analyses were performed assuming ex-vessel piping and PORV failures do not occur. Although ex-vessel piping failures would be effective in reducing the RCS pressure sufficiently prior to lower head failure to mitigate the effects of DCH, strategies that do not rely on such system component failures are preferred.

The final area of evaluation was operational performance. The operator's capability to perform intentional depressurization strategy using existing plant procedures was assessed. Based on this evaluation, current plant procedures do not allow for intentional depressurization under the conditions that would be encountered during the TMLB' transient and there would be a 100% probability of strategy failure. If operating procedures were modified and operators had at least 20 minutes to act, it is believed that intentional depressurization could be performed with a 96% probability of success.

Surry SCDAP/RELAP5/MOD3 Analysis

The Surry NPP is a Westinghouse 3-loop PWR and has the smallest capability of any PWR in Westinghouse Group 1 to employ the intentional depressurization strategy. The Surry analysis assumes a maximum breakup of the relocating core material into small debris particles. Because this assumption results in the maximum heat transfer between the relocating material and the liquid in the lower head, this scenario should result in the maximum pressure increase during relocation. In addition, because the stored energy of the relocating material is transferred to the lower head liquid, additional time would be required for the debris to heat up sufficiently to fail the lower head. This scenario should also result in the maximum time to lower head failure.

At the initiation of the TMLB' accident sequence, the reactor is scrammed and the reactor coolant pumps (RCPs) are tripped off. As the RCPs coast down, coolant is transported from the vessel to the steam generators. Full loop circulation of the coolant continues even after the RCPs completely coast down because the heat sink of the steam generator secondary side water volume sets up a natural circulation flow path for heat removal from the core. However, because there is no feedwater supplying water to the steam generators, full loop natural circulation continues only until the steam generator secondary side water volume becomes depleted. At this point, the RCS rapidly heats up and pressurizes until the PORV setpoint pressure is reached. The RCS pressure response for this analysis is presented in Figure 2.

Since the RCS coolant inventory is continually being removed while the PORVs cycle, the core eventually begins to uncover. As the core becomes uncovered, the fuel rod cladding in the upper regions of the core becomes steam cooled. However, as indicated by the maximum cladding temperature of Figure 3, the steam flow rate past the cladding is inadequate to maintain an equilibrium temperature. As the fuel cladding temperature increases, the steam becomes superheated, the core exit steam temperature reaches 922 K, and the PORVs are latched open.

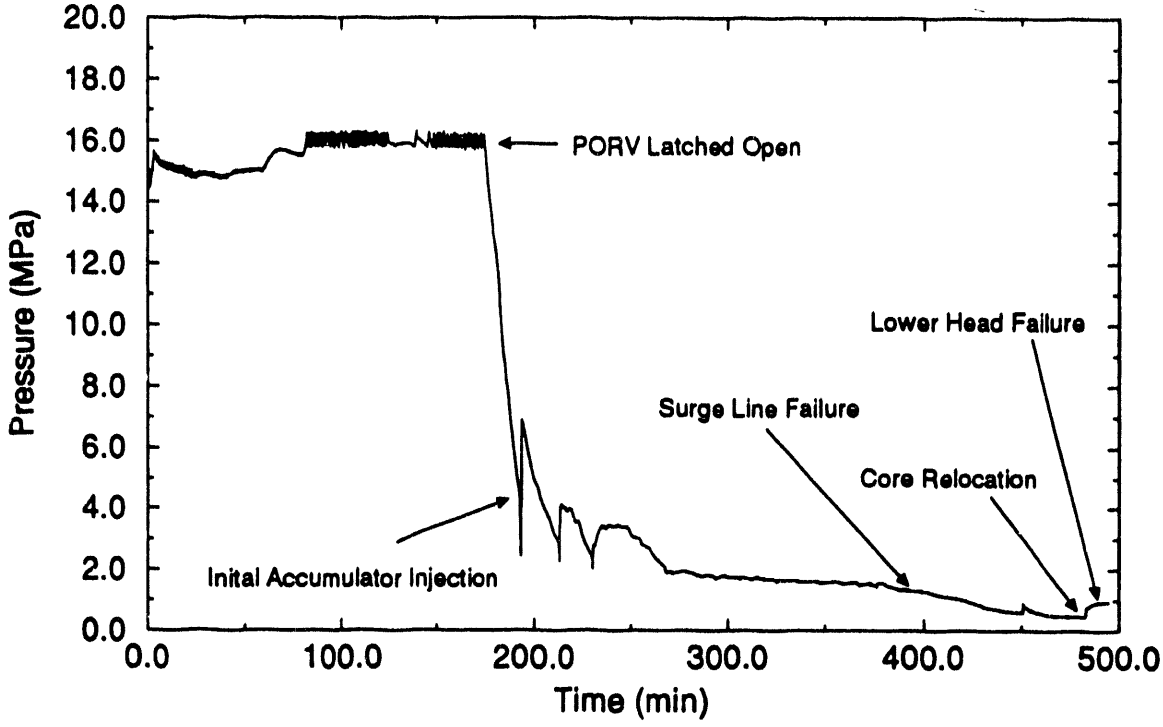


Figure 2. Surry RCS pressure response during intentional depressurization.

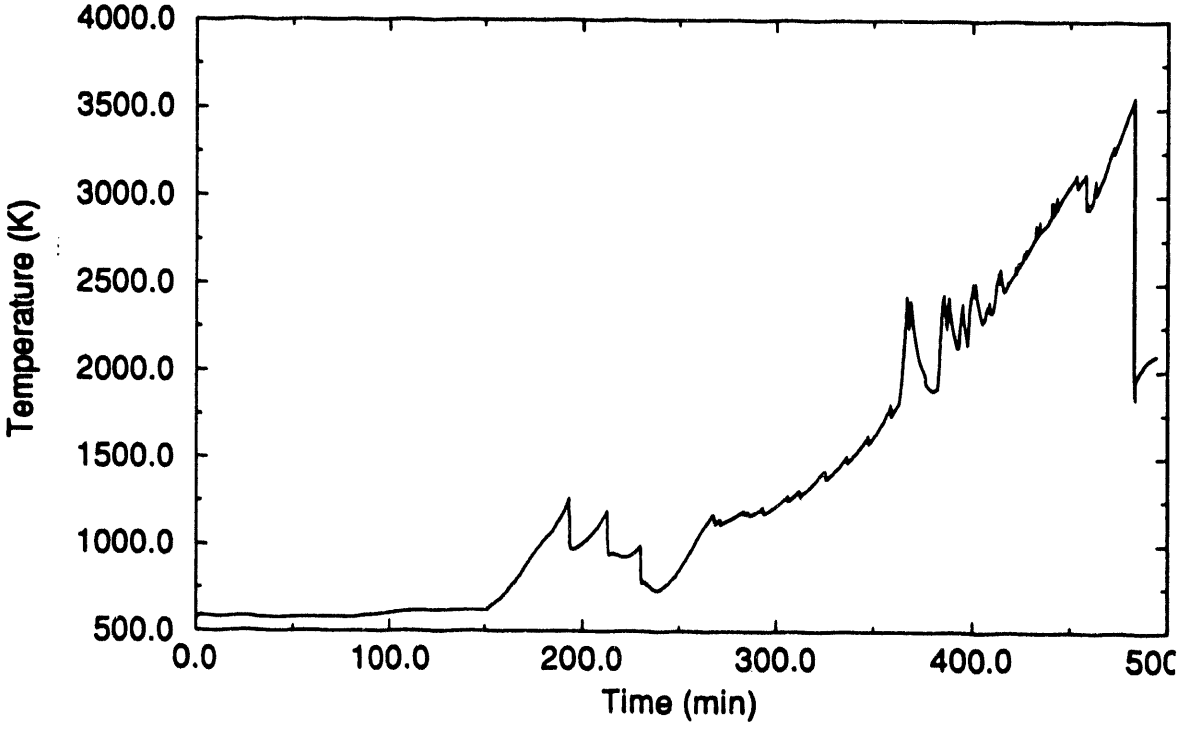


Figure 3. Surry maximum cladding temperature during intentional depressurization.

After the PORVs are latched open the RCS pressure begins to decrease until the accumulator setpoint pressure is reached. Depressurization of the RCS to the accumulator setpoint pressure takes 18.2 minutes. Once accumulator injection begins, injection cycles are predicted to continue until the accumulators are empty. As the accumulator liquid enters the vessel, energy is removed from the vapor in the cold leg, downcomer, and lower head as the injected fluid is heated. As energy is removed from the vapor it condenses causing the RCS pressure to decrease and allowing more accumulator liquid to be injected. This self-feeding process continues until the liquid level encounters heated core structures. The resulting vaporization of the liquid causes the pressure to increase rapidly. This effectively halts the accumulator injection until flow out of the PORV reduces the RCS pressure back to the accumulator actuation pressure.

During the time required to reduce the RCS pressure the core structures begin to heat up once again. Once the accumulator actuation pressure is reached for the next injection, this cycle is repeated. However, with each additional cycle the core structure temperature rise is not as great, the pressure increase following injection becomes less, and the time to the next cycle decreases. Accumulator injections maintain the liquid level in the core region until the accumulators are empty. Once the accumulators are empty, the RCS pressure smoothly decreases until core relocation begins.

The fuel begins melting when the UO_2 melt temperature of 3123 K is exceeded. As the fuel melts, a crust of metallic material is formed which contains the molten material in a pool at the bottom of the core. Before the molten material can relocate to the vessel lower head, the crust bottom must thin and fail. The mechanism for thinning the crust is by convective heat transfer at the pool/crust interface as natural circulation of the molten material occurs within the pool.

As the corium relocates, the small debris particle relocation mode dictates that the core material will be quenched to the saturation temperature upon contact with the liquid in the lower head. Because of the rapid energy transfer between the relocating core material and the liquid in the lower head, whatever liquid is not vaporized is carried out of the lower head with the steam. After 0.7 s of relocation, there is insufficient liquid in the lower head to quench the relocating material and the remainder of the relocation, roughly 99% of the total mass, relocates as a cohesive molten stream.

As the molten core material relocates to the lower head in a cohesive stream, the reactor vessel wall begins to heat up dramatically. At 489 minutes, creep rupture failure of the lower head is predicted. Because the amount of mass relocated with small debris particle relocation mode was small there was minimum heat transfer to the lower head liquid and the pressure rise associated with quenching this mass was small. The RCS-to-containment pressure difference at the time of lower head failure is predicted to be 0.76 MPa. Failure of the surge line was predicted to occur at 393 minutes, almost 100 minutes prior to lower head failure.

Sequoyah SCDAP/RELAP5/MOD3 Analysis

The Sequoyah NPP is a Westinghouse 4-loop PWR and has the smallest capability of any PWR in Westinghouse Group 2 to employ the intentional depressurization strategy. A single pressure bounding calculation was also performed for Sequoyah. This analysis assumes a maximum breakup of the relocating core material into small debris particles.

The predicted thermal-hydraulic phenomena is similar to that of Surry. RCS pressure reduction to the accumulator setpoint pressure takes slightly longer in this analysis because of Sequoyah's smaller PORV capacity. Like Surry, however, core heatup, melt, and relocation to the lower head does not occur until the accumulators empty. The predicted Sequoyah RCS pressure response during intentional depressurization is shown in Figure 4.

As the RCS coolant inventory heats up to the saturation temperature of the PORV setpoint pressure, it swells until the pressurizer is completely liquid filled. The PORVs begin discharging liquid and continue to cycle until the average coolant temperature in the core region reaches saturation temperature. The core region begins to void at this time and the RCS pressure begins to increase. Energy cannot be removed through the PORVs quickly enough to relieve this pressure increase and the RCS pressure continues to increase until the safety relief valve (SRV) setpoint pressure is reached. The SRVs cycle once before the pressure peaks and begins to decrease. The RCS pressure continues to decrease to the PORV setpoint pressure and the PORVs once again cycle to maintain RCS pressure. This pressure response was not evident when the average coolant temperature reached saturation in the Surry analysis. This is because of the differences in PORV relief capacity of these two NPPs. Surry, with the higher relief capacity is able to maintain an energy removal rate in excess of the decay heat generation rate.

Since the RCS coolant inventory is continually being depleted while the PORVs cycle, the core begins to uncover. As the core becomes uncovered, the fuel rod cladding in the upper regions of the core becomes steam cooled. However, as indicated by the maximum cladding temperature of Figure 5, the steam flow rate past the cladding is inadequate to maintain an equilibrium temperature. As the fuel cladding temperature increases, the steam becomes superheated, the core exit steam temperature reaches 922 K, and the PORVs are latched open.

Once the PORVs are latched open the RCS pressure begins to decrease until the accumulator setpoint pressure is reached. This occurs 24.0 minutes after latching the PORVs open. The time for RCS pressure reduction is one third longer than was predicted for Surry. That calculation predicted an 18.2 minute pressure reduction time. The longer time to depressurize is consistent with the large difference in PORV ratios and the relatively small difference in accumulator setpoint pressure.

Once accumulator injection begins, injection cycles are predicted to continue until the accumulators are empty. From Figure 4 it is seen that the pressure response during accumulator injection is similar for Sequoyah as was

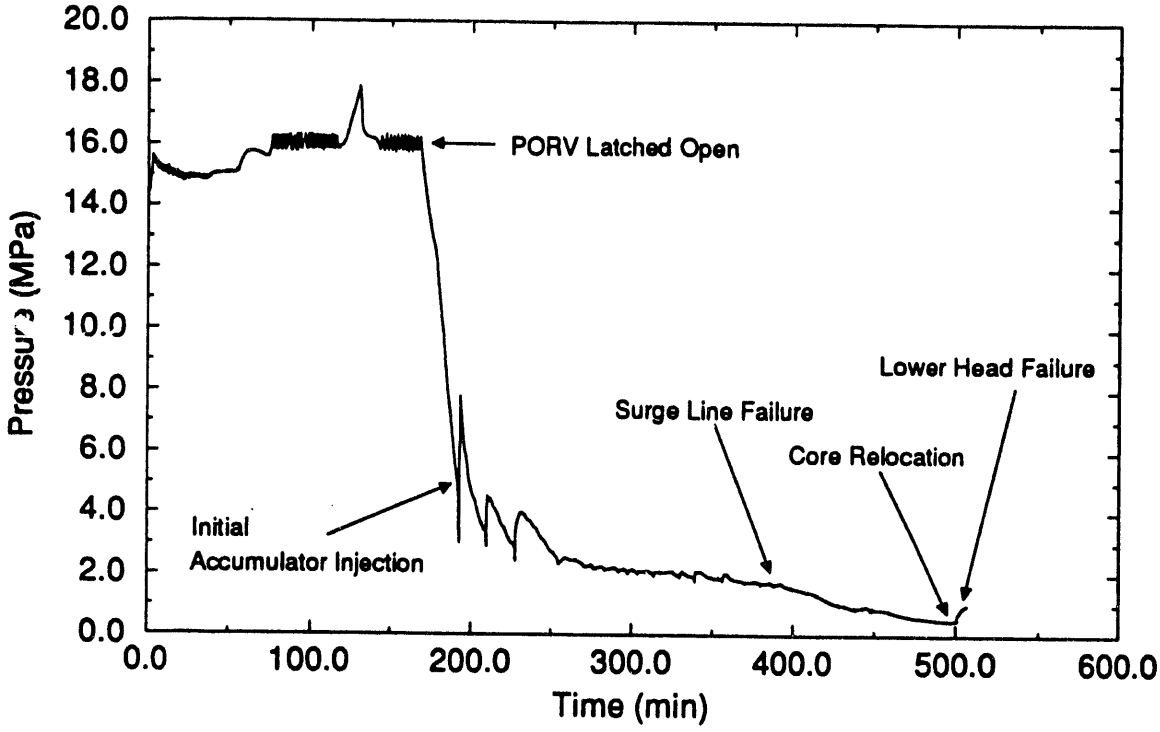


Figure 4. Sequoyah RCS pressure response during intentional depressurization.

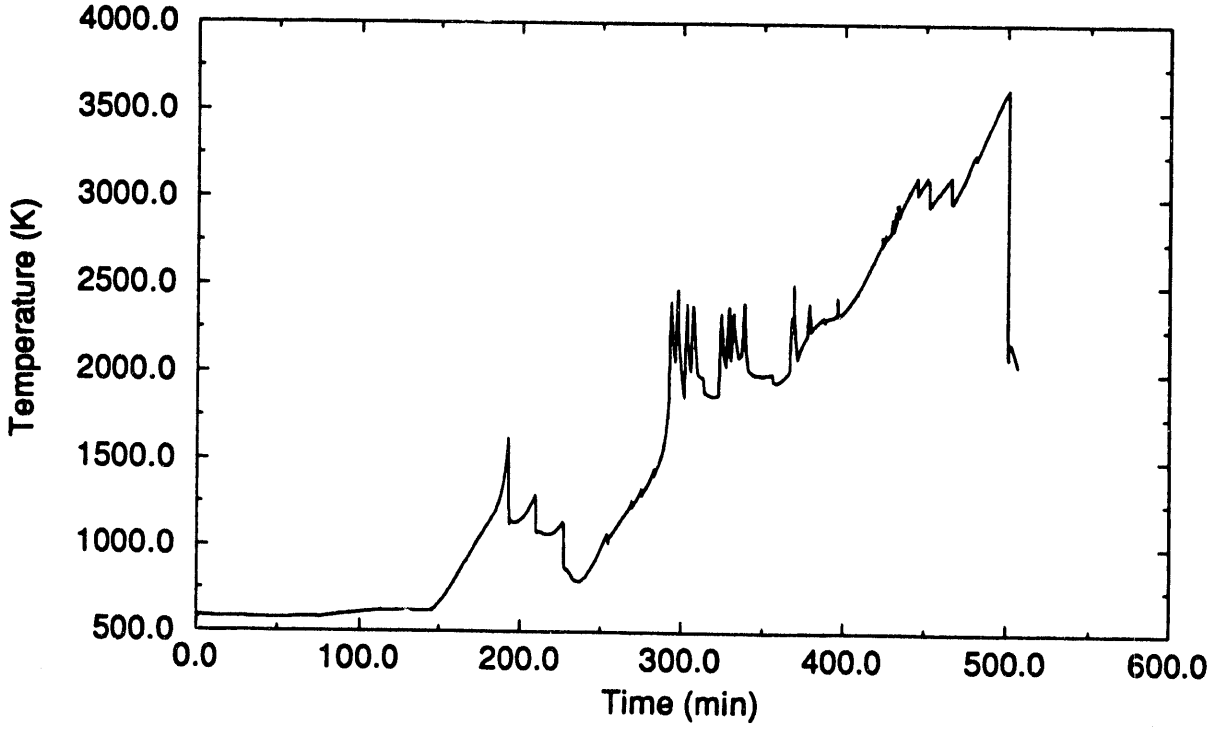


Figure 5. Sequoyah maximum cladding temperature during intentional depressurization.

observed for Surry (Figure 2). The initial injections result in a pressure decrease, which allows more accumulator liquid to be injected until the vessel level rises and comes into contact with heated vessel structures. The liquid is then vaporized causing the RCS pressure to increase and halt accumulator injection. The RCS pressure response to later injections is minimal resulting in an uneven, but steady pressure decrease as the accumulators empty. Once the accumulators are completely empty, the RCS pressure decreases until core relocation begins.

As the corium relocates, the small debris particle relocation mode dictates that the core material will be quenched to the saturation temperature upon contact with the liquid in the lower head. Because of the rapid energy transfer between the relocating core material and the liquid in the lower head, some of the liquid in the lower head is entrained and removed from the reactor vessel with the steam. After 0.4 s of relocation, there is insufficient liquid in the lower head to quench the relocating material and the remainder of the relocation, roughly 99% of the total mass, relocates as a cohesive molten stream.

As the molten core material relocates to the lower head in a cohesive stream, the reactor vessel wall begins to heat up dramatically. At 507 minutes, creep rupture failure of the lower head is predicted. Because the amount of mass relocated with small debris particle relocation mode was small there was minimum heat transfer to the lower head liquid and the pressure rise associated with quenching this mass was small. The RCS-to-containment pressure difference at the time of lower head failure is predicted to be 0.82 MPa. Failure of the surge line was predicted to occur at 384 minutes, over 100 minutes prior to lower head failure.

Calvert Cliffs SCDAP/RELAP5/MOD3 Analyses

Calvert Cliffs is a 2x4-loop (2 hot legs, 4 cold legs) CE PWR and has an intentional depressurization capability near the bottom of the CE Group. Two analyses were performed to bound the pressure behavior and the time to lower head failure following core relocation. These bounding analyses used different assumptions regarding the relocation mode of the relocating core material. The first analysis examines the assumption of maximum breakup of the relocating core material as small debris particles which would result in maximum interaction between the relocating core material and the lower head liquid. This scenario results in the maximum heat transfer between the relocating material and the lower head liquid and therefore a maximum pressure increase during relocation and the maximum time to lower head failure.

The second relocation mode examines the impact of no breakup of the relocating core material and relocation occurs as a cohesive molten stream with minimal interaction between the relocating core material and the lower head liquid. This scenario results in the minimum heat transfer between the relocating core material and the lower head liquid and therefore a minimum pressure increase during relocation and the minimum time to lower head failure. Both calculations were performed until lower head failure is predicted. Multiple core relocations were predicted to occur during the

Calvert Cliffs analyses resulting in different lower head failure times for the two relocation modes.

The RCS pressure response for the small debris particle relocation mode is shown in Figure 6. The PORV setpoint pressure is reached soon after steam generator dryout. As the RCS liquid heats up to the saturation temperature corresponding to the PORV setpoint pressure, it swells until the pressurizer is completely liquid filled. The PORVs begin discharging liquid and the pressure begins increasing towards the SRV setpoint pressure. Finally, the pressure peaks just short of the SRV setpoint pressure. The energy removal rate through the PORVs begins to exceed the core decay energy generation rate and the pressure begins to decrease. The RCS pressure continues to decrease to the PORV setpoint pressure and the PORVs once again cycle to maintain RCS pressure. This pressure response was not evident as the average coolant temperature increased towards saturation in the Surry analysis. This is because of the differences in PORV relief capacity of these two NPPs. Surry, with the larger relief capacity, is able to maintain an energy removal rate in excess of the decay heat generation rate throughout this period.

Since the RCS coolant inventory is continually being removed while the PORVs cycle, the core eventually begins to uncover. As the core becomes uncovered, the fuel rod cladding in the upper regions of the core becomes steam cooled. However, as indicated by the maximum cladding temperature of Figure 7, the steam flow rate past the cladding is inadequate to maintain an equilibrium temperature. As the fuel cladding temperature increases, the steam becomes superheated, the core exit steam temperature reaches 922 K, and the PORVs are latched open.

Once the PORVs are latched open the RCS pressure begins to decrease until the accumulator setpoint pressure is reached. This occurs 45.2 minutes after latching open the PORVs. The time for RCS pressure reduction is over twice as long as was predicted for Surry. That calculation predicted an 18.2 minute pressure reduction time.

Once accumulator injection begins, only three injection cycles are predicted to occur. A substantial volume of liquid is injected during each of these injections and about 86% of the total accumulator liquid inventory is injected before lower head failure occurs. The large injections result from the low RCS pressure at the time the accumulator initiates. As the accumulator liquid enters the cold leg, downcomer, and vessel, energy is removed from the vapor in the lower head to heat the injected fluid. As energy is removed from the vapor it condenses causing the RCS pressure to rapidly decrease. As the pressure decreases, more accumulator liquid is injected. This self-feeding process continues until the liquid level encounters heated core structures. The resulting vaporization of the liquid as it comes into contact with these structures causes the pressure to increase rapidly. This effectively halts the accumulator injection.

Because more time was required to reach the accumulator setpoint pressure, more core damage occurs prior to accumulator injection and the average core temperature is higher than what was seen for Surry. The higher

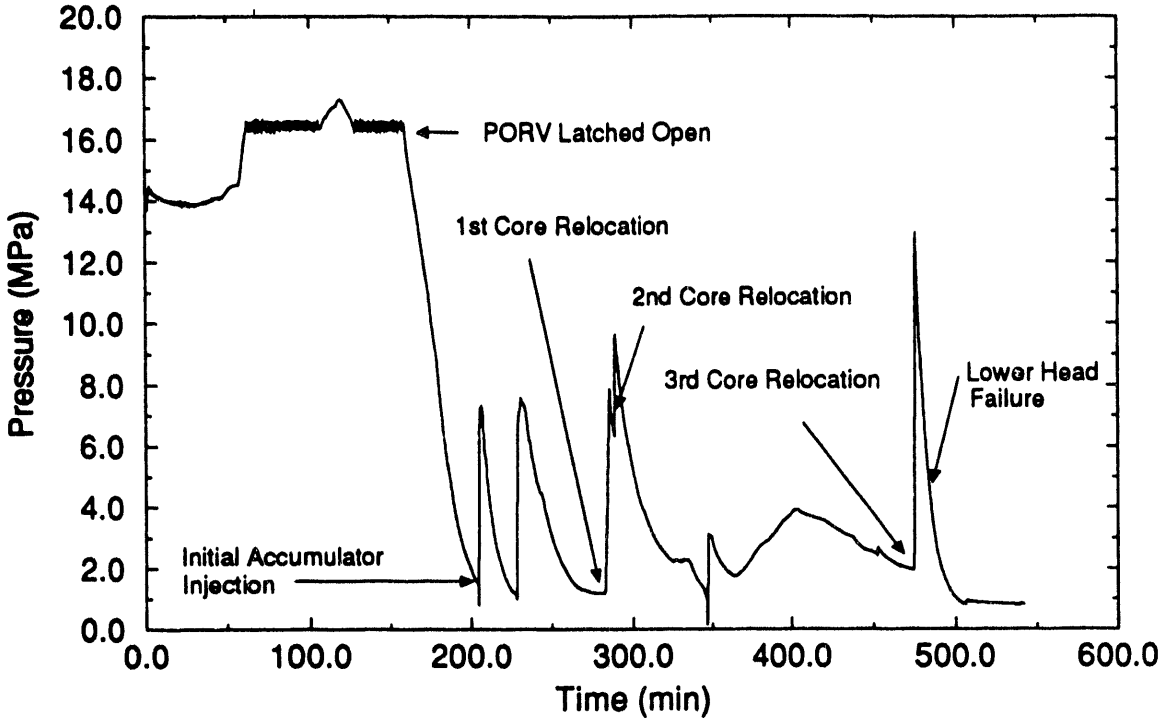


Figure 6. Calvert Cliffs small debris particle relocation mode RCS pressure response during intentional depressurization.

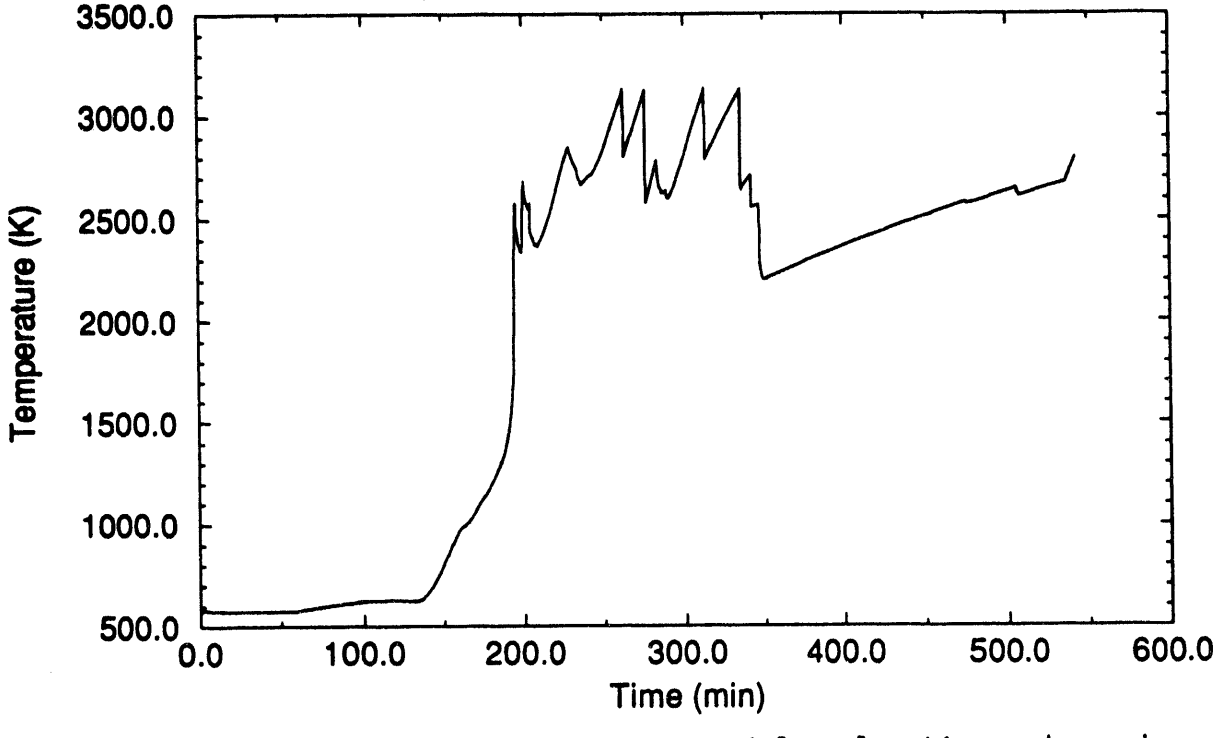


Figure 7. Calvert Cliffs small debris particle relocation mode maximum cladding temperature during intentional depressurization.

core structure temperatures result in fuel rod cladding fragmentation during the initial accumulator injection. Accumulator injections become ineffective to cool the core because of the resulting debris blockages. The core debris begins to heat up and melt. Multiple molten pools are predicted to form and relocate before lower head failure is predicted. The first molten pool is drained by two relocations which are small and are completely quenched by the lower head liquid.

Another molten pool forms before the third and final accumulator injection cools this pool sufficiently that an additional 131 minutes is required to heat up and cause bottom crust failure. Because there is insufficient liquid in the lower head to quench the entire relocation, 0.9 minutes after failure of the lower crust the core material begins to relocate as a cohesive molten stream.

As the molten core material relocates to the lower head in a cohesive stream, the reactor vessel wall begins to heat up dramatically. At 484 minutes, creep rupture failure of the lower head is predicted. The RCS-to-containment pressure at the time of failure is 4.2 MPa.

Failure of the surge line was not calculated to occur during this analysis because core blockages prevented the normal flow of steam through the core to the hot leg containing the surge. Reverse flow through the RCS loops was initiated with heat continually being removed from the steam and deposited in the RCS structures. But because of the large mass of the RCS structures and the small steam flow through these structures, the average structure temperature of any RCS component, other than the surge line, does not exceed 800 K during this entire time period.

For the cohesive molten stream relocation mode, calculation results are the same up to the time of the first molten pool relocation. Lower head failure is predicted to occur following this relocation at 296 minutes. This is 188 minutes before the predicted lower head failure time of the small debris particle relocation mode analysis. Reactor vessel wall heatup occurs much more rapidly for the cohesive molten stream relocation mode because the minimum heat transfer between the relocating core material and the lower head liquid allows almost all the energy of the relocating material to be retained. The RCS-to-containment pressure difference is predicted to 1.8 MPa. Surge line failure was not predicted for this analysis.

Oconee SCDAP/RELAP5/MOD3 Analyses

Oconee is a 2x4-loop B&W PWR and has an intentional depressurization capability near the bottom of the B&W Group. Two bounding analyses were performed for the Oconee NPP also. However, for the Oconee analyses only one molten pool was predicted to form and relocate compared to the three molten pool relocations of the Calvert Cliffs analyses.

The RCS pressure response for the Oconee small debris particle relocation mode analysis is shown in Figure 8. PORV activation occurs much more rapidly in this analysis compared to the previous NPPs because of the relatively small

water inventory of the Oconee once-through steam generators (OTSGs) secondary side. The secondary side inventory is approximately 50% smaller than the Surry steam generator. This results in the steam generators drying out much more quickly. In addition, the heat removal rate of the OTSG cannot keep pace with the decay heat generation rate in the core. This causes the coolant temperature and the RCS pressure to rise until the PORV actuates 3 minutes into the transient.

Once the PORV setpoint is reached, the PORV cycles to maintain RCS pressure, but because of the small relief capacity of the Oconee PORV, energy cannot be removed from the RCS quickly enough to maintain RCS pressure. The RCS coolant inventory continues to heat up and swell, completely filling the pressurizer before the average coolant temperature reaches saturation. The coolant temperature continues to increase and saturation temperature is reached. The core region begins to void increasing the RCS pressure above the PORV setpoint pressure. The PORV is incapable of removing enough energy from the RCS to maintain a balance with the decay heat generation rate and the RCS pressure continues to increase until the SRV setpoint pressure is reached. After 22 minutes the heat removal rate through the SRVs and PORV exceeds the core decay heat generation rate and the RCS pressure begins to decrease.

Since the RCS coolant inventory is continually being removed during this period, the core begins to uncover. As the core becomes uncovered, the fuel rod cladding in the upper regions of the core becomes steam cooled. However, the steam flow rate past the cladding is inadequate to maintain an equilibrium temperature. The maximum cladding temperature is presented in Figure 9. As the fuel cladding temperature increases, the steam becomes superheated and the core exit steam temperature reaches 922 K. At this point the PORV is latched open. This occurs soon after the SRVs cease operation, but before the RCS pressure has allowed the PORV to close.

Once the PORV is latched open the RCS pressure begins to decrease until the core flood tank (CFT) setpoint pressure is reached. This occurs 93 minutes after latching open the PORV. The time for RCS pressure reduction is over five times longer than was predicted for Surry. That calculation predicted an 18.2 minute pressure reduction time.

Before CFT injection begins, however, significant core damage has already occurred. Fuel melt and molten pool formation has already begun. Once CFT injections begin (CFTs are equivalent to accumulators in CE and Westinghouse PWRs except that CFTs inject directly into the reactor vessel instead of the cold leg piping), all injection cycles have a short duration, injecting only small quantities of water. This is because of the slow RCS pressure reduction caused by the small PORV capacity. The RCS pressure is barely decreased below the CFT setpoint before the injected liquid reaches the core and is vaporized, raising the RCS pressure above the CFT setpoint. The small CFT injections provide inadequate core cooling and the fuel continues to melt until bottom crust failure and relocation to the lower head occurs.

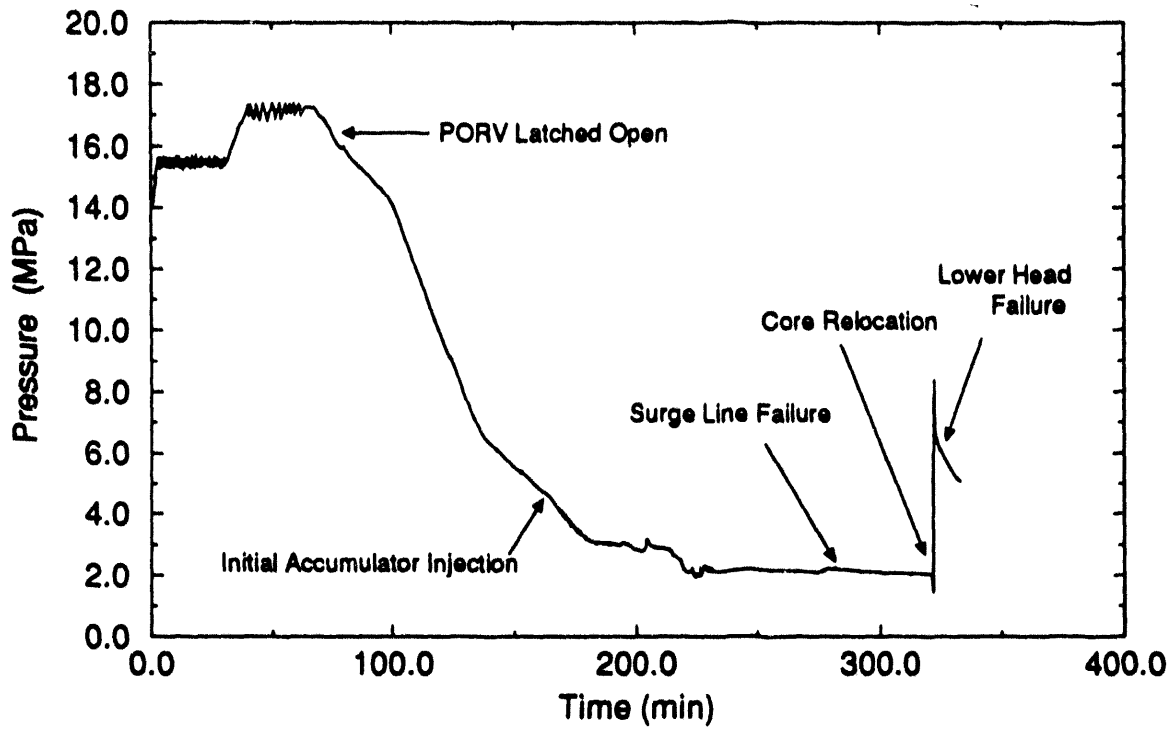


Figure 8. Oconee small debris particle relocation mode RCS pressure response during intentional depressurization.

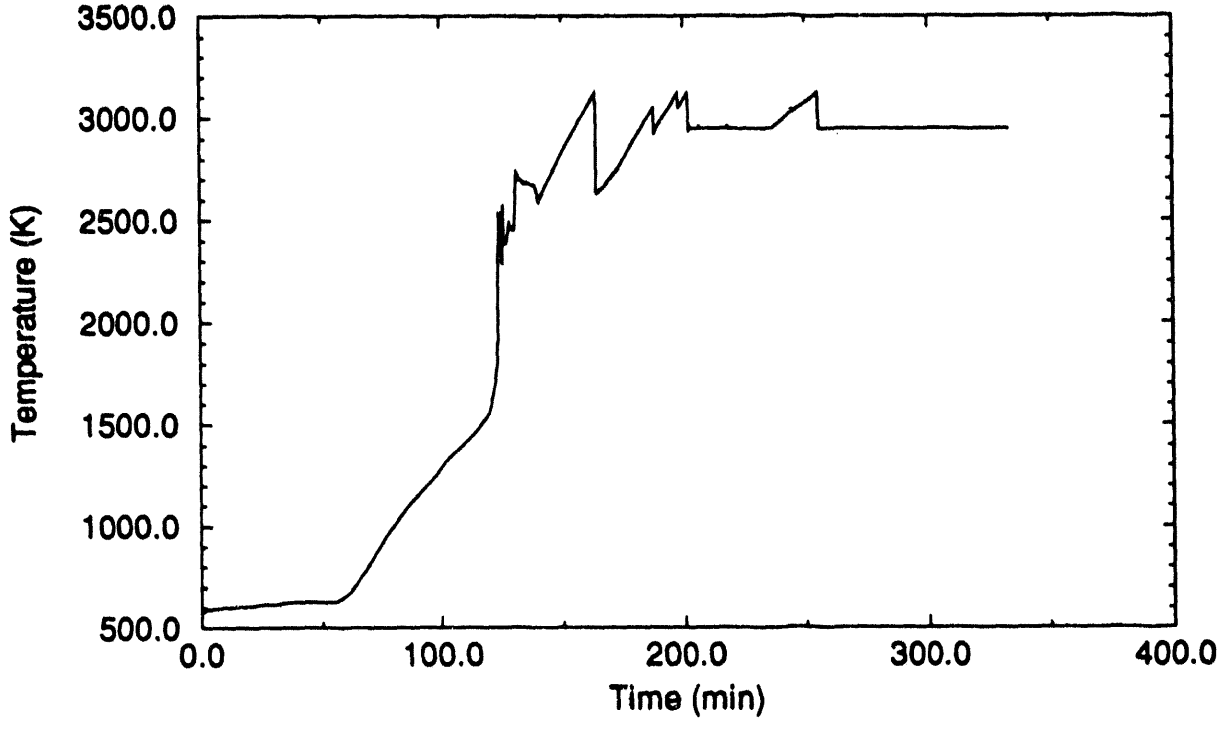


Figure 9. Oconee small debris particle relocation mode maximum cladding temperature during intentional depressurization.

Just prior to core relocation the final CFT injection occurs. The CFT injection causes the RCS pressure to decrease as the injected subcooled liquid begins to condense the vapor in the vessel lower plenum. The pressure decrease is reversed and the CFT injection halted by the relocating core material.

As the corium relocates, the small debris particle relocation mode of this case dictates that upon contact with the remaining reactor coolant, the corium will be cooled and its temperature lowered to saturation temperature. This process occurs for the first 0.4 minutes of the relocation period. After this time there is insufficient liquid in the vessel lower head to quench the relocating material and the core material relocates as a cohesive molten stream.

During the initial relocation mode, the rapid energy transfer between the relocating core material and the coolant causes the vapor generation rate to exceed the PORV relief capacity. This results in an RCS pressure increase from 1.5 to 8.4 MPa. Once the coolant in the lower head is completely vaporized, the RCS pressure begins to decrease as steam is removed from the RCS through the PORV. As the molten core material relocates to the lower head in a cohesive stream, the reactor vessel wall begins to heat up dramatically. At 328 minutes, creep rupture failure of the lower head is predicted. The RCS-to-containment pressure difference at the time of lower head failure is predicted to be 5.5 MPa. Prior to core relocation and lower head failure, failure of the surge line is expected to occur at 280 minutes.

For the cohesive molten stream relocation mode, calculation results are the same up to the time of the first molten pool relocation. Lower head failure is predicted to occur following this relocation at 328 minutes. This is only 2 minutes before the predicted lower head failure time of the small debris particle relocation mode analysis. Reactor vessel wall heatup occurs more quickly for the cohesive molten stream relocation mode because the minimum heat transfer between the relocating core material and the lower head liquid allows almost all the energy of the relocating core material to be retained. The RCS-to-containment pressure difference is predicted to 1.5 MPa. Surge line failure was predicted to occur at 280 minutes for this analysis also.

CONCLUSIONS

Table 1 provides a summary of the SCDAP/RELAP5/MOD3 results for all six calculations. It should be noted that although surge line failure is predicted in three of the four PWRs, the effects of such a failure are not accounted for in the lower head failure time or the RCS-to-containment pressure difference at the time of lower head failure.

For both the Surry and Sequoyah analyses, surge line failure is predicted to occur approximately 100 minutes prior to lower head failure. The RCS-to-containment pressure difference is predicted to be below the 1.38 MPa NUREG-

Table 1. Summary of SCDAP/RELAP5/MOD3 intentional depressurization results.

Nuclear Power Plant	Surge Line Failure Time (minutes)	Lower Head Failure Time[a] (minutes)	Pressure Difference at Lower Head Failure Time[a] (MPa)	Comments
Surry	393	489	0.76	No HPME.
Sequoyah	384	507	0.82	No HPME.
Calvert Cliffs	-	296[b]/484[c]	1.8[b]/4.2[c]	HPME. Early core blockage prevented significant surge line heatup.
Oconee	280	328[b]/330[c]	1.5[b]/5.5[c]	No HPME. Depressurization likely through surge line failure.

a Calculated results do not account for any ex-vessel piping failures.
b Results for cohesive molten stream relocation mode.
c Results for small debris particle relocation mode.

1150 DCH cutoff pressure at the time of lower head failure in both of the analyses. Using this criteria, HPME would not be expected for either NPP. Depressurization of the RCS would likely occur through the PORVs or surge line failure sufficiently prior to lower head failure to prevent HPME. Because similar thermal-hydraulic behavior would be expected in the remaining members of Westinghouse Group 1 and 2, it is likely that the intentional depressurization strategy could be successfully employed at all Westinghouse PWRs.

Calvert Cliffs is the only plant where surge line failure was not predicted to occur. Blockages in the core region prevented significant surge line heatup. These blockages also resulted in the formation of multiple molten pools and relocations. An analysis of cohesive molten stream relocation mode resulted in the prediction of lower head failure almost 200 minutes prior to that predicted for the small debris particle relocation mode. The RCS-to-containment pressure difference for these analyses were 1.8 and 4.2 MPa, respectively. Because the pressure difference in both cases exceeds the 1.38 MPa DCH cutoff pressure criteria and no ex-vessel piping failures are predicted prior to lower head failure, HPME is likely for Calvert Cliffs and the remaining members of the CE Group.

Two relocation mode calculations were also performed for Oconee. Both calculations predicted surge line failure would occur at 280 minutes. Only one molten pool was predicted to form and relocate for these analyses. In both relocation modes, lower head failure is predicted to occur at approximately the same time, 328 minutes for the cohesive molten stream relocation mode versus 330 minutes for the small debris particle relocation mode. However, the RCS-to-containment pressure difference at the time of lower head failure was predicted to vary from 1.5 MPa for the cohesive molten stream relocation mode to 5.5 MPa for the small debris particle relocation mode. Although the RCS-to containment pressure difference results indicate HPME would be likely, depressurization of the RCS sufficiently prior to lower head failure would likely occur through the failed surge line. Similar results would be expected for the remaining members of the B&W Group.

The evaluations of the study NPPs indicate that some plant modifications may be necessary. These modifications primarily affect the PORV(s) and operation procedures. There is a high probability that a block valve on one of the PORV lines will be closed as a result of leakage. Because these block valves operate using only ac power, it would be impossible to open them during a TMLB′ sequence. The effect of a closed block valve causes its PORV to be unavailable for use during intentional depressurization, significantly increasing the time to depressurize the RCS. The power source of the PORV block valves should be converted to dc power to ensure PORV availability at the start of the transient.

In addition, the capacity of the PORV support systems should be increased to ensure PORV availability throughout the entire transient. Both the dc power and supply of pressurized air required to force the Surry PORVs open and maintain them in an open position would not support PORV operation for the entire eight to nine hour time period of the TMLB′ sequence. The dc power supply of the Oconee PORV can support PORV operation for a one hour period only. The Calvert Cliffs PORVs are ac powered and would be unavailable throughout the entire TMLB′ station blackout sequence.

An assessment of PORV reliability indicates that there is a likelihood of their failure during intentional depressurization. However, insufficient data exists to determine whether the PORVs will fail in an open or closed position. PORV closure results in the unavailability of the PORVs for the remainder of the sequence and may result in HPME.

The emergency operating procedures should be revised to instruct plant operators to perform intentional depressurization. Current emergency operating procedures (EOPs) at Surry, Calvert Cliffs, and Oconee do not instruct the plant operators to initiate RCS depressurization during a TMLB′ sequence. A human reliability analysis (HRA) at each of these NPPs indicate that if procedure and equipment modifications are made, there is a probability that the plant personnel could successfully initiate intentional depressurization.

It is further recommended that certain uncertainties be considered before implementing the intentional depressurization strategy. The exact magnitude

of the RCS-to-containment pressure difference below which the effects of DCH will most likely be prevented or mitigated is unknown. A DCH cutoff pressure difference higher than the 1.38 MPa considered in NUREG-1150 may result in the acceptance of all PWRs for use of the intentional depressurization strategy. A pressure difference lower than 1.38 MPa could potentially exclude all PWRs. This uncertainty is believed to affect only those members of the CE Group as Westinghouse and B&W PWRs would be expected to be depressurized sufficiently prior to lower head failure to prevent HPME.

There are uncertainties associated with the core damage progression models and assumptions that influence the time to lower head failure and the RCS pressure at the time of lower head failure. However, these uncertainties are believed to have been minimized through the selection of best-estimate values for those parameters influencing core damage progression and the performance of bounding heat transfer calculations for Calvert Cliffs and Oconee.

In summary, the intentional depressurization may be a viable strategy for the minimization of the effects of DCH. However, prior to taking any accident management actions, consideration of the uncertainties related to PORV reliability and DCH cutoff pressure and a cost benefit analysis of equipment and procedure modifications should be made.

REFERENCES

1 U. S. Nuclear Regulatory Commission, *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*, NUREG-1150, December 1990.

2 D. J. Hanson, et al., *Depressurization as an Accident Management Strategy to Minimize the Consequences of Direct Containment Heating*, NUREG/CR-5447, EGG-2574, October 1990.

3 D. A. Brownson, *Extension of Surry Late Depressurization Strategy Results to Commercially Operating Pressurized Water Reactors*, EGG-EAST-9717, October 1991.

4 D. A. Brownson et al., *Intentional Depressurization Accident Management Strategy for Pressurized Water Reactors*, NUREG/CR-5937, EGG-2688, April 1993.

5 C. M. Allison et al., *SCDAP/RELAP5/MOD3 Code Manual*, NUREG/CR-5273, EGG-2555 (DRAFT), Revision 2, Volumes 1-4, September 1991.

NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes andy warranty, expressed or implied, or assumes any legal liability of responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights. The views expressed in this report are not necessarily those of the U.S. Nuclear Regulatory Commission.

NRC Confirmatory Safety System Testing in Support of AP600 Design Review

Gene S. Rhee
David E. Bessette
Louis M. Shotkin

ABSTRACT

Westinghouse Electric Corporation has submitted the Advanced Passive 600 MWe (AP600) nuclear power plant design to the NRC for design certification. The Office of Nuclear Regulatory Research is proceeding to conduct confirmatory testing to help the NRC staff evaluate the AP600 safety system design. For confirmatory testing, it was determined that the most cost-effective route was to modify an existing full-height, full-pressure test facility rather than build a new one. Thus, all the existing integral effects test facilities, both in the United States and abroad, were screened to select the best candidate. As a result, the ROSA-V (Rig of Safety Assessment-V) test facility located in the Japan Atomic Energy Research Institute (JAERI) was chosen. However, because of some differences in design between the existing ROSA-V facility and the AP600, the ROSA-V is being modified to conform to the AP600 safety system design. The modification work will be completed by the end of this year. A series of facility characterization tests will then be performed in January 1994 for the modified part of the facility before the main test series is initiated in February 1994. A total of 12 tests will be performed in 1994 under Phase I of this cooperative program with JAERI. Phase II testing is being considered to be conducted in 1995 mainly for beyond-design-basis accident evaluation.

I. INTRODUCTION

Westinghouse Electric Corporation has submitted the Advanced Passive 600 MWe (AP600) nuclear power plant design to the NRC for design certification. The Office of Nuclear Regulatory Research is proceeding to conduct confirmatory testing of AP600 safety systems to help the NRC staff evaluate the AP600 safety system design.

In contrast to the current generation of reactors, this new design features passive safety systems for mitigating accidents and operational transients. Since these passive safety systems rely on gravity-driven flow, the driving forces for the safety functions are small compared to those available under conventional pumped systems. Thus, the performance of these new safety systems may be adversely affected by small variations in thermal-hydraulic conditions. Also, the computer analyses of the passive safety systems pose a challenge for current thermal-hydraulic system analysis codes in that the current codes were not sufficiently assessed for conditions of low pressure and low driving heads and for the system interactions that may occur among the multiple flow paths used in the AP600 design. Therefore, integral effects test data are being obtained for evaluation of AP600 safety system performance and for independence assessment and validation of computer analysis codes. Westinghouse is sponsoring integral test programs in the SPES-2 (Simulatore Per Esperienze di Sicurezza-2) and OSU (Oregon

State University) test facilities. SPES-2 is a full-pressure, full-height test facility in Italy but much smaller in scale (1/395 by volume) than ROSA which represents a 1/48 volume-scale for current 3423 MW_t reactors and a 1/30 volume-scale for AP600. OSU facility is a low pressure, reduced height facility with a considerably smaller volumetric scale (1/200 by volume) as compared to ROSA. NRC confirmatory safety system testing is not required for design certification but would provide additional technical bases for the NRC licensing decisions.

For confirmatory testing, it was determined that the most cost-effective route was to modify an existing full-height, full-pressure test facility rather than build a new one. Thus, all the existing integral effects test facilities, both in the United States and abroad, were screened to select the best candidate. The criteria for the initial screening included the size, facility configuration similarity, availability schedule, willingness to share the cost, and the ability to enter into a confidential agreement with Westinghouse for handling proprietary information. This screening revealed that the best candidate was the Rig of Safety Assessment (ROSA) Large Scale Test Facility in Japan Atomic Energy Research Institute (JAERI). Even though the existing ROSA-V facility scored best, it lacked certain safety systems which are unique to the AP600. Therefore, it was necessary to modify the facility to simulate the AP600 safety systems.

II. COOPERATIVE ARRANGEMENT

To finance the facility modification as well as testing and analysis, a cooperative arrangement was worked out between the NRC and JAERI through a bilateral agreement which was signed on October 5, 1992. Under this agreement, the NRC is to:

- Provide funding for facility modification to simulate AP600 safety systems. Sumitomo Heavy Industries (SHI) which has been operating and maintaining the facility for JAERI, was selected for modification of the facility.
- Provide a resident engineer to the test site to facilitate communications and to support data analyses and report preparations.
- Prepare test specifications.
- Perform test data analyses.

JAERI is to:

- Perform test facility characterization tests.
- Maintain the facility.
- Qualify test data.
- Perform 12 tests under phase I program and additional 6-12 tests under phase II program.

- Prepare quick-look and data reports.
- Provide test data tapes.
- Perform test data analyses.

III. TEST FACILITY CONFIGURATION

A. Existing ROSA Facility

The existing facility, called ROSA-V LSTF, is a 1/48 volumetrically scaled, full-height, full-pressure conventional Westinghouse four-loop 3423 MW_t pressurized water reactor (PWR) simulator. The reference PWR used for the ROSA-V facility design was very similar to the Trojan Plant. When compared to AP600, ROSA-V represents 1/30-volume scaling. The ROSA facility includes two primary loops, each containing one cold leg, one hot leg, an active inverted-U tube steam generator, and an active reactor coolant pump. Each ROSA-V loop represents two of the reactor loops lumped together. The loop horizontal legs are sized to conserve the scaled volume as well as the ratio of length to the square root of diameter, $L/D^{0.5}$, in order to better simulate the two-phase flow regime transitions. The inverted-U tube steam generators are full-length and contain 141 tubes. Tube thickness, outside diameter, and length are identical to those of the reference PWR. A pressurizer is connected to one of the hot legs. The ROSA-V vessel includes an annular downcomer and contains 1064 full-length electrically heated rods capable of operating at 10 MW, or 14 percent of scaled full power for the reference PWR. The heater rod dimensions and pitch are the same as for the 17x17 fuel assembly used in the reference PWR core. Emergency core cooling (ECC) components, typical of those in the reference PWR, are included in ROSA-V. The current ROSA-V facility is very similar to the ROSA-IV facility described in a October 1990 JAERI report, JAERI-M-90-176, "ROSA-IV Large Scale Test Facility System Description" (Reference 2).

B. Facility Modification

A comparison between the existing ROSA facility and the AP600 design showed that ROSA did not contain the key components important for safety response of the AP600. It was not obvious how much hardware modification to the ROSA facility would be needed to simulate the AP600. The fidelity of simulation must be balanced against the associated cost. The fidelity should be high enough to result in a facility capable of producing data for code assessment covering the major AP600 phenomena in the correct sequence. At the same time, the cost and the schedule have to be affordable. To make an optimum choice, the Idaho National Engineering Laboratory (INEL) was asked to consider four levels of modifications in progressively more extensive stages, the first level of modifications being the absolute minimum, and the fourth level the most inclusive among the four levels (Reference 1). To judge the fidelity of simulation of each level of modification, the following steps were followed.

C. Criteria Used for Evaluating Each Level of Modification

In evaluating each level of modification, the RELAP5/MOD2.5 code was used as a primary tool for comparing the predicted behavior of ROSA with that of AP600 for selected accident scenarios. This approach is based on the assumption that RELAP/MOD2.5, although not assessed against AP600 systems test data, will show major trends in overall behavior in such global parameters as depressurization rate, mass inventory, and energy distribution. The validity of this assumption is partially supported by the fact that the RELAP5 code reasonably matched experimental data from many different facilities, of different sizes, which were designed to simulate current PWRs. Since the thermal-hydraulic processes involved in current reactors and passive reactors are fundamentally the same, it is likely that the RELAP5 code will also show the major trends in AP600 and ROSA, even though the predictions may not be as accurate until further improvements are made in such areas as mathematical modeling of condensation in the presence of noncondensible gases, boron transport, and the computation of level tracking and thermal stratification in a tank.

D. Accident Scenarios Studied

In determining the ability of the ROSA facility to simulate the AP600 reactor, the following accident scenarios were analyzed with RELAP5 in both the AP600 and ROSA.

- 1 and 3-in. diameter breaks in a cold leg
- A 3-in. diameter break in a pressure balance line between the core makeup tank (CMT) and a cold leg
- One and three tube ruptures in a steam generator
- A main steam-line break

These scenarios were selected because they challenge the passive safety features of the AP600. The processes and governing mechanisms participating in these accidents span a reasonably complete range of important phenomena.

E. Different Levels of Modifications

The four levels of facility modifications that were considered are defined below.

1. First-level modifications were determined merely by inspection of the two designs, with only essential modifications considered, including the addition of the passive safety features not present in ROSA: the core makeup tank (CMT) and appropriate pressure balance lines, a passive residual heat removal (PRHR) system with simulated secondary cooling, automatic depressurization system with stages 1 through 3 on top of the pressurizer, stage 4 on the hot leg, and minimization of the reactor coolant pump loop seal height.

2. Second-level modifications were derived from the analysis of the first-level modifications and by adding to the first level properly scaled AP600 pressurizer, surge line, and surge line connection.

3. Third-level modifications included all the above plus the splitting of one cold leg into two to incorporate two CMTs. A CMT is connected to each split part of the cold leg, as in the AP600.

4. The fourth-level modifications resulted from the initial analyses, more in-depth inspection of the plant design differences, and discussions with representatives of the JAERI which owns the ROSA facility. These included the first and second levels coupled with appropriate upper head flow paths and adding an incontainment refueling water storage tank and an additional CMT. Since there is only one cold leg in each loop, CMT cold leg pressure balance lines are connected to the same cold leg for most transients when asymmetry between the two CMTs is not expected, but connected to a different cold leg for a non-symmetric pressure-balance-line-break scenario.

The comparisons among RELAP5 calculations for four different levels of modifications showed that the first-level modifications were capable of reasonably representing AP600 behavior during the early portion of most transients when asymmetric behavior between the two CMTs was not expected. However, the behavior in slow transients, or the latter part of fast transients, was distorted partly because of the larger friction and metal mass to volume ratio used in the calculations and partly because of the other differences in hardware. Most of the hardware differences were eliminated as the level of modification moved from Level 1 to Level 4.

Since the first-level modifications have only one CMT, it can not simulate a situation in which two CMTs act differently, e.g., a break in the pressure balance line to one of the CMTs. On the other hand, splitting a ROSA cold leg into two to be able to attach a CMT to each part of the split cold leg (Level 3 modification) did not produce good results because, unlike AP600, the split cold legs had to be merged before they enter the vessel since another large hole could not be drilled into the vessel wall. Therefore, in the Level 4 modification, splitting a cold leg was not incorporated. Instead, both of two CMTs were connected to the same cold leg when asymmetry between the two CMTs was not expected, and one of the two CMTs is connected to a different loop when asymmetry is expected. This arrangement produced reasonable approximation of the behavior of two CMTs in AP600.

In addition to the above-mentioned modifications, a steam distributor was installed at the steam flow entrance at the CMT top to be consistent with the recently changed AP600 CMT design. Westinghouse Electric Corporation indicated that it had decided to add a steam distributor at the CMT top based on recently obtained CMT separate-effects test results.

F. Final Level of Modifications

In summary, the following modifications are being implemented in the ROSA-V facility:

- Stand pipes (3.8M high) in accumulators to reduce capacity to scaled values.
- Increased flow paths between upper plenum and head.
- Properly scaled pressurizer.
- Two CMTs (Core Makeup Tanks).
- ADS (automatic depressurization system) 1-4 stages.
- IRWST (In-containment Refueling Water Storage Tank).
- PRHR (Passive Residual Heat Removal) system (45 tubes).
- Connecting lines (pressurizer surge line, CMT pressure balance lines, CMT and IRWST discharge lines, direct vessel injection (DVI) lines, etc.).
- CMT steam distributor in each CMT.
- Two catch tanks to collect fluid from ADS stage 4.

IV. INSTRUMENTATION

The instruments used in the current ROSA-V facility are shown in Table 1. They include a large number of thermocouples, differential pressure cells, and conductivity probes along with a fair number of two phase flow instruments, such as gamma densitometers and drag disks. For the modified part of the facility, the NRC added a sufficient number of single-phase flow instruments as shown in Table 2. For two phase flow instruments, the existing instruments were used. The instruments were selected based on the following criteria.

- Provide adequate data on fluid and energy distributions for code assessment
  - Provide mass and energy balance information
    - Two phase flow measurements in
      CMT cold leg pressure balance lines
      Pressurizer surgeline
      ADS lines
      Break flow lines
    - Single phase flow measurements in all other lines
    - Level measurements in all tanks

Table 1 Summary of measurement Types and Locations

Instrument/Measurement	Symbol	Pressure Vessel	Primary System	Steam Generators	Pressurizer	Secondary System	Surpression Tank and Break Units	Other	Total
Fluid Temperature	TE	191	60	246	17	15	17	97	643
Wall Temperature	TW	485	50	92	16		4	9	656
Differential Temperature	DT	112	24	70	2				208
Conductance Probe	CP	143	20	20	4		1		188
Conductance Probe with TC	CPT		10	224					234
Flow Rate	F	2	4	12	3	8	4	25	58
Pitot-tube Velocimeter	PIT		3						3
Liquid Level	L	1		8	1	1	4	4	19
Pressure	P	3	10	2	8	5	10	4	42
Differential Pressure	DP	24	62	22	9		6	2	125
Gamma Densitometer(1 Beam)	GD_1		3	1	3				7
Gamma Densitometer(3 Beam)	GD_3		6	1			3		10
Drag Disk Flow Meter	DD		26		6		4		36
Video Probe	VP	2	6						8
Rotation Speed	RE		2						2
Pump oscillation	VE		2						2
Pump Torque	TQ		2						2
Power	WE	11	8	16	4			4	43
Total		974	298	714	73	29	53	145	2286

Table 2

Summary of Instrumentation in New ROSA/AP600 Components									
	Level	DPs	P	Fluid TCs	Metal TCs	DTs	Spool Pieces[1]	Flow	g-D
CMTs	8	2	2	48		26			
PZR PBLs		4		6	2			2	
CL PBLs		6	2	8	4		2	2	2
CMT Headers		2		2					
CMT Dschrgs		2		4				2	
ACC Dschrgs		2	2	8	2			2	
IRWST Dschrg		2		2				2	
DVI Lines		2	4	2			2[2]	2	
PRHR	1	3		33	22			1	
IRWST		2		19					
ADS-1,2,3		3	2	2	1		1		1
ADS-4		4		4					2
Pressurizer	1	8	2	6	6				
Surge Line		2							1
Loop Seals		4		2	2			2	

[1]The instruments included in the spool pieces have been included in the table.
[2] These spool pieces will be used only during a DVI break scenario.

-- 3 catch tanks to collect fluid from each ADS stage 4 and a break nozzle

- Track mass inventory distribution

- Measurement principles already proven and practical applications already demonstrated.
- Commercially available.
- Instrument delivery schedule compatible with facility modification schedule (delivery within 5 months generally)
- Acceptable to JAERI in maintaining the instruments
- Cost

For the thermal stratification measurement in each CMT, 20 thermocouples were distributed axially and 4 radially in the tank. In addition, 13 differential thermocouples were installed across the CMT wall. A sufficient number of thermocouples were also installed for heat transfer measurements in PRHR.

A critical instrument list will be prepared for each test as part of test specifications. All of the instruments in this list will be assured to be working before the test is carried out.

V. TEST MATRIX

Twelve tests are planned under Phase I of this program. They consist of:

1	Inadvertent ADS 1 Opening
4	Cold Leg (CL) SBLOCA • 1/2 Inch Break • 1 Inch Break • 2 Inch Break, Non-Safety System on • 1 Inch Break, ADS 1-3 Stage Failure
1	Direct Vessel Injection (DVI) Line LOCA (200%)
3	Cold Leg Pressure Balance Line (PBL) LOCA • 2 Inch Break • 2 Inch Break, 1 RC Pump on in CMT Side Loop • 100% Break
2	Steam Generator Tube Rupture (SGTR), Single and Multiple Tube Ruptures
1	Main Steam Line (MSL) LOCA
12	

As shown above, Phase I testing is mainly for design-basis accident evaluation. One notable exception is 1 inch cold-leg break with ADS stage 1 through 3 failure. Additional 12 tests are being considered for Phase II testing which will be devoted mainly to beyond-design-basis accidents.

VI. CURRENT STATUS

The facility components to be modified have been fabricated and installed and are being checked out. A facility shakedown and acceptance testing is planned in the latter part of December 1993. A series of facility characterization tests including measurement of heat loss to the ambient air will be performed in January-February 1994. The Phase I testing will then be initiated some time in February 1994 and is scheduled to be completed by the beginning of 1995. The Phase II testing is being considered to be conducted in 1995 before the final design approval (FDA) of AP600 which is currently scheduled for February 1996 (Reference 3).

VII. REFERENCES

1. Ortiz, M. G. et al., "Investigation of the Applicability and Limitations of the ROSA Large-Scale Test Facility for AP600 Safety Assessment," NUREG/CR-5853, December 1992.

2. ROSA-IV Group, "ROSA-IV Large Scale Test Facility (LSTF) System Description for Second Simulated Fuel Assembly," JAERI-M-90-176, October 1990.

3. SECY-93-097, "Integrated Review Schedules for the Evolutionary and Advanced Light Water Reactor Projects," April 14, 1993.

NRC CONFIRMATORY TESTING PROGRAM FOR SBWR

James T. Han, David E. Bessette, Louis M. Shotkin
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission

Abstract

The objective of the NRC Confirmatory Testing Program for SBWR is to provide integral data for code assessment, which reasonably reproduce the important phenomena and processes expected in the SBWR under various loss-of-coolant accident (LOCA) and transient conditions. To achieve this objective, the Program consists of four coupled elements: (1) to design and construct an integral, carefully-scaled SBWR test facility at Purdue University, (2) to provide pre-construction RELAP5/CONTAIN predictions of the facility design, (3) to provide confirmatory data for code assessment, and (4) to assess the RELAP5/CONTAIN code with data. A description of the "preliminary design" of the Purdue test facility and test matrix is presented. The facility is scheduled to be built by December 1994. Approximately 50 tests will be performed from April 1995 through April 1996 and documented by interim data reports. A final and complete data report is scheduled to be published by July 31, 1996.

1. Introduction

General Electric Company (GE) has submitted for design certification an advanced boiling water reactor (BWR) called the Simplified BWR (SBWR)[1]. The SBWR design is largely based on the proven BWR technology of many years of operating experience. However, there are some differences. First, unlike most of the operating BWRs, SBWR is a natural circulation reactor with core flow driven by the hydrostatic head difference between the downcomer and the core. There is a long chimney region above the core to enhance the natural circulation flow in the SBWR vessel; there are no jet pumps in the vessel downcomer region nor the recirculation pumps outside the vessel. Second and more importantly, the SBWR uses passive (not pump-driven), safety systems to provide emergency core and containment cooling. These passive systems rely on gravity-driven stored energy (e.g., a water tank at higher elevation than the core), natural convection, and condensation to provide driving forces to maintain their operation without the use of any pumps or AC power. In addition to the passive systems, the SBWR also has pump-driven, non-safety systems that are normally operating and can be used as the first line of defense to prevent and mitigate accidents.

There are three passive safety systems in the SBWR that provide emergency core and containment cooling: (1) the low-pressure Gravity-Driven Cooling System (GDCS) for providing emergency cooling and makeup water to the reactor vessel, (2) the low-pressure Passive Containment Cooling System (PCCS) for maintaining containment cooling and integrity, and (3) the high-pressure Isolation Condenser System (ICS) that is capable of maintaining core cooling for non-LOCA transients with scram. Both the GDCS and PCCS are unique to the SBWR and do not exist in any of the operating BWRs, while the ICS is similar to those on some of the earlier BWRs but with a different condenser design. Since the GDCS is a low-pressure system, it can be initiated "only" after the vessel is almost depressurized by the automatic depressurization system (ADS), which is actuated when the vessel water level drops to 3.6 m (i.e., 11.8 ft) above the top of active fuel during a LOCA or transient (normal vessel water level at full power operation is at 18.26 m above the core). Note that the GDCS and ADS comprise the SBWR emergency core cooling systems (ECCS)[1].

Because of the unique features in these passive safety systems of the SBWR, GE has established testing programs[2] to demonstrate their performance and to provide a data base for assessing analytical tools, in compliance with the requirements of 10 CFR 52.47 for design certification[3]. The GE testing programs include three integral test facilities - namely, GIST[2,4], GIRAFFE[2], and PANDA[5], which are used to assess the performance of the GDCS (GIST), PCCS (GIRAFFE and PANDA), and ICS at low pressure (PANDA). GE also has a separate-effect PANTHERS facility[6] investigating the performance of full-pressure, prototypical condensers of the ICS and PCCS. In addition, tests were conducted to assess the performance of prototypical depressurization valves (DPVs)[2], which are part of the ADS and are also installed on the GDCS injection lines and the suppression pool equalization lines connected to the vessel[1].

To provide data for code assessment and to confirm GE test results for the SBWR including the GDCS and PCCS performance, the NRC has established a Confirmatory Testing Program for SBWR.

2. Objective

The objective of the NRC Confirmatory Testing Program for SBWR is to provide integral data for code assessment, which reproduce the important phenomena and processes as expected in the SBWR under various loss-of-coolant accident (LOCA) and transient conditions. These data will significantly broaden the current SBWR data base (to be discussed later in this paper). The data will be used to confirm GE test results for the SBWR.

3. Program Elements

The NRC Confirmatory Testing Program consists of four coupled elements being performed jointly at Purdue University and Brookhaven National Laboratory (BNL):

(1) To design and construct at Purdue University[7] a carefully-scaled integral SBWR test facility, which has all of the key components and

systems required for investigating integral performance of GDCS and PCCS (Purdue University).

(2) To provide two pre-construction predictions using RELAP5/CONTAIN[9-10] for a main steam line break and a bottom drain line break. The results will be compared with similar calculations for the SBWR. Propose design improvements to the Purdue test facility, if comparison is not acceptable (BNL).

(3) To provide confirmatory data for code assessment (Purdue University).

(4) To assess the RELAP5/CONTAIN code with data from the Purdue test facility (BNL).

The first element above includes a detailed scaling analysis being performed by Purdue and a Phenomena Identification and Ranking Table (PIRT) being performed by BNL and Purdue. The purpose of the scaling analysis, PIRT, and comparison of RELAP5/CONTAIN calculations (stated in the second element above) is to ensure that the test facility as designed can reasonably reproduce the important phenomena and processes (e.g., core coolant makeup by GDCS, containment cooling by PCCS, etc.) expected to occur in the SBWR. As a result, the data from the Purdue test facility should be valid for code assessment.

Although only two RELAP5/CONTAIN calculations of the Purdue facility are currently planned before facility construction, additional calculations of the facility and comparisons with the similar SBWR calculations will be made afterward.

4. Preliminary Design of the Purdue Test Facility for SBWR

The Purdue test facility for SBWR will have all of the key components and systems required for investigating the integral performance of GDCS and PCCS. The facility consists of a vessel with electrically-heated fuel rods, an upper drywell and a lower drywell, suppression pool (namely, wetwell), safety systems including GDCS, PCCS, and ICS, non-safety systems (including drywell spray, wetwell spray, and pump-driven water injection to the vessel), and connecting pipes and valves. Sufficient instrumentation will be provided to collect data for code assessment. Non-safety systems are included in the facility so that possible interactions with the safety systems such as GDCS and PCCS can be investigated. Figure 1 shows a simplified drawing of the preliminary design of the Purdue test facility including a vessel, upper and lower drywells, suppression pool, three GDCS pools (only one is shown), three PCCS condensers and three ICS condensers (only one each is shown). Not shown in Fig. 1 are the non-safety systems mentioned earlier and a feedwater tank. In comparison, GIST did not have PCCS and ICS, and GIRAFFE was not equipped with concurrent operation of ICS and PCCS. Non-safety systems such as drywell spray and wetwell spray are not present in GIST, GIRAFFE, and PANDA.

Since the SBWR does not have high-pressure safety systems to provide emergency coolant injection to the vessel and both GDCS and PCCS are designed to operate

at low pressure, a "low-pressure" test facility is deemed technically adequate as a cost-effective design for providing integral data for code assessment. The Purdue test facility is a low-pressure facility with its vessel designed for 150 psia and containment components designed for about 90 psia. It is worth noting that all of the GE integral facilities including GIST, GIRAFFE, and PANDA are also low-pressure facilities.

Based on a detailed scaling analysis performed by Purdue, the height scale of the Purdue facility is selected to be 1/4 of the SBWR height, and the volume scale is 1/400 of the SBWR volume. This leads to an area scale of 1/100 of the SBWR flow area. In comparison, GIST, GIRAFFE, and PANDA are full-height facilities. GIST has a volume scale of 1/508 of an earlier SBWR design; GIRAFFE has a volume scale of 1/400 of an earlier SBWR design; PANDA has a volume scale of 1/25 of the current SBWR design. The volume scale of Purdue facility is the same as GIRAFFE, but smaller than PANDA.

However, the Purdue facility has an aspect ratio (AR) of 2.5 (defined here as = height scale/diameter scale = 0.25/0.1), which is closer to the SBWR (AR = 1) than GIST (AR = 22.5), GIRAFFE (AR = 20), and even PANDA (AR = 5). The Purdue facility has a favorable aspect ratio for investigating multi-dimensional phenomena in the vessel and containment.

5. Preliminary Test Matrix

The preliminary test matrix consists of a total of approximately 50 tests divided in Phases 1 and 2, which cover a broad spectrum of LOCAs and transients. For each LOCA or transient test, there can be a single failure of a component (e.g., a GDCS injection line that is connected to the vessel, a PCCS unit, etc.), or multiple component failure, or no component failure (for base cases only).

Phase 1

Phase 1 of the preliminary test matrix is listed in Table 1. It consists of 17 tests - 5 base case tests (Tests 1, 4, 7, 10, and 12), 8 GE counterpart tests (Tests 2, 5, 8, 11, and 14 - 17), and 4 complementary tests (Tests 3, 6, 9, and 13). Four types of LOCAs and a transient will be investigated: bottom drain line break (BDLB), main steam line break (MSLB), GDCS line break (GDLB), feedwater line break (FWLB), and loss of feedwater (LOFW).

The five base case tests are the tests in which all of the listed components that are supposed to be operational are operational. The components listed in Table 1 include PCCS (a total of 3 in SBWR), ICS (a total of 3 in SBWR), DPV (a total of 6), VB (vacuum breaker between the upper drywell and gas space of the suppression pool, a total of 3), and EQUAL (equalization line between the suppression pool and the vessel, a total of 3), DWS (drywell spray, 0 means that it is not operational), and WWS (wetwell spray, 0 means not operational).

The eight GE counterpart tests have similar test conditions, to the extent feasible, as the integral tests in GIST, GIRAFFE, and PANDA. The four complementary tests complement the base case tests and GE counterpart tests.

For instance, Test 3 has the same break size and location as Test 1 (a base case test for MSLB) and Test 2 (a counterpart test to GIST Test B01) but with different operational components. Test 3 has less operational components than Test 1 but more than Test 2. Note that the number of operational PCCS or ICS in Test 2 is zero due to the lack of PCCS or ICS in GIST. To assess the impact of PCCS and ICS on the GDCS performance, Test 3 has three PCCS units and three ICS units operational in addition to what are available in Test 2.

It should be pointed out that Tests 12 and 13 for FWLB have no counterpart tests in GIST, GIRAFFE, and PANDA. The numbers of operational components for Tests 14 - 17 are left in blank for current lack of information. In addition to those 17 tests listed in Table 1, a few repeatability tests may also be needed as part of the Phase 1 tests.

Phase 2

Table 2 lists Phase 2 of the preliminary test matrix that includes sensitivity study tests and beyond DBA (design-basis accidents) tests. Table 2 should consist of Tests 18 - 50, but only Tests 18 - 24 are listed. Tests 25 - 50 are yet to be selected to accommodate the future NRC needs. Tests 18 - 22 are for BDLB concurrent with a single component failure. Test 18 has a single DPV failure (i.e., not open). Test 19 has a single failure of a GDCS injection line (i.e., a valve on the line not open on demand). Test 20 has a single failure of an equalization line (i.e., a valve on the line not open on demand). Test 21 has a vacuum breaker failed in open position. Test 22 has a vacuum breaker failed in closed position. The purpose of Tests 18 - 22 is to assess the impact of a single component failure on GDCS and PCCS performance. Test 23 has multiple component failure - all three vacuum breakers failed in open position. Test 24 is a station blackout test (namely, loss of all AC power) concurrent with a PCCS unit not available for operation.

It should be pointed out that most of the tests in Phase 1 and Phase 2 will begin when the vessel is depressurized to about 150 psia and continue to cover the short-term cooling involving initial injection of GDCS water to the vessel and the long-term cooling. The tests will last long to capture the important phenomena and processes expected to occur during the long-term cooling, which include continuous replenishment of GDCS pools by PCCS condensate, PCCS purging of drywell noncondensibles to the suppression pool, possible suppression pool water injection to the vessel via equalization lines, etc. In comparison, GIST tests only covered the short-term cooling and ended at less than 30 minutes after an accident or transient initiation; as a result, the long-term cooling was not investigated in GIST. GIRAFFE and PANDA tests begin at about 1 hour after LOCA initiation, and consequently the short-term cooling is not covered.

6. Schedule

The Purdue test facility for SBWR is scheduled to be built by the end of 1994. It will become fully operational and begin to produce data around April 1995. A total of approximately 50 tests will be performed from April 1995 through April 1996 with interim data reports published. A final and complete data

report will be published by July 31, 1996. Meanwhile, assessment of the RELAP5/CONTAIN code will be performed against the data.

7. Conclusions

The NRC Confirmatory Testing Program for SBWR will provide integral data for code assessment and for confirming GE test results. A total of approximately 50 tests, which cover a broad spectrum of LOCAs and transients, will be performed at the Purdue test facility from April 1995 through April 1996. The data from these tests are expected to reasonably reproduce important phenomena and processes expected in the SBWR and will significantly broaden the current SBWR data base for code assessment.

8. Acknowledgement

The authors wish to thank their NRC colleagues (including Alan Levin, Robert Jones, Robert Elliott, Joseph Staudenmeier, and Allen Notafrancesco) for helping develop the test matrix.

9. References

1. GE Nuclear Energy, "SBWR Standard Safety Analysis Report," 25A5113 Rev. A, August 1992.

2. A. S. Rao, "SBWR Design and Testing Program," presented to the ACRS Thermal Hydraulic Phenomena Subcommittee on April 23, 1993.

3. U. S. Government, "Code of Federal Regulations," 10 Parts 51 to 99, Revised as of January 1, 1993, U. S. Government Printing Office, 1993.

4. P. F. Billig, "Simplified Boiling Water Reactor (SBWR) Program Gravity-Driven Cooling System (GDCS) Integrated System Test - Final Report," GEFR-00850, October 1989.

5. J. R. Fitch, "ALPHA Test Program," presented to the ACRS Thermal Hydraulic Phenomena Subcommittee on April 23, 1992.

6. P. F. Billig, "PANTHERS - IC/PCCS Heat Exchanger Test Program," presented to the ACRS Thermal Hydraulic Subcommittee on April 23, 1992.

7. U. S. Nuclear Regulatory Commission, Contract No. NRC-04-93-049, awarded on July 26, 1993 to Purdue University.

8. NUREG/CR-5535 (Draft), "RELAP5/MOD3 Code Manual," Vols 1-5.

9. NUREG/CR-5026, "User's Manual for CONTAIN 1.1: "A Computer Code for Severe Nuclear Reactor Accident Containment Analysis," November 1989.

10. NUREG/CR-5715, "Reference Manual for the CONTAIN 1.1 Code for Containment Severe Accident Analysis," July 1991.

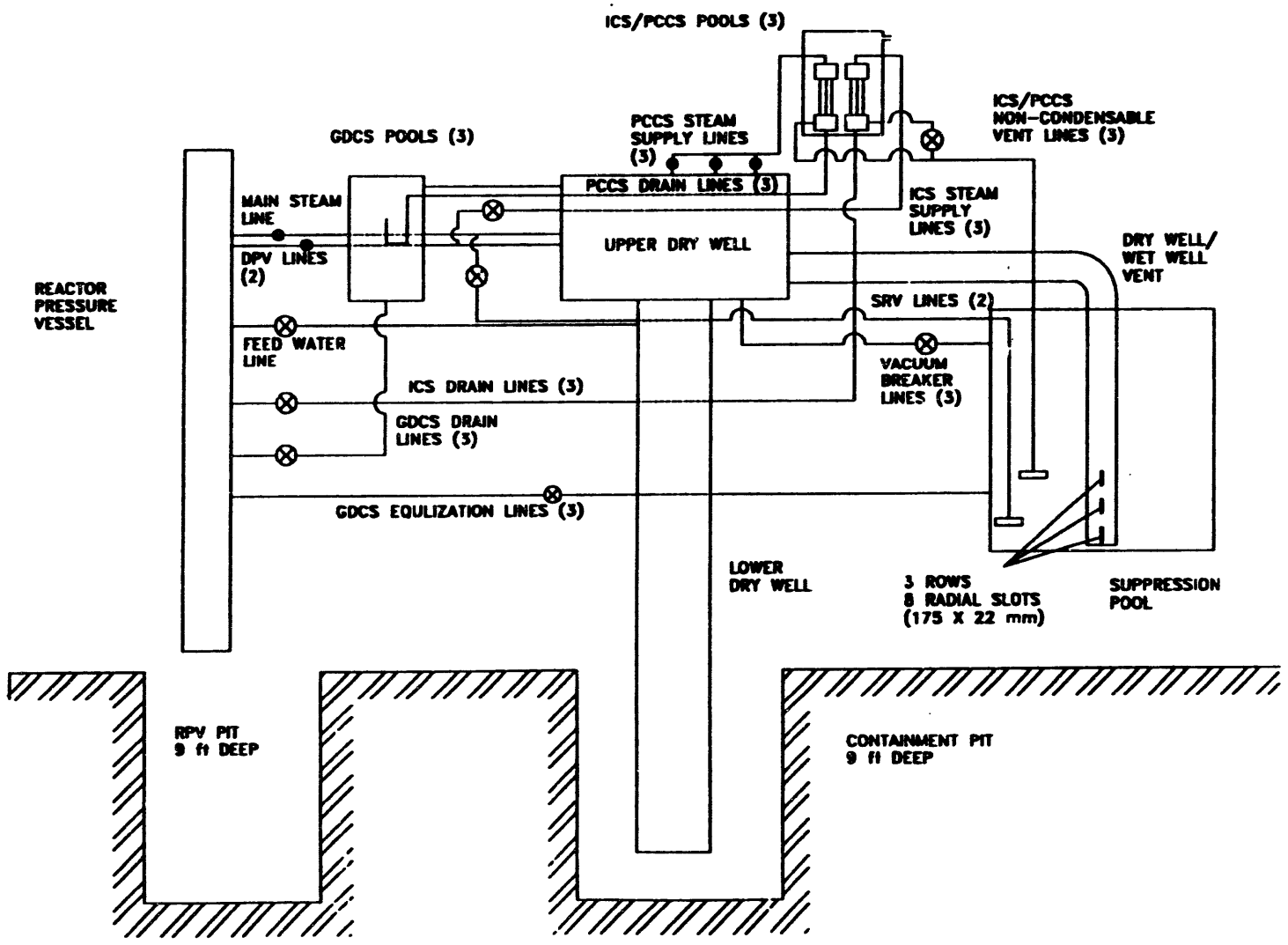


Fig. 1. A simplified drawing of the Purdue test facility for SBWR.

Table 1. Phase 1 of the test matrix - Base case and GE counterpart tests

Test	Event	Operational Components							
		PCCS	ICS	GDCS Lines	DPV	VB	EQUAL	DWS	WWS
1 (Base)	MSLB	3	3	6	6	3	3	0	0
2*	MSLB (GIST B01)	0	0	4	6	3	3	0	0
3	MSLB	3	3	4	6	3	3	0	0
4 (Base)	BDLB	3	3	6	6	3	3	0	0
5*	BDLB (GIST A07)	0	0	4	6	3	3	0	0
6	BDLB	3	3	4	6	3	3	0	0
7 (Base)	GDLB	3	3	5	3	3	0	0	0
8*	GDLB (GIST C01A)	0	0	4	6	3	3	0	0
9	GDLB	3	3	4	6	3	3	0	0
10 (Base)	LOFW	3	3	6	6	3	3	0	0
11*	LOFW (GIST D03A)	0	0	4	6	3	3	0	0
12 (Base)	FWLB	3	3	6	6	3	3	0	0
13*	FWLB	0	0	4	6	3	3	0	0
14	MSLB(GIRAFFE/PANDA)								
15	BDLB(GIRAFFE)								
16	GDLB(GIRAFFE/PANDA)								
17	ICRLB(PANDA)								

*Test will be terminated when a temperature or pressure setpoint is reached to prevent damage.
VB = vacuum breaker between drywell and wetwell, EQUAL = equalization line connecting suppression pool to the vessel (e.g., 3 means all three equalization lines will open if actuated automatically or manually), DWS = drywell spray, WWS = wetwell spray, MSLB = main steam line break, BDLB = bottom drain line break, GDLB = GDCS line break, LOFW = loss of feedwater, FWLB = feedwater line break, ICRLB = isolation condenser condensate return line break. No information is currently available regarding the number of operational components in the GIRAFFE and PANDA tests.

Table 2. Phase 2 of the test matrix - sensitivity study and beyond DBA tests

Test	Event	Operational Component							
		PCCS	ICS	GDCS Lines	DPV	VB	EQUAL	DWS	WWS
18	BDLB	3	3	6	5	3	3	0	0
19	BDLB	3	3	5	6	3	3	0	0
20	BDLB	3	3	6	6	3	2	0	0
21	BDLB (1 VB failed in open position)	3	3	6	6	2	3	0	0
22	BDLB (1 VB failed in closed position)	3	3	6	6	2	3	0	0
23	BDLB (all 3 VBs failed in open position)	3	3	6	6	0	3	0	0
24	Blackout	2	3	4	6	3	3	0	0

In addition to the above tests, the following tests will be selected:

1. Several additional tests with multiple component failure.
2. A few tests to assess the impact of non-safety systems upon GDCS and PCCS (e.g., control rod drive flow or RWCU/SDCS flow on GDCS performance, drywell spray on PCCS and GDCS performance, wetwell spray on suppression pool flow to the vessel via equalization line).
3. A few tests at different break sizes (e.g., 50% of BDLB).
4. A few tests to assess natural circulation flow characterization by measuring core flow as a function of power, downcomer water level, and vessel pressure (including the determination of any flow oscillation or instability).
5. Several sensitivity tests by varying core power or other PIRT-identified important parameters.
6. A few helium tests to investigate the presence of hydrogen on PCCS performance.
7. A few repeatability tests.

RELAP5/MOD3 CALCULATIONS FOR GIST DATA

K. R. Jones, J. C. Determan, and G. E. McCreery
Idaho National Engineering Laboratory
EG&G Idaho, Inc., Idaho Falls, ID 83415
J. T. Han
U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research

Abstract

An input deck for the thermal-hydraulic modeling code RELAP5/MOD3 was constructed to simulate the Gravity Driven Cooling System (GDCS) Integrated Systems Test (GIST) facility. The GIST facility was operated by General Electric at their site in San Jose, CA, as part of the GDCS test program. Capabilities and limitations of the database generated during the test program with respect to code assessment are discussed. Five calculations were performed with the RELAP5/MOD3 GIST model. The calculations include four loss-of-coolant accident calculations (LOCAs) and one feedwater trip calculation. The results of the calculations are presented, including a discussion of code errors found and corrected.

1 Background

General Electric Company (GE) has proposed an advanced light water reactor design, the Simplified Boiling Water Reactor (SBWR) that relies on passive, gravity-driven safety systems to provide emergency core coolant injection under postulated accident conditions.[1] A unique element of the SBWR emergency core cooling system that has not been used in previous reactor designs is the gravity-driven cooling system (GDCS). In the current design the GDCS provides three basic functions: short term coolant injection during a loss-of-coolant accident (LOCA), via three elevated GDCS pools; long term coolant makeup during a LOCA, via the suppression pool; and flooding of the lower drywell floor in the event of a severe accident, also via the three elevated GDCS pools. Because the passive containment cooling system (PCCS) drains condensed steam to the GDCS pools the PCCS also plays a role in the long term coolant makeup. The current SBWR GDCS design is illustrated in Figure 1.

This is contrasted with the March 1987 conceptual SBWR design, illustrated in Figure 2, which is the basis for the GIST facility. This design contained no GDCS pools, but instead had an elevated suppression pool to provide both short and long term coolant makeup. The long term coolant

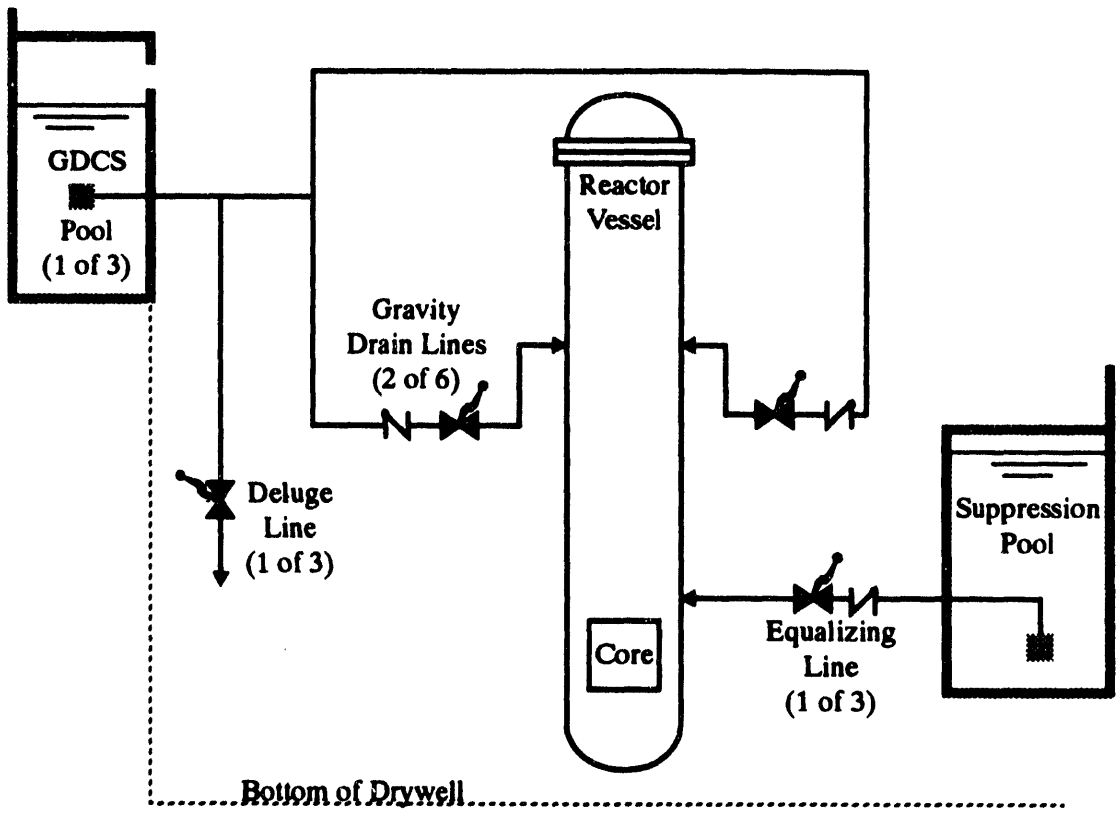


Figure 1. GDCS proposed for the current SBWR design.

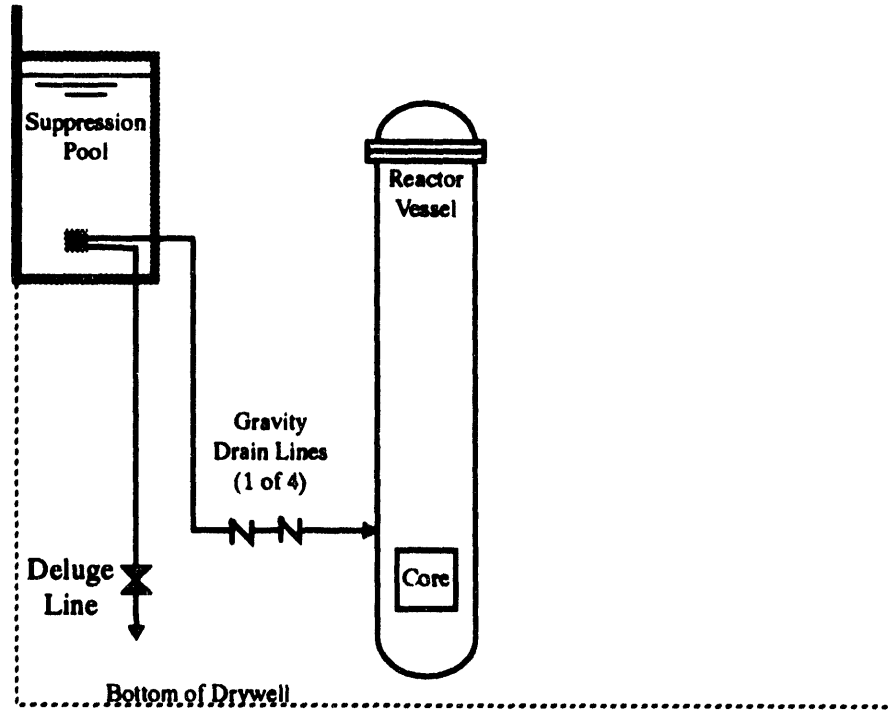


Figure 2. GDCS used in March 1987 SBWR conceptual design.

makeup was assisted by condensation of steam in the suppression pool. Although the GIST facility design was based on an early conception of the SBWR, the GDCS concept simulated in the GIST facility is functionally similar to the short-term gravity drain function of the GDCS in the current SBWR design. Further information concerning the current SBWR design is contained in Reference 1.

A GDCS test program conducted by GE and sponsored by the U. S. Department of Energy was completed in December of 1988.[2] This test program involved the construction of a full-height, low-pressure GDCS Integrated Systems Test (GIST) facility and performance of a series of GDCS tests simulating a wide range of conditions. The facility was designed to simulate only the latter stages of depressurization transients, where the vessel pressure is less than 1067 kPa (140 psig). The primary objectives of the GIST test program were to demonstrate the technical feasibility of the GDCS concept and to provide a sufficient database to qualify the thermal-hydraulic modeling code TRACG for use in SBWR accident analysis with respect to GDCS phenomena.

This paper documents calculations performed with a model of the GIST test facility to exercise the RELAP5/MOD3 computer code. RELAP5/MOD3[3] is a light water reactor thermal-hydraulic transient analysis code developed at the Idaho National Engineering Laboratory for the U. S. Nuclear Regulatory Commission to provide an advanced best-estimate predictive capability to support the regulatory process. The calculations consist of four loss-of-coolant accident calculations (LOCAs) and one feedwater trip calculation. The results include a comparison of RELAP5/MOD3 calculations with the experimental data available from each test. The data consists of the absolute pressures in the reactor pressure vessel, the upper drywell, and the wetwell, differential pressures for different regions of the vessel, and the GDCS mass flow rates. Although the original purpose of these calculations was to perform an assessment of RELAP5/MOD3, the lack of break flow measurements, measurement uncertainties and detailed facility design information precludes the ability to perform an effective code assessment with the GIST data.[4]

2 Facility and Test Description

The GIST facility was constructed at GE's Nuclear Energy site in San Jose, California. The major components of the GIST facility are shown in Figure 3 and include the reactor pressure vessel (RPV), the suppression pool or wetwell, the upper drywell and the lower drywell. Systems modeled include the automatic depressurization system (ADS) and the GDCS.

The GDCS test program was designed to study transients in the pressure range representing post-LOCA conditions during the recovery period. The GIST facility was scaled to full-height. The vessel heights and relative elevations are approximately those of the early SBWR design, while the volumes were scaled with a ratio of approximately 1:508. The liquid inventories and core power were also scaled by this ratio. Although the facility was a low pressure facility, the pressure was scaled as 1:1 over the GDCS operating range for which the facility was designed. Tests were initiated at 791 kPa (100 psig) after blowing down from approximately 1067 kPa (140 psig).

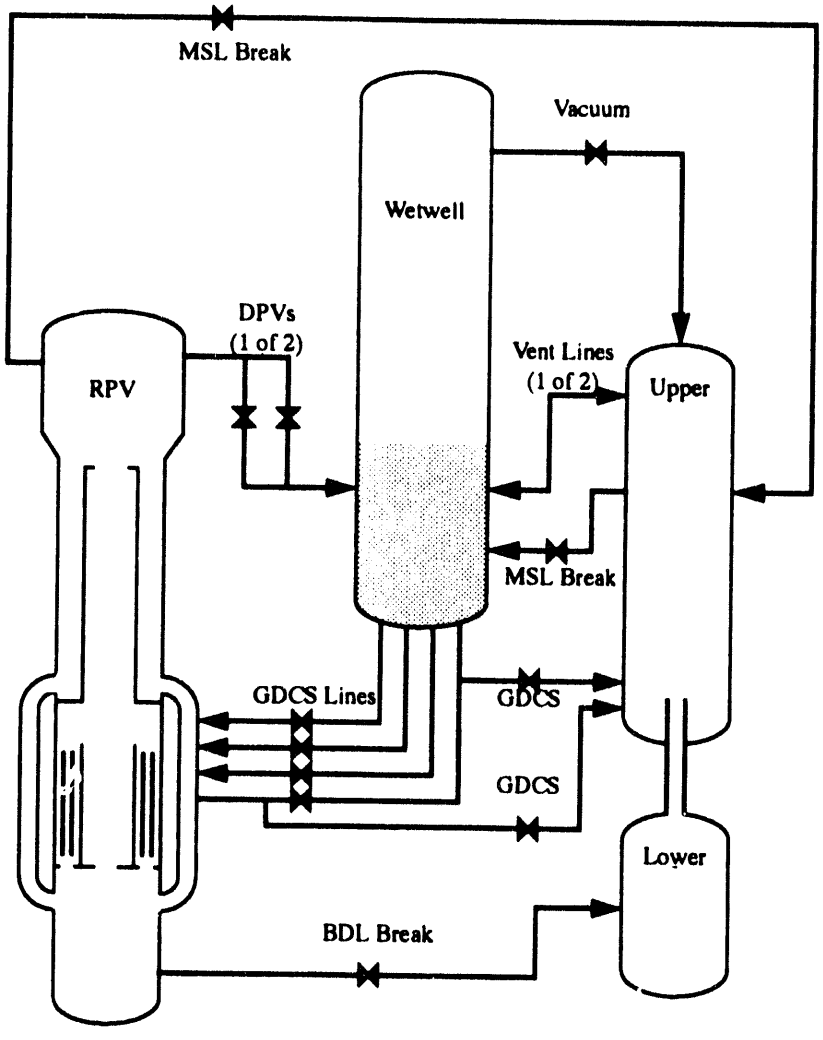


Figure 3. GIST facility major flow paths.

The GIST reactor vessel mock-up simulates the fuel rods, guide tubes, shroud, and steam separator stand pipes. The steam separators and dryers are not explicitly modeled because it was judged that only steam would transit the separator/dryer region and thus this feature was not critical to the test results.

The upper drywell, lower drywell, and wetwell (WW) or suppression pool (SP) are represented by large cylindrical tanks. Breaks to containment are simulated by pipes connected to the upper or lower drywell. The SP is the principal heat sink for vessel energy released through the depressurization system or reactor coolant system break. In GIST the SP is located above the core to provide gravity driven makeup water.

The ADS consists of two banks of depressurization valves (DPVs) in parallel. Bank A represents the valves on one steam line and two stub lines. Bank B represents those on one steam line only.

The ADS is exhausted to the suppression pool via two lines with quencher connections. It should be noted that this differs from the current SBWR design, in which the DPVs exhaust to the upper drywell (the safety relief valves, which are part of the ADS, still exhaust to the suppression pool). The GDCS consists of 4 lines injecting makeup water from an elevated suppression pool to the RPV. Each line contains two check valves in series which open when the RPV pressure has sufficiently decreased to allow passive gravity flow into the RPV. To simulate the consequence of a GDCS line failure, each line can be manually isolated.

Four major categories of design basis accidents were simulated with the GIST facility. These categories are as follows:

- Main steam line breaks (MSLBs)
- Bottom drain line breaks (BDLBs)
- GDCS drain line break LOCA (GDLB)
- Loss of feedwater or no break (NB).

A total of 24 unique experiments falling into the above categories were performed. For each class of accidents, parametric variations in test conditions were examined to ensure that GDCS response would maintain the core in a cooled state. Table 1 shows the complete test matrix.

Because GIST was designed to simulate only the latter stages of depressurization transients, initial test conditions were formulated with estimates from TRACG simulations used to calculate the transition period between nominal operating pressure of 7171 kPa (1025 psig) and the initial test pressure of 791 kPa (100 psig). The TRACG output was then used to establish the initial conditions for the GIST facility at 140 psig. The depressurization rate for the facility between 1067 kPA (140 psig) and 791 kPa (100 psig) was controlled to establish the proper depressurization rate and vessel initial conditions at 100 psig. The actual tests started when the vessel pressure reached 791 kPa (100 psig), at which time the vessel discharge was switched from the atmosphere to the containment mock-up.

At 515 kPa (60 psig) the low pressure DPVs opened, accelerating the blowdown. Once the RPV pressure dropped below the GDCS discharge head, check valves on the GDCS lines opened, allowing flow to enter the downcomer and begin refilling the RPV. The effect of the GDCS injection was to quench the core and provide sufficient cooling to prevent rod temperature excursions. The collapsed liquid level also began to increase as a result of the GDCS injection. When the collapsed liquid level rose to an elevation above the top of core the test was terminated. Simulation of long term recovery was outside of the test program scope.

The GIST fuel mock-up was composed of forty-five 2.74 m (9 ft) long, electrically-heated rods. Fuel bundle geometry was arranged in a circular pattern around a smaller pipe pathway that represented the core bypass region. The experimental axial power profile was flat except for a drop-off in power imposed at the top of the fuel to accurately simulate any departure from nucleate boiling in the region where the mixture void fraction was the highest. Decay energy was generated to match the expected values at the time the RPV pressure reached 791 kPa (100 psig).[5]

TABLE 1. GIST test matrix

Variation	BDLB	MSLB	GDLB	NB
Number of unique tests	7	6	4	7
Base case	√	√	√	√
Low SP level	√	√	-	-
Maximum GDCS (4 lines operational)	√	-	-	√
Minimum GDCS (1 line operational)	√	-	-	-
Control rod drive flow reduction	√	-	-	-
Low RPV level	√	√	-	-
Low-low RPV level	-	√	-	-
No low pressure DPVs	√	-	-	-
High pressure injection[a] -case 1	-	√	-	-
High pressure injection[a] -case 2	-	√	-	-
Maximum DPV area	-	-	√	-
Minimum DPV area	-	-	√	-
Higher low pressure DPV setpoint	-	-	√	-
Appendix K decay power	-	-	-	√
Pressurized WW	-	-	-	√
High pool temperature	-	-	-	√
No power	-	-	-	√
Lowered GDCS injection point	-	-	-	√

a. Current SBWR design does not have a safety grade high pressure injection system.

In addition to modeling core decay power, heating due to stored energy within vessel internal structures was included in the vessel mock-up. Insulation was provided to minimize environmental heat losses. Because of the increased area to volume ratios, energy release from heat structures to the vessel liquid occurred at a faster rate in GIST than would occur in the SBWR. In addition, the metal temperatures in GIST were initialized to lower temperatures than would be expected in the SBWR at that point in the blowdown phase. Initial wall temperatures for GIST were based on saturation temperature of 452 K (353°F) corresponding to 1.07 MPa (140 psig). The wall temper-

atures for SBWR would not be expected to drop significantly from the power operation value of 561 K (549°F) at 7.17 MPa (1025 psig) while the system blows down to 1.07 MPa (140 psig).[6]

3 RELAP5/MOD3 GIST Model Description

Five test cases representing the full range of GIST experiments were selected for the TRACG assessment effort performed by GE. These same five test cases were selected for the RELAP5/MOD3 calculations. The final calculations were performed with RELAP5/MOD3 version 8y, which contained error corrections resulting from code errors found during the initial calcalculations performed for this project. The available design data for the GIST facility is contained in General Electric Company's test record files. Some of the key design information required for model development such as isometric drawings of the of the system was not available. Due to the lack of sufficient facility design information the RELAP5/MOD3 models developed for code assessment were based to a large degree on TRACG models supplied by GE. Several discrepancies were found between the TRACG models supplied by GE and the facility design information that was provided. The modeling discrepancies were corrected in the RELAP5/MOD3 model where design data were available.

The RELAP5/MOD3 GIST model consists of four major regions and connecting piping, as shown in Figure 4. These regions include the reactor pressure vessel, the wetwell, the upper drywell, and the lower drywell. The connecting pipes include the GDCS lines, the steamlines, the vent line, and the break lines. The model is comprised of 197 hydrodynamic volumes, and 109 heat structures. Table 2 shows the RELAP5/MOD3 component numbering scheme used.

There are several assumptions common to all the calculations discussed in this report. For SBWR LOCA analysis it is assumed that loss of AC power is coincident with the opening of the break, resulting in the immediate loss of feedwater.[1] The NB experiments at the GIST facility are assumed to be initiated by a loss of feedwater event. Therefore, it is a basic assumption of the GIST experiments, and the RELAP5/MOD3 simulations, that feedwater is lost at the start of the transient.

No information concerning the insulation material used in the GIST facility was provided, nor were environmental heat losses measured. Therefore adiabatic boundary conditions were assumed throughout the model.

The RELAP5/MOD3 GIST model simulates blowdown to atmospheric conditions through the MSIV to establish a glide path for the transient. When the RPV pressure decreases below 791 kPa (100 psig) the MSIV closes and blowdown continues through the DPVs to the suppression pool. The DPVs in each steamline open halfway at the start of the blowdown to containment, representing the DPVs which would already be open at this point in the SBWR transient. The DPVs open fully when the RPV pressure decreases below 515 kPa (60 psig), representing the last of the DPVs to open.

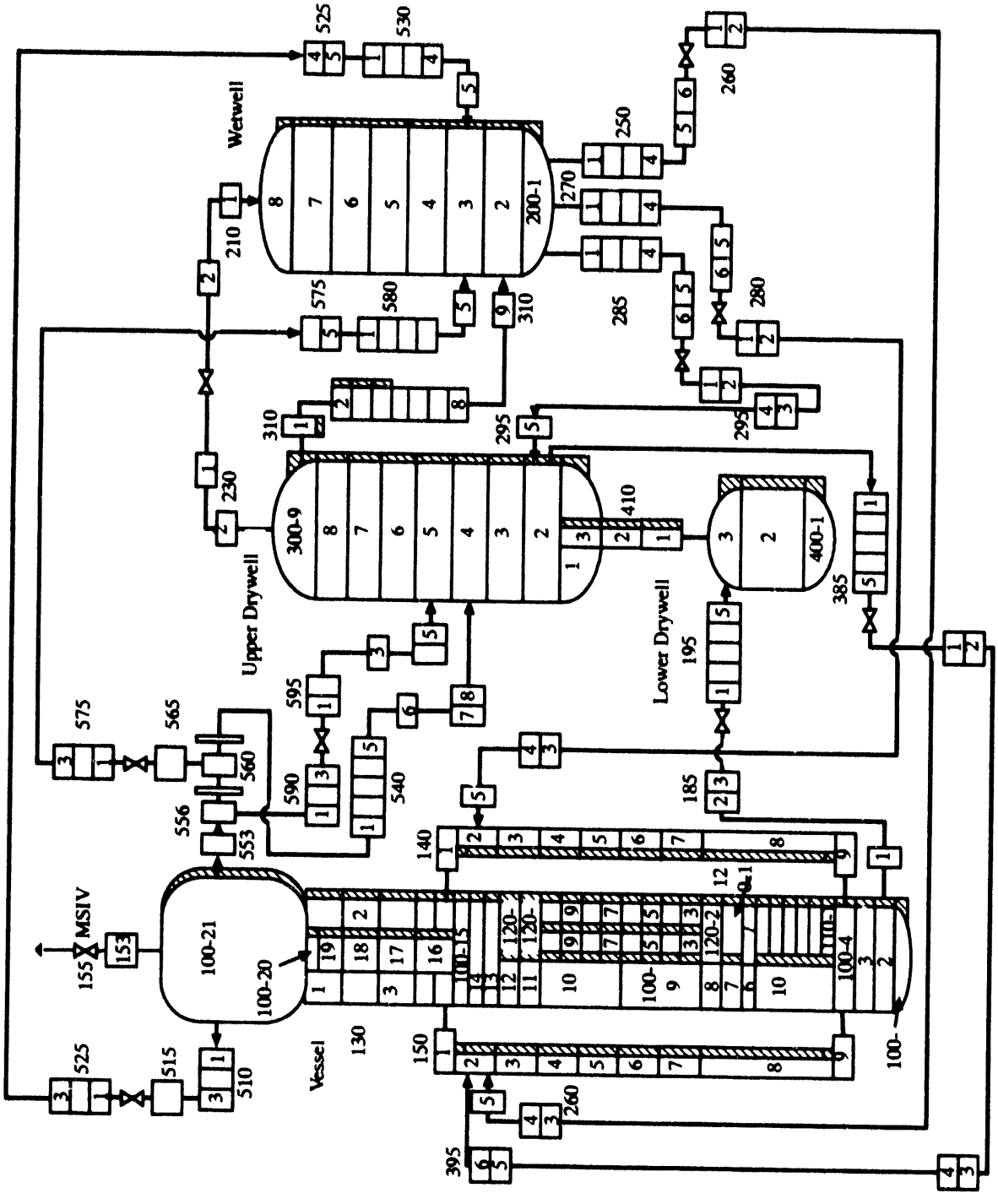


Figure 4. RELAP5/MOD3 GIST input deck nodalization diagram

In all of the GIST facility experiments simulated with RELAP5/MOD3, it was conservatively assumed that one of the four GDCS lines is unavailable. Therefore only three lines are represented in the RELAP5/MOD3 facility model; these are modeled as one double capacity line and one single capacity line. Check valves in these lines open when the vessel pressure has decreased below the drywell pressure plus the head of liquid in the suppression pool.

TABLE 2. RELAP5/MOD3 GIST facility model component numbering

Region	Component #
Vessel	100
Guide Tube	110
Core	120
Upper Annulus	130
Lower Downcomers	140, 150
MSIV	153, 155, 160
Wetwell	200
GDCS lines	250 - 280
Vacuum Breaker	210 - 230
Upper Drywell	300
Drywell Vent	310
Lower Drywell	400, 410
Intact Steamline	510 - 530
"Broken" Steamline	550 - 580
GDCS Break Line, WW to UDW	285 - 295
GDCS Break Line, RPV to UDW	385 - 395
Steamline Break Line, WW to UDW	540
Steamline Break Line, RPV to UDW	590, 595
Bottom Drainline Break Line	185 - 195

Breaklines to the drywell volumes are also modeled. The bottom drainline break line connects from the lower plenum of the RPV to the top of the lower drywell. A system of valves converts one of the steamlines to a pair of break lines, one from the RPV to the upper drywell, and one from the wetwell to the upper drywell. Likewise, one of the GDCS lines may also be replaced by

a set of break lines. Control logic exists to select the appropriate break lines for a given calculation.

4 Calculation Results

Test B01 was designed to simulate a MSLB LOCA within the containment. The MSLB LOCA represents the largest pipe break that can occur on the SBWR vessel. This transient is characterized by rapid blowdown of the RPV and high coolant inventory loss. This test was selected for thermal-hydraulic code assessment because of the challenge presented by the rapid blowdown.

The following sequence of events is expected to occur for the base case MSLB transient. High break flow causes the drywell pressure to rise rapidly, initiating a scram. At the same time the MSIVs close on high steam flow. The feedwater pumps are assumed to trip at the start of the LOCA due to loss of AC power, resulting in a gradual reduction of reactor water level and eventual initiation of the ADS when the level 1 setpoint is reached. Due to the effect of the combined break and ADS flow the RPV pressure decreases sufficiently to initiate GDCS flow.

The blowdown of the RPV is the primary driving force in the GIST experiments and calculations. In all the calculations it was observed that choking occurred in the blowdown lines and that the blowdown rate predicted by RELAP5/MOD3 was greater than the measured data. The blowdown rate was adjusted by the application of discharge coefficients to the choked junctions to effectively reduce the flow area and mass flow rate. A discharge coefficient was determined which reduced the blowdown rate in all the calculations, when applied to all of the choked locations. Figure 5 shows the RPV dome pressure traces for the GIST facility and the RELAP5/MOD3 calculations.

Table 3 displays the sequence of events as observed in the facility and the RELAP5/MOD3 calculation. Both RELAP5/MOD3 and the facility indicate that natural circulation between the core and bypass begins at about 20 s, as the potential for upward flow through the bypass and toward the MSIV decreases. Natural circulation enhances the core cooling and the blowdown rate decreases. This is seen as a "knee" in the curve at about 20 s, in both the measured and calculated data. The atmospheric blowdown ends and blowdown to containment begins when the dome pressure decreases below 791 kPa (100 psig). This occurs 14 s later in the RELAP5/MOD3 calculation than in the facility. The opening of the low pressure DPVs is 18 s later in the RELAP5/MOD3 calculation than in the experimental data. The GDCS flow initiates at about 244 s in both the RELAP5/MOD3 calculation and the experimental data when the vessel pressure decreases below the wetwell pressure.

Figure 6 illustrates a comparison of GDCS flow rates, for both a single line and the total flow. The flow rate is about 20% higher in the RELAP5/MOD3 calculation than in the facility data. The GDCS flow has a significant influence on the behavior of the transient, and the affect of this variation will be discussed in the succeeding paragraphs.

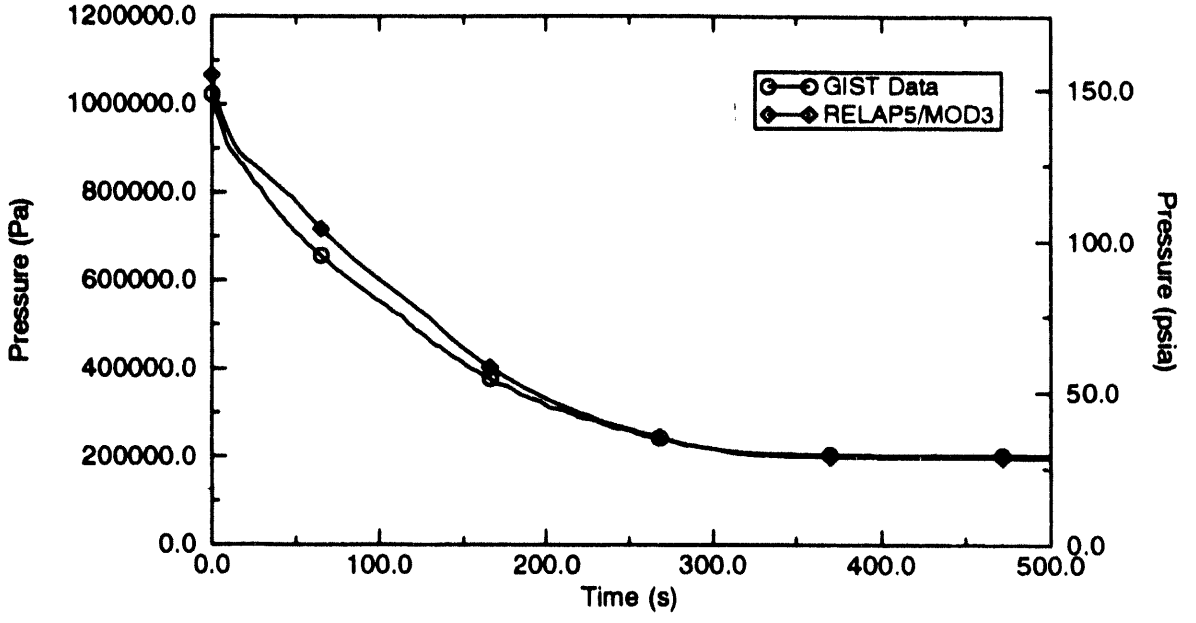


Figure 5. Comparison of RPV dome pressure calculated by RELAP5/MOD3 to GIST data for case B01, main steam line break.

TABLE 3. Transient sequence for MSLB base case

Event	Facility Time (s)	RELAP5/MOD3 Time (s)
RPV at 140 psig, MSIV opens	0.	0.
Core and bypass circulation begins	~20.	~20.
RPV at 100 psig, MSIV closes, high pressure DPV and steamline break open	32.	46.
RPV at 60 psig, low pressure DPV opens	111.	129.
GDCS flow initiates	247.	244.

Figures 7 - 9 provide a comparison of pressure drops at various locations in the RPV. The differential pressure in both the facility and the RELAP5/MOD3 model reflects both static and dynamic effects. Because the GIST facility modeled only the late phase of the blowdown, fluid velocities tend to be relatively low and the differential pressure is dominated by the static head. Although this cannot be confirmed from the facility data, it can be observed from a comparison of the calcu-

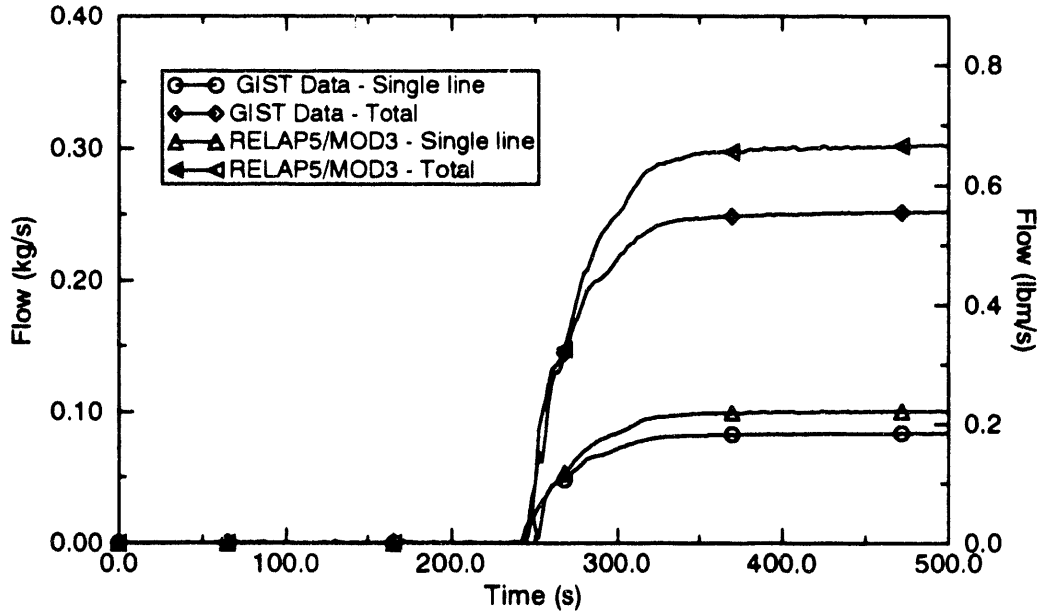


Figure 6. Comparison of GDCS flow calculated by RELAP5/MOD3 to GIST data for case B01, main steam line break.

lated static and dynamic heads at various locations in the RELAP5/MOD3 model. Therefore, it is assumed that the pressure differences observed between the calculation and the test are primarily an indication of water level differences. Within the core region, where vapor velocities on the order of 5 m/s are seen, is the only location where dynamic effects are appreciable.

Liquid levels tend to decrease during blowdown due to inventory loss, and begin recovery following GDCS initiation. This is illustrated in Figure 7, the lower downcomer annulus differential pressure. The RELAP5/MOD3 calculation and the facility data agree for the first 250 s. For the remainder of the transient RELAP5/MOD3 predicted a greater annulus differential pressure than observed in the facility. This is primarily due to the greater GDCS flow calculated in RELAP5/MOD3.

A general decrease in the core pressure drop is observed out to 300 s, as illustrated in Figure 8. Evaluation of the static head indicates that the liquid level decreases during the blowdown, but this is obscured by the dynamic effects of the rising steam. Rapid decreases in the core differential pressure calculated by RELAP5/MOD3 are evident at about 50 s and 130 s, and correspond to decreases in the static head. Table 3 indicates that the high pressure DPV and the steamline break open at 46 s and the low pressure DPV opens at 129 s. These events account for the observed behavior. Increased depressurization leads to flashing of saturated liquid in the core and a decrease of the static head. After 250 s the dynamic head calculated by RELAP5/MOD3 decreases dramatically due to quenching of the core by the GDCS. Overall, RELAP5/MOD3 predicts a greater

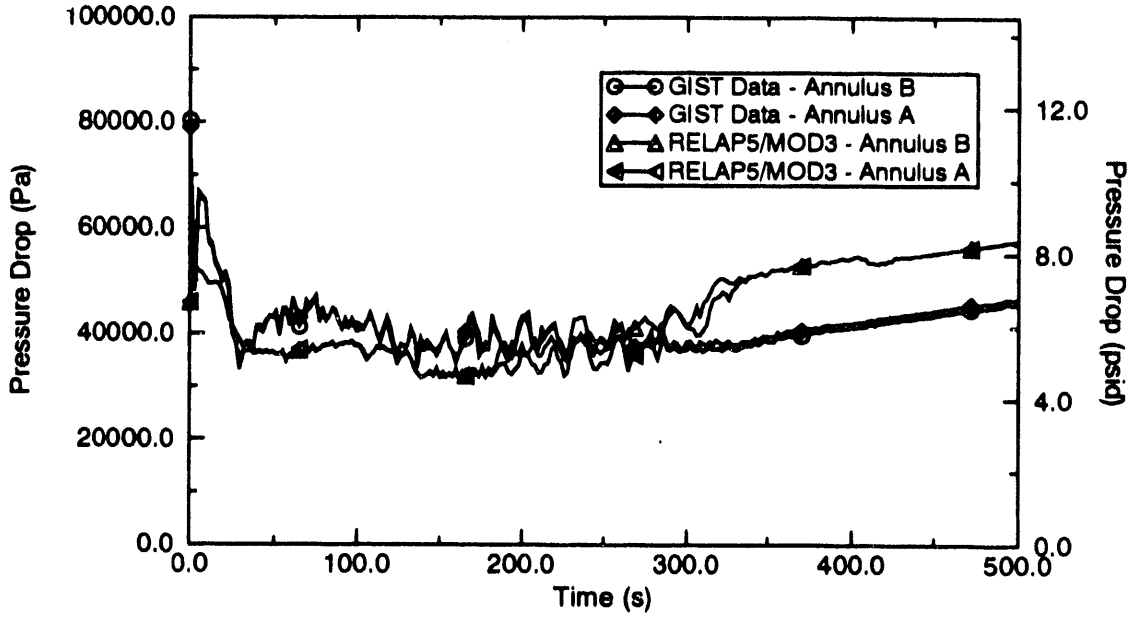


Figure 7. Comparison of annulus pressure drops calculated by RELAP5/MOD3 to GIST data for case B01, main steam line break.

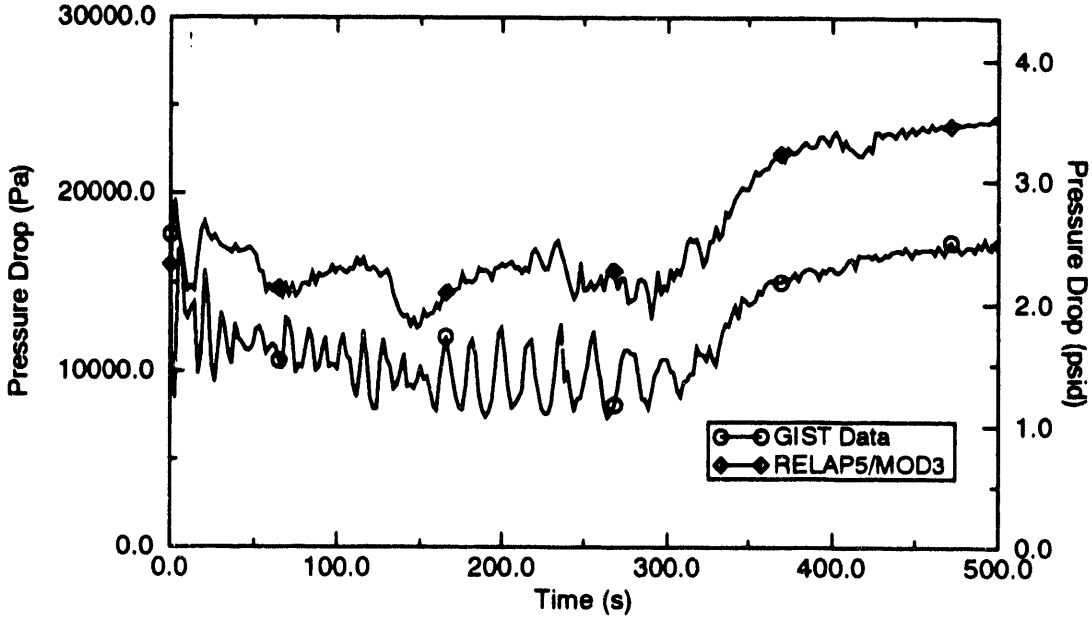


Figure 8. Comparison of core pressure drop calculated by RELAP5/MOD3 to GIST data for case B01, main steam line break.

core differential pressure than observed in the facility data, including portions of the transient when the dynamic head becomes negligible. This indicates that RELAP5/MOD3 calculates a higher fraction of liquid present in the core than seen in the GIST facility data.

Figure 9 shows the core bypass pressure drop. Dynamic effects are negligible within the bypass, but the static head increases to manometrically balance the core pressure drop, so that the liquid level does not decrease significantly during the blowdown. The differential pressure predicted by RELAP5/MOD3 in the bypass is greater than observed in the facility data, but this is directly related to the increased differential pressure in the core.

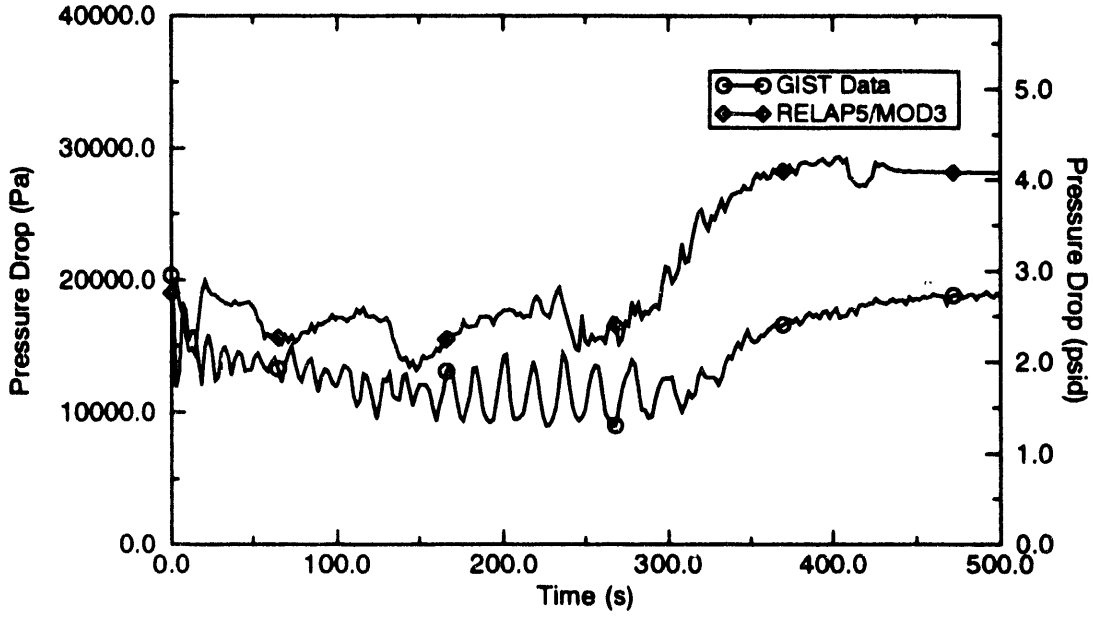


Figure 9. Comparison of bypass pressure drop calculated by RELAP5/MOD3 to GIST data for case B01, main steam line break.

An anomaly referred to as standpipe percolation was observed in the GIST experiments. Standpipe percolation in the GIST facility resulted from a slug of two-phase liquid in the standpipe being forced upwards by a pocket of steam in the upper plenum and expelled. This occurred in a cycle with a period of approximately 20 s. Examination of Figures 8 and 9 reveals one additional fact. Standpipe percolation, or chugging, is calculated by RELAP5/MOD3, but with a noticeably lower amplitude than in the GIST facility data. This is observed most clearly in Figure 10, a comparison of the calculated and measured upper plenum pressure drops.

The general trends discussed in the preceding paragraphs were observed for all of the calculations. Table 4 provides a comparison of the transient event timings between the data and the calculations for each of the four remaining cases. The calculated event timings for each calculation are similar to those observed in the experiments, with the most significant variation occurring at the time of GDCS injection.

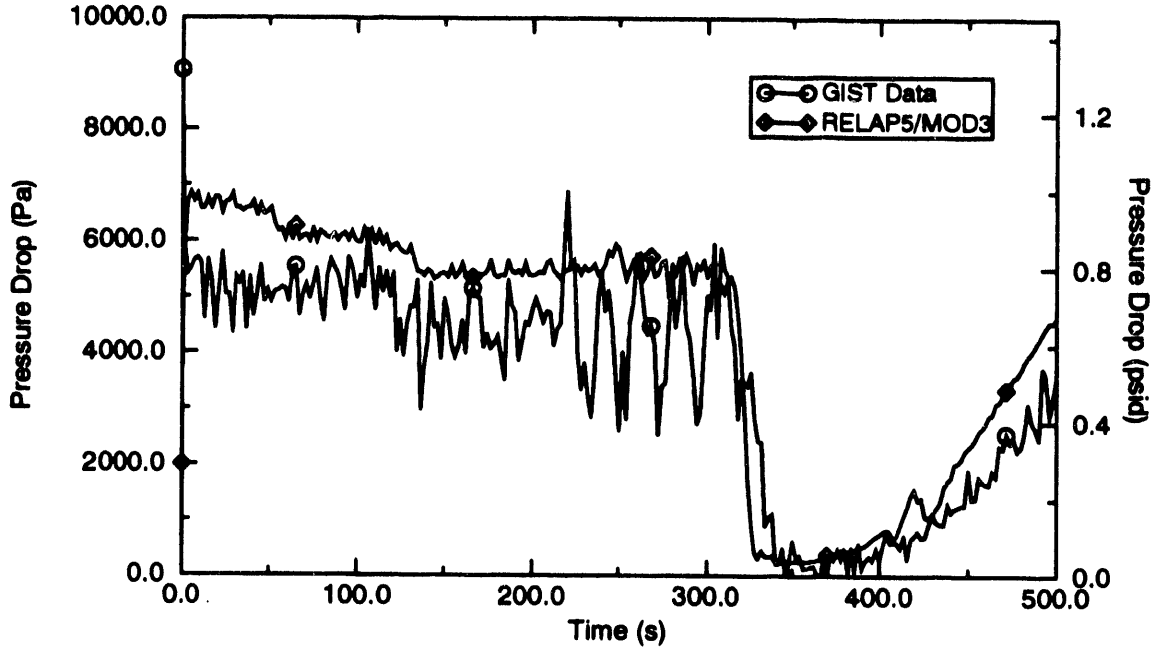


Figure 10. Comparison of upper plenum pressure drop calculated by RELAP5/MOD3 to GIST data for case B01, main steam line break.

TABLE 4. Comparison of the transient event timings between the data and the calculations

	A07		B07		C01		D03	
Event Timing (s)	**Fac.**	**Calc.**	**Fac.**	**Calc.**	**Fac.**	**Calc.**	**Fac.**	**Calc.**
RPV at 140 psig, MSIV opens	0.	0.	0.	0.	0.	0.	0.	0.
Core and bypass circulation begins	~20.	~20.	~5.	~5.	~10.	~10.	~20.	~20.
RPV at 100 psig, MSIV closes, high pressure DPVs open	49.	44.	25.	23.	50.	45.	55.	50.
RPV at 60 psig, low pressure DPVs open	176.	179.	93.	95.	173.	181.	180.	187.
GDCS flow initiates	538.	534.	213.	195.	345.	345.	416.	378.

5 RELAP5/MOD3 Code Modifications

Several minor coding errors were discovered and corrected during the analysis due to the occurrence of code failures and unrealistic results. In one calculation, an error in the calculated heat transfer was observed. In a volume containing primarily air and with the gas temperature exceeding the wall temperature, the gas temperature was rising in the absence of compression. The

problem was traced to the RELAP5/MOD3 routines "DITTUS" and "HTRC1". The calculation of the phase heat flux values involved weighting the total wall heat flux by the void fraction. However, the total wall heat transfer was calculated from the temperature difference between the wall and the liquid, which is inappropriate for the heat flux to the vapor. The problem was corrected by applying the weighting factors to the heat transfer coefficients rather than the total wall heat flux. This permits the calculation of the phase heat flux values using the phase temperatures. This error appeared during recent code development work aimed at partitioning the wall heat transfer between the phases above a void fraction of 0.9 rather than depositing all of the heat in the predominant phase, as has always been done in the past. The aim is to smooth the transition between two-phase and single phase vapor conditions.

In another case, the code experienced thermodynamic state property errors resulting in code failures in vapor-filled volumes as liquid began to enter. This was found to be related to a discontinuity in the Chen correlation for nucleate boiling.[3] In this correlation the heat transfer coefficient is formed from macroscopic and microscopic contributions. The macroscopic portion is directly proportional to F, the Reynold's number factor. F correlates with the reciprocal of the Martinelli parameter, X_{tt}, for $1/X_{tt}$ between 0.1 and 100. The Martinelli parameter is dependent on the ratio of the vapor mass flux to the liquid mass flux. For small values of the liquid mass flux, large values of $1/X_{tt}$ were produced, exceeding the upper limit of the correlation. Thus, a small value of the liquid flux produced an abnormally large heat transfer coefficient, leading to a rapid rise in temperature and pressure that resulted in code failure. To solve this problem the liquid mass flux was assigned a lower limit of 0.001 kg/s and $1/X_{tt}$ was limited to 100., the top of its valid range. A separate factor in this problem was that the routine "HTRC1" did not allow a surface to go into dryout cooling when the wall temperature remained within one Kelvin above the saturation temperature. This restriction was removed.

In a volume filled primarily with air, the equilibrium quality did not approach 1.0 as the void fraction reached 1.0. This problem was eliminated by determining the equilibrium quality from the gas enthalpy, considering only the contribution from the steam and ignoring the contribution from the air.

6 Summary and Conclusions

- A number of coding errors in RELAP5/MOD3 were discovered and corrected during this analysis. These include:
  -- a violation of second law of thermodynamics for heat transfer in presence of non-condensables;
  -- a discontinuity in Chen correlation for nucleate boiling;
  -- an error in the heat transfer logic for selection of dryout cooling;
  -- the calculation of the equilibrium quality in the presence of non-condensables.

- No information is currently available concerning the break flow rates nor the measurement uncertainties associated with the GIST data. The lack of this information and detailed facility design information limit the usefulness of direct comparisons between code calculations and experimental results.
- The following trends were uncovered in the data comparison, and may be useful in providing direction for future work:

  --RELAP5/MOD3 calculated a GDCS flow rate that was about 20% greater than the value measured at the GIST facility,

  --RELAP5/MOD3 predicted a higher fraction of liquid present in the core than seen in the GIST facility data.

  -- RELAP5/MOD3 calculated a lower amplitude chugging in the standpipe than observed in the GIST facility data.

References

1. *SBWR Standard Safety Analysis Report*, GE Nuclear Energy, 2515113 Rev. A, August 1992.
2. P. F. Billig, *Simplified Boiling Water Reactor (SBWR) Program Gravity Driven Cooling System (GDCS) Integrated Systems Test -- Final Report*, GEFR-00850, October 1989.
3. C. M. Allison et al., *RELAP5/MOD3 Code Manual, NUREG/CR-5535, EGG-2596 (Draft), Volumes 1-4*, June 1990 (available from EG&G Idaho, Inc.).
4. J. T. Han, *Summary of the RES/NRR Meeting on SBWR-Related Topics on June 10, 1993 (an NRC memo dated July 1, 1993).*
5. C. M. Kullberg et al., *Survey of Experimental Data Base for the Simplified Boiling Water Reactor*, EGG-NE-10474 (Draft), May 1993.
6. G. E. McCreery, *Adequacy of the GIST Test Program for Modeling SBWR Accidents and Transients*, proprietary, EG&G Letter Report, April 1993.

RELAP5/MOD3 CODE COUPLING MODEL

R. P. Martin, G. W. Johnsen
Idaho National Engineering Laboratory

ABSTRACT

A new capability has been incorporated into RELAP5/MOD3 that enables the coupling of RELAP5/MOD3 to other computer codes. The new capability has been designed to support analysis of the new advanced reactor concepts. Its user features rely solely on new RELAP5 "styled" input and the Parallel Virtual Machine (PVM) software, which facilitates process management and distributed communication of multi-process problems. RELAP5/MOD3 manages the input processing, communication instruction, process synchronization, and its own send and receive data processing. The flexible capability requires that an explicit coupling be established, which updates boundary conditions at discrete time intervals. Two test cases are presented that demonstrate the functionality, applicability, and issues involving use of this capability.

I. INTRODUCTION

The primary purpose of the development of this new capability was for the coupling of RELAP5/MOD3 (1), a best-estimate thermal-hydraulic systems code, and CONTAIN (2), a best-estimate containment analysis code. The motivation for the union of these two computer codes stems from the unique safety analysis challenge presented by the new Advanced Light Water Reactor (ALWR) designs. Incorporated into these designs are long term passive cooling systems integrating mechanisms in the main reactor coolant system and in the containment. Westinghouse's AP600 and General Electric's SBWR are two examples of designs that meet this description.

A proof-of-principle that RELAP5/MOD3 could be coupled with CONTAIN was performed by Smith at the Pennsylvania State University (3). This work demonstrated that the state-of-the-art best estimate codes could be linked to generate very meaningful results. The RELAP5/MOD3 code coupling capability evolved from this project to feature a generic infrastructure within RELAP5/MOD3 for defining links between RELAP5/MOD3 and another computer code. The implementation of this concept as described in the following sections extends Smith's previous work by addressing the lessons learned from the original effort and through added robustness of the coupling.

The code coupling model exploits the Parallel Virtual Machine (PVM) Software (4) developed at the Oak Ridge National Laboratory for the Department of Energy. The PVM software was designed to provide multiprocessing capabilities on a loosely coupled network of diverse computer systems. The primary role of PVM, as applied to RELAP5/MOD3 code coupling capability, is the process management, inter-process communication, and synchronization capabilities it offers. These routines manage the identification of parallel processes, the timing of when data is delivered from one code to the other, and the transmission of data from one code to the other.

The code coupling link described here is used to define an "explicit couple" with RELAP5/MOD3. An explicit couple implies that the calculation solutions of

RELAP5/MOD3 and the coupled code are performed independently. Data from one code is introduced into the other code through static or dynamic boundary conditions imposed on the system models. Application of an explicit coupling model, while not as accurate as an implicit method that simultaneously solves the solution matrices of the complete problem described by separate system models, allows for the general application of a coupling model. Moreover, an explicit coupling lends itself to the modeling the RCS/containment linkage since conditions change very slowly in the containment relative to the RCS.

The ability to couple a RELAP5/MOD3 reactor coolant system model to a CONTAIN containment model eliminated the need to develop and assess new containment modeling capabilities in RELAP5/MOD3. Such an effort would have been redundant to the development and assessment of CONTAIN being carried out by Sandia National Laboratory. This added capability allows for improved analysis and simulation of thermal-hydraulic systems by providing a means for applying phenomenological models of systems that are beyond the scope of RELAP5/MOD3. New models can also be tested through this link quickly while maintaining the integrity of the RELAP5/MOD3 coding. An additional benefit of this feature is that it allows for the exploitation of dual processor machines that will enhance speed performance.

II. SOFTWARE DESIGN

The software design philosophy for implementing the code coupling capability into RELAP5/MOD3 was to ensure ease of use. The result is the analyst must only learn how to provide coupling input to the RELAP5/MOD3 input models and how PVM works with processes.

II.A The Role of Parallel Virtual Machine (PVM) Software

The PVM software was designed to provide multiprocessing capabilities on a loosely coupled network of diverse computer systems. The application of PVM to the RELAP5/MOD3 code coupling capability provides process management, inter-process communication, and synchronization capabilities. These routines manage the identification of parallel processes, the timing of when data will be delivered from one code to the other, and the transmission of data from one code to the other.

The process management routines in PVM that are used in the coupling feature include functions that identify potential processes for parallel execution and initiate individual processes. The identification of potential processes for parallel execution involves the establishment of a link that can be referenced for all communication between parallel processes. Initiatior of a process begins execution of a second process and begins any further communication between processes.

The data transfer routines in PVM provide the message passing feature necessary for communicating RELAP5/MOD3 data and data from another code. With PVM a message destination is referenced with data transmission routines during execution. Query routines are also available to monitor how the communication is proceeding. PVM version 3.1 was used with the RELAP5/MOD3 code coupling capability.

II.B Coordination Strategy

The design of a code coupling capability in RELAP5/MOD3 required that some overhead must be performed for this to be a useful feature. The performance of this overhead distinguishes RELAP5/MOD3 as the "parent" process in any coupled calculation. The actual "parent" responsibilities of RELAP5/MOD3 are minimal. It involves execution of the "child" process; reading information provided by input;

determining what information is required by the "child"; sending that information; and then finally releasing the link. The data that is sent to the "child" process contains information on the frequency of communication and the structure of the data transmission data streams. Following this step, both processes run independently, pausing for data transmission at the prescribed times. Both the "parent" and "child" processes are responsible for the collection of data needed to be transferred and integration of received data into respective solution schemes. For synchronization of the two processes, it is assumed that the parent process will be the most CPU intensive process and will run slower than the child process. This situation has the child process waiting for information from RELAP5/MOD3 while RELAP5/MOD3 performs its calculation.

II.C Data Compilation, Manipulation, and Integration in RELAP5/MOD3

Since RELAP5/MOD3 is the "parent" process when coupled with another code, it has the responsibility for determining the shared data between RELAP5/MOD3 and the other code and conveying that information to that other process. This information must contain a RELAP5/MOD3 source type, volume number, labels that describe the source in the child process, and a message tag that specifically identifies the information that is being sent. All this information comes from the RELAP5/MOD3 input file.

The RELAP5/MOD3 source type and volume number define the source or sink of data going to and from RELAP5/MOD3, respectively. The RELAP5/MOD3 source type refers to a RELAP5/MOD3 variable (defined like minor edits) that is available during a calculation. The advantage of using RELAP5/MOD3 variables directly is in the reduction of specific hardwired coding into RELAP5/MOD3, the flexibility in being able to define control variables that are not normally available, and in the general application of this coupling model. This data is sent to the other code sorted by message tag as described in the input defining this information. Data received from the child process is incorporated into a time dependent volume or time dependent junction depending on the type of information received.

The child process simply must act on the data it receives from RELAP5/MOD3. RELAP5/MOD3 is responsible for sending the data needed by the child process to use in its calculation procedure. As determined by the RELAP5/MOD3 input file, a data stream is sent from RELAP5/MOD3 to the child process. The child process receives this information and incorporates this data appropriately into the child process as defined by the labels given in the input. Conversely, the child process must gather the data that RELAP5/MOD3 needs and send it to RELAP5/MOD3.

II.D Input Format

The input format contains information on what process to start, frequency of data transmission for both sending and receiving data for the parent, the parent-to-child link descriptions, and the child-to-parent link descriptions. The child process name identifies the child process. Data transmission frequency can be provided as a function of time through the inclusion of additional input cards. This gives the user flexibility to perform coupled calculations more efficiently by eliminating unnecessary communication between processes. Separate lists describe exactly what is sent and how to send it to the child process and what information is received from the child process and where to put it. This list includes "minor edit" styled RELAP5/MOD3 variables, label words that describe the message, and an integer message tag. The 20900000 card number series has been created for this new feature.

III. DESCRIPTION OF NEW CODING

The existing coding in RELAP5/MOD3 conforms to the FORTRAN 77 standard and all modifications and extensions to the existing coding adhere to this standard and the existing style and idiom of RELAP5/MOD3. Additionally, a RELAP5/MOD3 executable must include the library of routines that make up the PVM software. Figure 1 presents a flow chart of how RELAP5/MOD3 and a generic child process are coupled.

Code modifications to RELAP5/MOD3 are isolated to single calls to new subroutines that involve the execution of the child process, and the reading and interpreting of the coupling data. Interpreting the coupling data includes assigning variables containing this information, and sending the relevant child process information to the child process.

RR5COUP and IR5COUP are the input processing routines. RR5COUP performs the actual reading of the input file and the storing of that information. STRPVM is the subroutine responsible for the initialization of the any coupling calculation. This involves enrolling RELAP5/MOD3 as a process under PVM and spawning the second process under PVM. PVMSND and PVMRCV are subroutines call by RELAP5/MOD3 subroutine DTSTEP to monitor the data exchange frequency, create or interpret a data stream based on the coupling information and exchange the data stream at the specified interval times. A new common variable, TIMEHO, is used to indicate whether PVMSND and PVMRCV are being called at the first time step. At the first time step of any coupling calculation, PVMSND provides the child process with the start and end times of the calculation, the number of send and receive messages, the frequency of communication information, and the specific messages. TIMEHO is then reset in the subroutine TRAN to indicate that RELAP5/MOD3 has advanced past the first time step. During the calculation, PVMSND and PVMRCV determine whether if at any given time step, it is time to exchange data to or from the child process. If so, data is exchanged. This procedure requires synchronization with the child process; therefore, every send call is followed by a receive call verifying that the data was sent properly. PVMPUT and PVMSET are subroutines that manage the implementation of data received from the child process into RELAP5/MOD3's time dependent volume and time dependent junction components. Both of these subroutines are called by subroutine TSTATE before processing the time dependent volumes. PVMFXREC and GETSEC are subroutines designed to provide error checking during sending or receiving between RELAP5/MOD3 and the child process. They provide a means for a "time out" if the child process has not responded within a specified time interval. PVMFXREC also checks to ensure that PVM is still activated.

IV. CAPABILITY, LIMITS, AND EXPANDABILITY OF RELAP5-BASED CODE COUPLING

Coupling RELAP5/MOD3 and a child process in this configuration creates a powerful new tool for nuclear power plant systems analysis. This configuration permits wide range flexibility for establishing links between two codes with very specific coupling information. The coupling data input tells the two codes exactly what and when to transfer data and how to use it when it is received by the other process. However, this configuration does not facilitate the coupling of the simultaneous equations in both codes to achieve the best accuracy possible. Instead the data that are received by a process are integrated as constant boundary conditions (i.e., an explicit couple). This can introduce error that is dependent on the frequency of communication. In the extreme case where communication between the codes occurs every time step, this error may be negligible; however, this may be a computationally intensive situation that would not be attractive from a productivity standpoint. Conversely, using very large time steps would not be

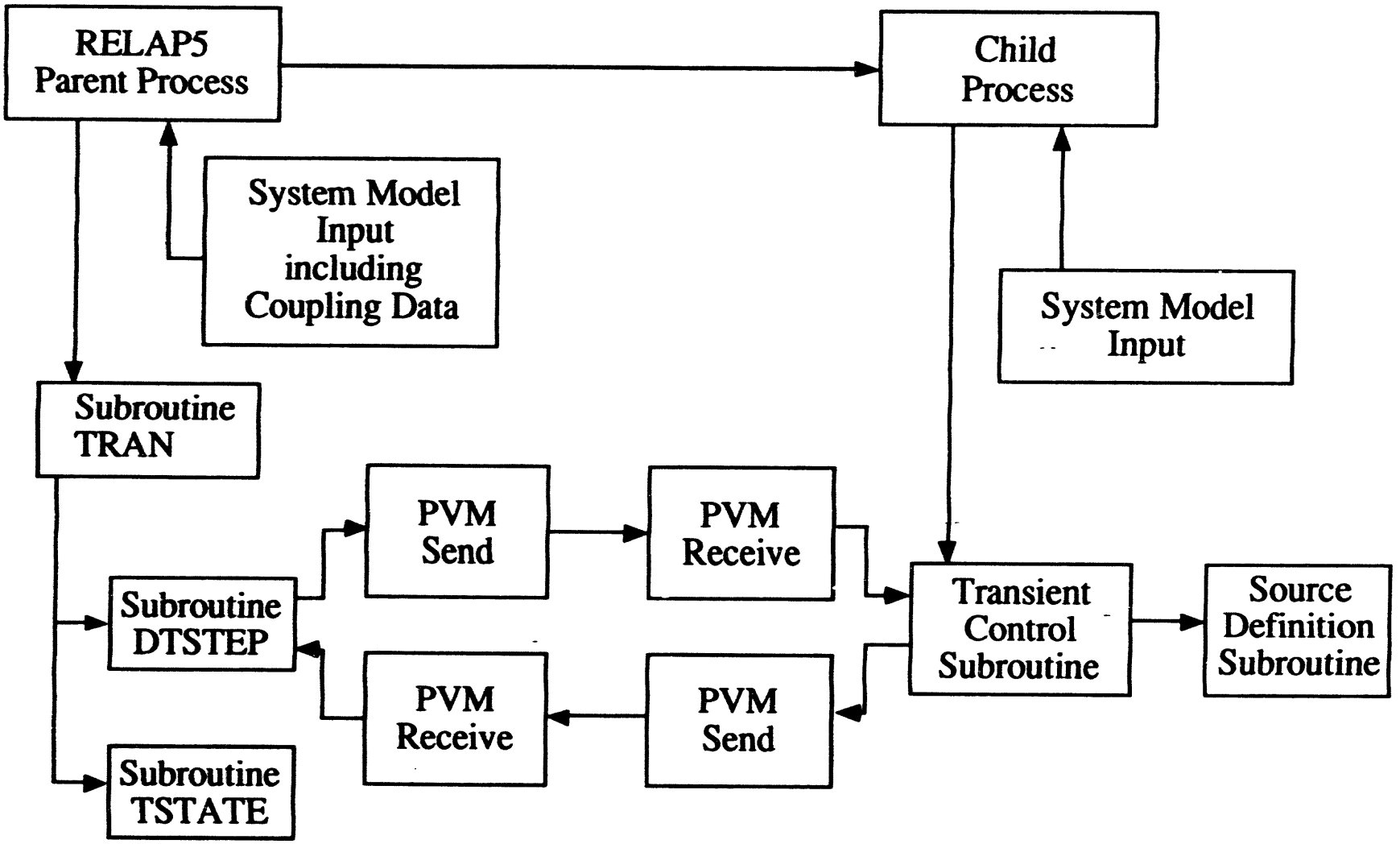


Figure 1. RELAP5/MOD3 Generic Code Coupling Flow Chart.

attractive from an accuracy standpoint. This situation requires the analyst to perform time step sensitivity calculations to assess the accuracy benefits of smaller time steps versus the productivity benefits of larger time steps. Since RELAP5/MOD3 control variables are available to send to a child process, corrections can be applied to data being sent to reduce this error. A possible future feature of this coupling might include a time step control based on information passed from RELAP5/MOD3 through control variables.

V. TESTING, VERIFICATION, AND EXPERIENCE WITH MODEL

The new coding has been verified through four test cases, two of which are described here. The first case tested a simple connection of two separate RELAP5/MOD3 models. A more robust case connected RELAP5/MOD3 and CONTAIN models to simulate a main steam line break in the General Electric Simplified Boiling Water Reactor (SBWR).

V.A RELAP5/MOD3 coupled with RELAP5/MOD3

This case demonstrated the applicability of the RELAP5/MOD3 coupling model to couple with other RELAP5/MOD3 processes. This simple case involves two identical RELAP5/MOD3 models of a pipe bounded by time-dependent volumes (TMDPVOLs) on either end. In one model the pressure is ramped from 100 kPa to 200 kPa. The other model receives the pressure information through the coupling link and advances the pressure discretely. Figures 2 and 3 show the pressure signatures from both models. While the pressure is linearly ramped in the parent process, the child process experiences the discrete stepwise pressure advancement. Figure 3 shows this difference in greater detail.

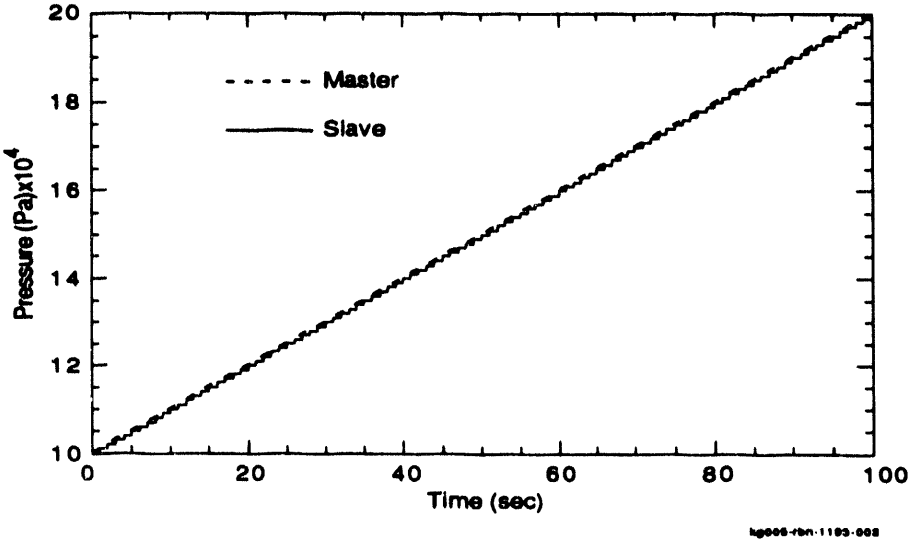


Figure 2. Volume Pressures in RELAP5 Test Case

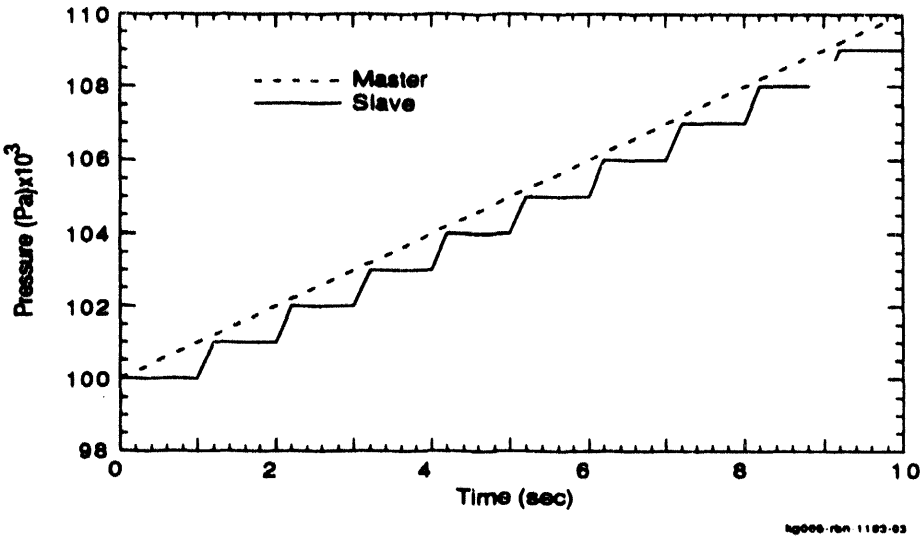


Figure 3. Volume Pressures in RELAP5 Test Case - Expanded Scale

This test case plainly demonstrates how the code coupling feature applies an explicit couple. Using an explicit couple requires that sensitivity studies need to be performed to assure that a proper communication frequency is used to adequately couple the problem.

V.B SBWR Main Steam Line Break

This case simulated a main steam line break (MSLB) in the SBWR and presented a much more sophisticated test for coupling RELAP5/MOD3 and CONTAIN. In this case over fifty variables were exchanged between the two codes. Figure 4 shows a simple nodalization of the SBWR containment and indicates coupling locations. Table I identifies those variables shared between the codes. A unique aspect of the SBWR containment is the passive containment cooling system (PCCS). The PCCS is responsible for long term cooling of the containment during abnormal conditions. The containment atmosphere is driven into the PCCS through natural convection and vapor is condensed while noncondensible gases are separated and diverted into the suppression chamber. Since CONTAIN does not have a model for describing this component, RELAP5/MOD3 was used to mechanistically model this component as best as possible.

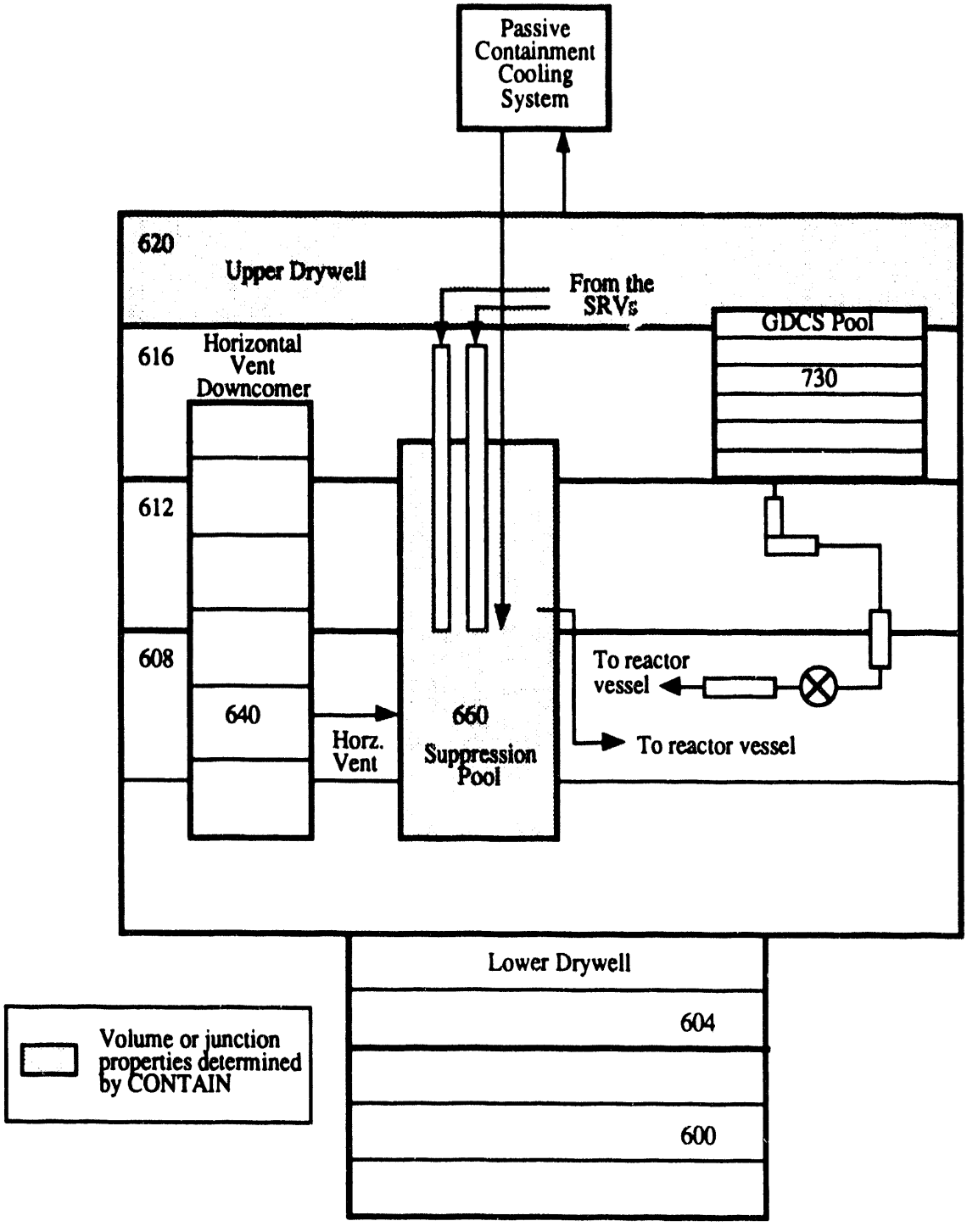


Figure 4. SBWR containment nodalization with coupling locations identified.

Table I
Coupling variables for the SBWR Main Steam Line Break

Phenomena	RELAP5/MOD3	CONTAIN
Break Mass Flow	X	
PCCS Mass In-Flow	X	
PCCS Mass Out-Flow	X	
Break Enthalpy Flow	X	
PCCS Enthalpy In-Flow	X	
PCCS Enthalpy Out-Flow	X	
Drywell Pressure		X
Drywell Temperature		X
Drywell Void Fraction		X
Drywell Liquid Internal Energy		X
Drywell Vapor/Noncondensible Internal Energy		X
Noncondensible Quality in Drywell		X
Suppression Chamber Pressure		X
Suppression Chamber Temperature		X
Suppression Chamber Void Fraction		X
Suppression Chamber Liquid Internal Energy		X
Suppression Chamber Vapor/Noncondensible Internal Energy		X
Noncondensible Quality in Suppression Chamber		X
Vacuum Breaker Mass Flow		X

While a number of important lessons were learned from the limited amount of experience using this new feature, the most important lesson involved what information should be passed between the codes. It was determined that when sending information to RELAP5/MOD3 TMDPVOLs, the input model developer should ensure that the child process sends all the same variables described with the initial condition option. This became clear when performing the SBWR MSLB. This very robust problem involved the sending and receiving of the multi-species (air, vapor and liquid water) volume properties.

The break was initiated by instantaneous rupture of one steam line upstream of the main steam isolation valves (MSIVs). This results in a break that discharges to the drywell. Break flow from the reactor vessel is limited by restricting orifices in the steam nozzles. Break flow from the MSIV side of the break stops almost immediately after break initiation as the MSIVs close quickly. The transient calculation was performed for 60 seconds following the break.

Following the break the reactor vessel pressure decreased rapidly as shown in Figure 5. Figure 6 shows the break flow from the steam line; this represents the boundary condition sent to CONTAIN from RELAP5/MOD3. As the vessel depressurized, liquid

was pulled up the downcomer and into the broken steam line, as evidenced by the oscillation in the break flow seen in Figure 6 beginning at approximately 40 seconds.

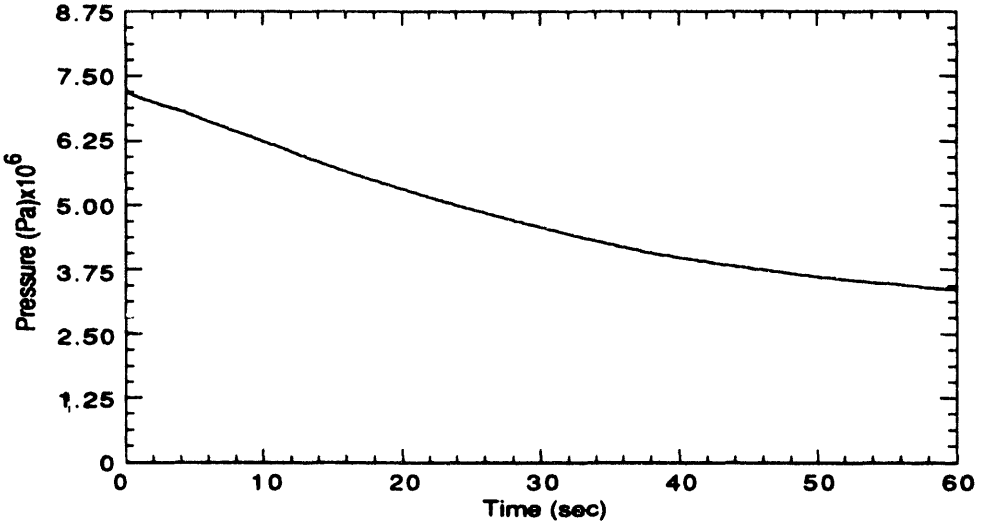


Figure 5 Vessel Pressure for SBWR MSLB Simulation

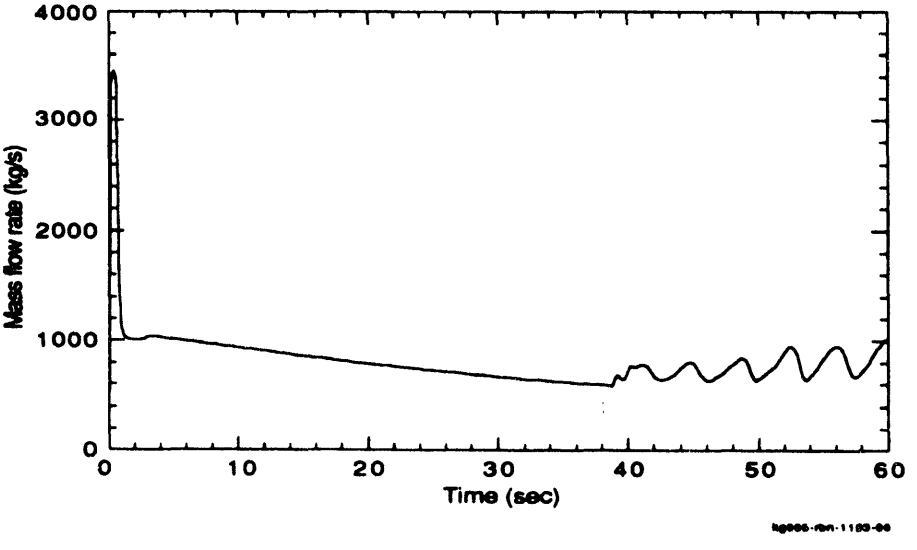


Figure 6 Break Discharge for SBWR MSLB

Figures 7-10 present the pressure and temperature from the drywell and suppression chamber, respectively. The RELAP5/CONTAIN calculation predicted a gradual pressurization of both the drywell and suppression chamber without the blowout of the horizontal vents.

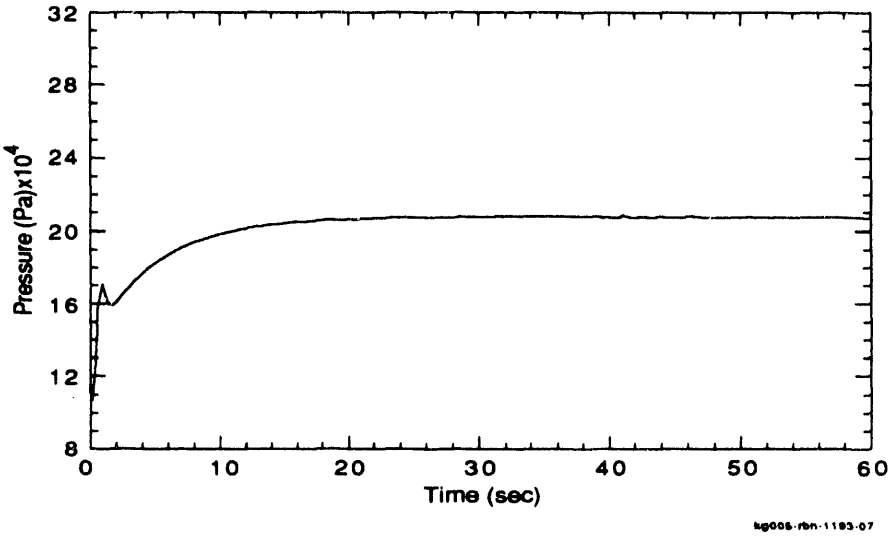


Figure 7. Drywell Pressure for SBWR MSLB

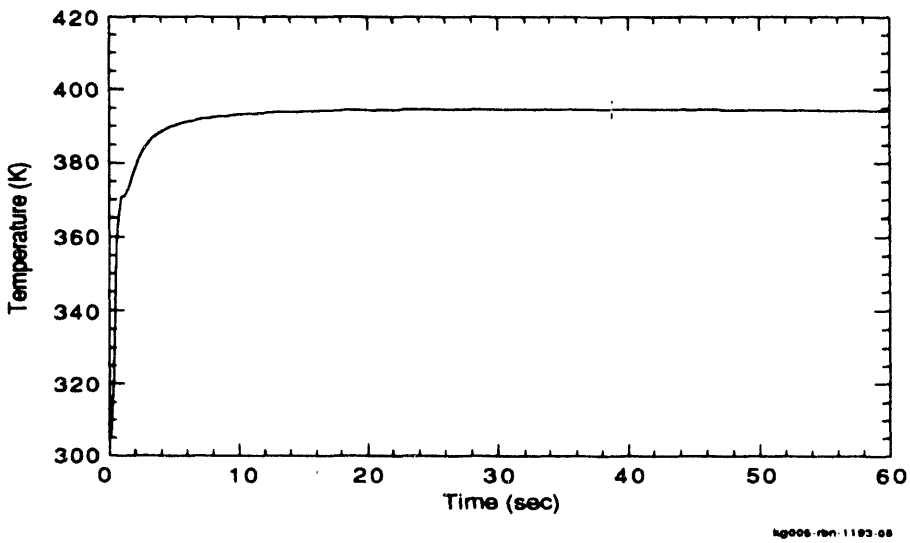


Figure 8. Drywell Temperature for SBWR MSLB

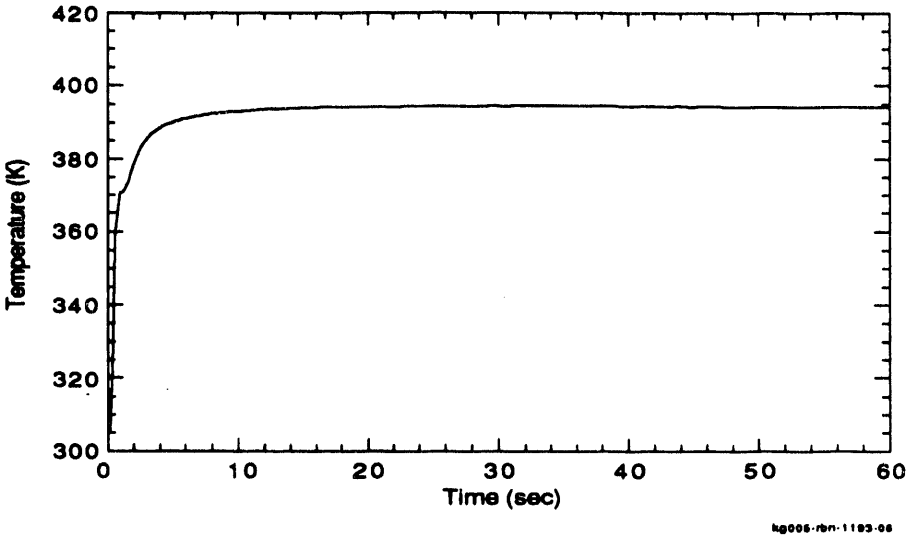


Figure 9. Suppression Chamber Pressure for SBWR MSLB

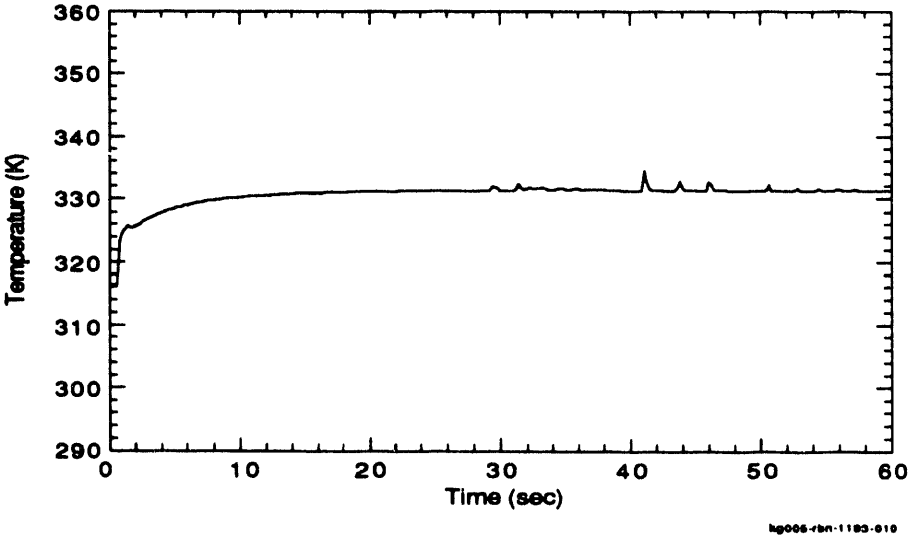


Figure 10. Suppression Chamber Temperature for SBWR MSLB

As two-phase discharge from the break enters the drywell, the vapor displaces the air in the containment and the two species stratify, with the lighter water vapor filling the topmost regions of the containment. The noncondensable quality (weight percent of air) in these regions quickly decreases as shown in Figure 11. The increase in water vapor entering the PCCS heat exchanger gives rise to a rapid increase in heat removal via condensation inside the PCCS tubes. Figure 12 shows the calculated heat removal rate

during the transient, which is shown as a negative quantity (i.e., negative heat addition to containment atmosphere).

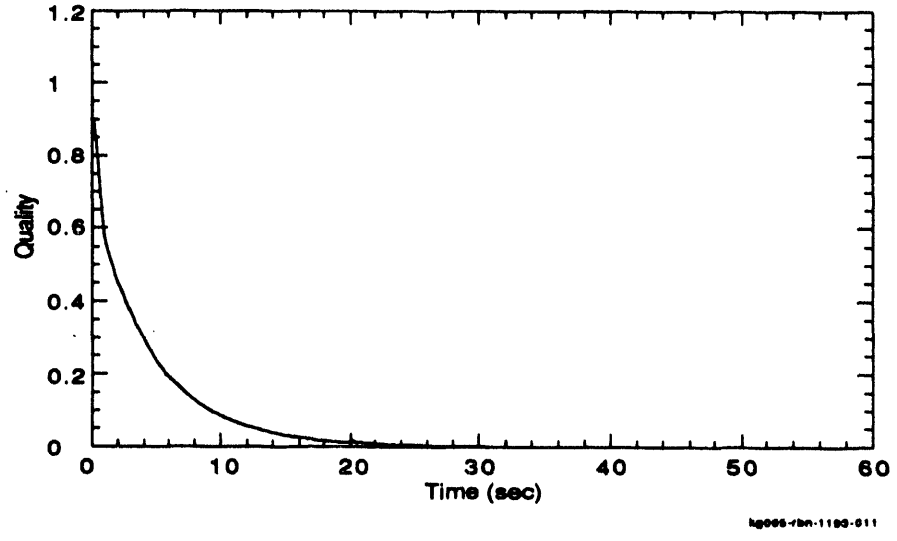


Figure 11. Noncondensable quality in upper Drywell for SBWR MSLB

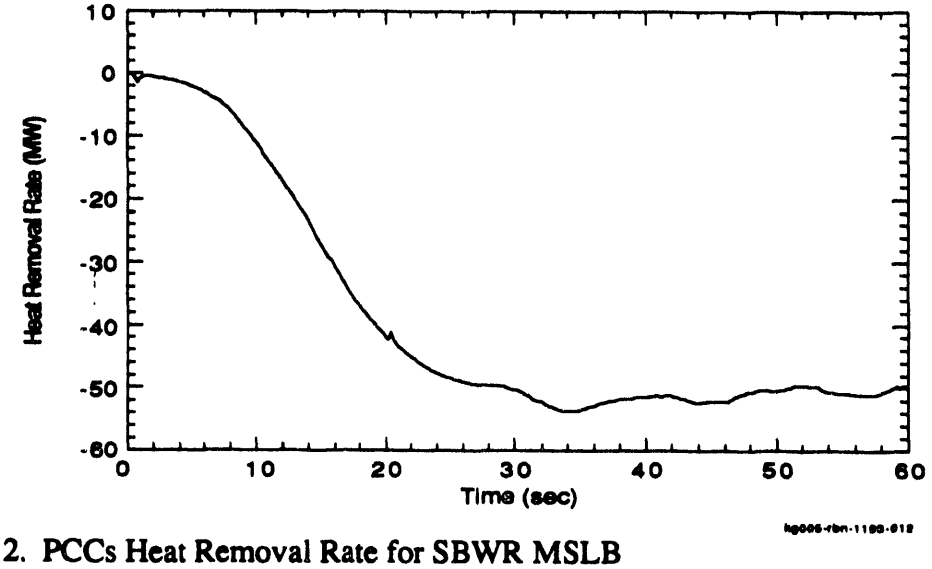


Figure 12. PCCs Heat Removal Rate for SBWR MSLB

VI. SUMMARY AND CONCLUSIONS

A new feature has been developed and implemented in RELAP5/MOD3 that allows the coupling of data between RELAP5/MOD3 and other codes. Specifically, the containment analysis code CONTAIN has been linked with RELAP5/MOD3. This feature uses the parallel process management and data transfer capabilities provided by the Parallel Virtual Machine (PVM) software. An explicit coupling method was used with this new capability. An explicit couple discretely updates boundary conditions between codes rather than solving a combined solution matrix of the two processes as required by a rigorous implicitly coupled model. While the explicit model may be less accurate, it can be generally applied to many problems. Coupling with RELAP5/MOD3 is activated by introducing new input into any standard RELAP5/MOD3 input model file that includes the name of the code to be coupled, a table of time dependent data transmission frequencies, a table of variables to be sent to the coupled code (e.g., CONTAIN) and a table of variables to receive data from the coupled code. The infrastructure of this model has been designed to be as general as possible to allow the coupling of RELAP5/MOD3 with any code. Results from four test problems demonstrate the feasibility of the coupling model through the proper transmission, processing and integration of data between RELAP5/MOD3 and other codes.

ACKNOWLEDGMENTS

This work was supported by the U.S. Nuclear Regulatory Commission Contract L2537 under the DOE contract DE-AC07-76ID01570.

REFERENCES

1) K. E. Carlson, et. al., "RELAP5/MOD3 Code Manual, Volume I: Code Structure, System Models, and Solution Methods (Draft)," NUREG/CR-5535 (EGG-2596), EG&G Idaho, Inc., 1990.

2) K. K. Murata, et. al., "User's Manual for CONTAIN 1.1, A Computer Code for Severe Nuclear Reactor Accident Containment Analysis," NUREG/CR-5026 (SAND87-2309), Sandia National Laboratory, 1990.

3) K. A. Smith, "Multiprocessor Based Simulation of Degraded Core and Containment Responses," Ph.D. Thesis, Pennsylvania State University, December 1992.

4) A. Geist, et. al., PVM (Parallel Virtual Machine) User's Guide and Reference Manual, Oak Ridge National Laboratory, Oak Ridge, TN, ORNL/TM-12187, 1993.

RAMONA-4B DEVELOPMENT FOR SBWR SAFETY STUDIES *

U. S. Rohatgi, A. L. Aronson, H. S. Cheng, H. J. Khan, A. N. Mallen
Department of Advance Technology, Brookhaven National Laboratory, Upton, New York 11973

1. INTRODUCTION

The Simplified Boiling Water Reactor (SBWR) is a revolutionary design of a boiling-water reactor. The reactor is based on passive safety systems such as natural circulation, gravity flow, pressurized gas, and condensation. SBWR has no active systems, and the flow in the vessel is by natural circulation. There is a large chimney section above the core to provide a buoyancy head for natural circulation. The reactor can be shut down by either of four systems; namely, scram, Fine Motion Control Rod Drive (FMCRD), Alternate Rod Insertion (ADI), and Standby Liquid Control System (SLCS). The safety injection is by gravity drain from the Gravity Driven Cooling System (GDCS) and Suppression Pool (SP). The heat sink is through two types of heat exchangers submerged in the tank of water. These heat exchangers are the Isolation Condenser (IC) and the Passive Containment Cooling System (PCCS).

The unique design of SBWR imposes new requirements on the analytic methods for modeling its behavior. The close coupling between the power and flow, and also flow distribution among the parallel channels require a multidimensional power-prediction capability. The startup of the reactor has vapor generation and condensation taking place in the core requiring a model with a non-homogeneous, nonequilibrium, two-phase formulation. The instability at low flow/high power conditions requires modeling of the control systems and balance of plant, which has significant impact on the amplitude of the instability-induced power and flow oscillations.

The RAMONA-4B code has been developed to simulate the normal operation, reactivity transients, and to address the instability issues for SBWR. The code has a three-dimensional neutron kinetics coupled to multiple parallel-channel thermal-hydraulics. The two-phase thermal hydraulics is based on a nonhomogeneous nonequilibrium drift-flux formulation. It employs an explicit integration to solve all state equations (except for neutron kinetics) in order to predict the instability without numerical damping.

The objective of this project is to develop a Sun SPARC and IBM RISC 6000 based RAMONA-4B code for applications to SBWR safety analyses, in particular for stability and ATWS studies.

---

* This work was performed under the auspices of the U.S. Nuclear Regulatory Commission.

2. CODE IMPROVEMENTS

2.1 Steady-State Natural-Circulation Capability

The steady-state flow calculation in RAMONA-4B requires an iterative procedure to ensure equal pressure drop across the parallel core channels and to satisfy the loop momentum balance. The inner loop iterates on the core pressure drop and the outer loop iterates on the momentum balance. In the earlier version RAMONA-3B [1], the outer iteration loop is replaced by an adjustment of the jet pump head to satisfy the loop momentum balance. This simple adjustment is not applicable to an SBWR with natural circulation.

For general applicability of the code to both the natural and forced circulation, an outer iteration loop has been added to the steady-state flow calculation so that the loop momentum balance is achieved by adjusting the loss coefficient at the riser exit. This approach has worked quite well for the SBWR. However, because of the sensitivity of the thermal-hydraulic instability to the loss coefficient in the high-void region, it is recommended that the core inlet and single phase loss coefficient which supplement the two-phase losses in loop momentum equation be properly estimated.

2.2 Chimney Component

The chimney of SBWR is an additional vertical height extended from the upper plenum. It has been modeled in the RAMONA-4B code as a modified riser component, such that the total length of the riser can be divided into two parts, comprising the chimney and the separator.

The vertical height due to the riser is a one-dimensional flow path with two-phase wall friction, while the separator has its own loss-coefficient model. The upper plenum, separator, and the riser are modeled together with the assumption that there is no steam generation. The design objective of this component is to maintain a one-dimensional flow and provide required buoyancy head.

2.3 Flow-Dependent Loss Coefficients

The flow-dependent loss coefficients are important for the natural-circulation system of SBWR. The resistance due to the abrupt change in flow area and flow through orifices are functions of the Reynolds number. In RAMONA-4B, this has been accounted for by providing explicit loss coefficients for the inlet and exit of each flow segment in the form

$$f = a\,Re^{b} + c \quad ,$$

where, a, b, and c are user-specified input data on the flow-dependent loss coefficients. These values are different for laminar and turbulent flow regimes.

2.4 Isolation Condenser

Isolation Condensers (IC) are important components of the safety systems for the advanced design of SBWR by General Electric (GE). Active usage of Isolation Condensers can also be found in a few of the current operating reactors, e.g., Oyster Creek, Millstone, etc. Applications of these components include passive operation for reactor pressure regulation as well as in decay-heat removal. IC consists of a heat exchanger submerged in a pool. The heat exchanger is connected to the steam dome for steam supply and to the downcomer for the return of condensate.

The Isolation Condenser model incorporated into RAMONA-4B is based on the IC design of GE SBWR [2]. The Isolation Condenser has been modeled as a single control volume enclosing the condenser tubes with an upper and a lower plenum. The model accounts for variation in pool side heat transfer coefficient in different tubes. Transient mass and energy balance equations are used to solve for pressure and enthalpy within the control volume. Momentum change in the IC is assumed to be negligible. The governing equations for the IC model and the geometry of the IC have been reported earlier [3]. The flow inertia in the lines to and from the IC are assumed to be negligible. Therefore, they are decoupled from the transient mass and energy balance of the IC. The quasistatic momentum equations for the inlet steam line and the condensate return line determine the rate of steam inflow and condensate outflow from the IC. Steam entering the IC is assumed to be always saturated, while the liquid leaving the IC is at either subcooled or saturated condition, depending on the heat removal capacity. The initial level of liquid in the IC is a variable depending on the existing two-phase mixture state.

Heat removal from the system is dependent on the IC pool condition and the heat transfer characteristics of the IC tubes in response to the variable thermal conditions inside the tubes. Three important heat transfer mechanisms considered in this model are:

1. Turbulent film condensation heat transfer inside the multiple parallel IC tubes,

2. Heat conduction through the tube wall, and

3. Natural convection and pool boiling heat transfer between the tube external surfaces and the pool water.

2.5 Balance of Plant (BOP)

Balance-of-plant models are needed for a realistic prediction of plant transients. For the earlier version RAMONA-3B without the BOP models, it was necessary to prescribe the BOP response in a plant transient as the boundary conditions (e.g., feedwater flow and temperature). Since the boundary conditions are not known *a priori*, such an approach will contribute to the uncertainty of the predicted transient response. Furthermore, the BOP response might have a feedback effect on the large-amplitude density-wave oscillation owing to the thermal-hydraulic instability.

The BOP models [4] of the BNL Engineering Plant Analyzer (EPA) have been implemented in the RAMONA-4B code. The BOP models consist of:

1. Turbine dynamics,
2. Feedwater train dynamics,
3. Feedwater preheater dynamics,
4. Condenser dynamics.

The turbine dynamics is modeled by quasistatic mass, energy, and momentum balance. The high-pressure turbines and low-pressure turbines are lumped into a two-stage turbine, an impulse stage and a reaction stage. The inlet and exit mass flow rates of the turbines as well as the extraction steam are calculated without the flow inertia (quasistatic momentum balance). The inlet and exit turbine enthalpies are calculated in terms of the isentropic turbine enthalpy loss and a turbine efficiency.

The feedwater train dynamics is modeled by a centrifugal feedwater pump for an incompressible single-phase liquid with constant loss coefficients and friction factors. The quasi-static momentum balance is used to derive the feedwater mass flow rate and an equation of conservation of angular momentum is employed to calculate the feedwater pump speed using an input moment of inertia for the feedwater pump/turbine assembly.

The feedwater preheater dynamics is modeled by a counter-current flow heat exchanger consisting of a drain cooler and a main cooler in series. The quasistatic energy balance in the heat exchanger gives rise to the overall temperature rise of the feedwater in the preheaters, which determines the feedwater temperature.

The condenser dynamics is modeled by an equilibrium mixture of vapor and liquid water at rest. Transient mass and energy balances along with the equation of state give rise to the state equations for the condenser pressure and mixture enthalpy. These equations are integrated in time to obtain the transient response of the condenser pressure and enthalpy.

2.6 Boron Circulation in the Vessel

The boron transport model in RAMONA-3B [1] is inadequate for accurate tracking of boron in the reactor core because of the very few nodes used for boron transport. There are only ten nodes used for the reactor pressure vessel (RPV) of which three are used for the core. Furthermore, the multiple core channels are lumped into a single channel for boron tracking in the core. The strong nuclear-thermal-hydraulic coupling in a SBWR, due to the natural circulation coolant flow, requires an accurate calculation of boron concentration in the multiple parallel channels of the core. To this end, a new detailed boron transport model has been implemented in the upgraded version RAMONA-4B.

For RAMONA-4B, the boron circulation in the vessel is modeled by a local transient boron transport equation, which is integrated in time in every hydraulic cell throughout the vessel including the multiple parallel coolant channels in the core. Furthermore, the boron flow reversal can also be calculated everywhere in the vessel. These features allow the code to

predict accurately the nonuniform boron dispersion in the vessel.

In order to account for the imperfect boron mixing with the liquid water (especially at the low-flow condition), three flow-dependent boron-mixing efficiency functions have been introduced to be associated with the boron flow for the up-flow, down-flow, and horizontal flow (at lower plenum), respectively. This feature makes it possible to predict the potential boron stratification that may occur in the lower plenum at very low flow rates (less than 5% of rated core flow).

2.7 Standby Liquid Control System (SLCS)

The Standby Liquid Control System of SBWR is a backup shutdown system to be used in case of the failure of normal scram system. The system consists of an accumulator tank maintained at a high pressure, a piping system with control logic, and a high-velocity core injection system.

In RAMONA-4B, this system has been modeled as an independent component. Momentum balance between the accumulator tank and the RPV injection port is used to determine the flow rate of boron solution from the tank. The initial conditions inside the tank are user specified, which include the cover-gas pressure, solution density, liquid level within the tank, and other geometric and initialization data. Polytropic expansion of the cover gas is assumed to determine the transient cover gas pressure in the momentum equation. The boron solution level, flow rate, and void fraction as a function of time are also calculated.

The transient boron flow rate is used as the boron injection rate to the boron transport model for calculating local boron concentrations, which in turn provide input to neutron kinetics for boron reactivity calculation. The SLCS can be activated either automatically or manually. The automatic SLCS actuation is initiated by high-pressure and low-level setpoints. Delays in the control logic and valve operation are taken into account in accordance with the actual system specification.

3. DEVELOPMENTAL ASSESSMENTS

3.1 Calculational Model

RAMONA-4B is a detailed best-estimate thermal-hydraulics computer code with 3D neutron kinetics, capable of modeling a full core with 800 neutronic channels and 200 thermal-hydraulic channels along with 24 axial cells. The hydraulic model is based on nonequilibrium drift-flux formulation for two-phase flow with provision for flow reversal [4]. The neutronic model is based on a well-established 1½-group diffusion theory [1]. The three-dimensional neutron kinetics is an important feature of the calculational model described below. RAMONA-4B has a separate section to generate a steady-state condition. This section uses the same formulation as the transient section.

The RAMONA-4B calculational model used in the present assessment is shown in Figure 1. It includes the reactor pressure vessel with all important internal components (reactor core,

upper plenum and riser, steam separator and dryer, steam dome, downcomer, lower plenum, and jet pumps) and the recirculation loops, steam lines and control systems. The reactor core is modeled with 101 neutronic channels and 25 thermal-hydraulic channels assuming eighth-core symmetry as shown in Figure 2. Twenty-four axial cells are used in each of the multiple core channels in order to obtain accurate axial power and void distributions.

The nuclear parameters for the 3D neutron kinetics correspond to Browns Ferry Unit 3, a typical BWR4. The cross sections and their feedback coefficients were generated to represent the end of cycle 5 (8766 MWD/MTU). The three-dimensional exposure and the history-dependent void distributions were taken into account using the auxiliary code BLEND [5] to produce 77 sets of cross sections and the corresponding feedback coefficients. These cross section sets have been used to predict both the radial and axial power distributions in very good agreement with the Browns Ferry-3 cycle-5 measurements [6].

3.2 SBWR Natural Circulation Steady State

As an assessment of the natural circulation steady-state capability for the SBWR, a null transient from hot-full-power conditions was run for 500 seconds to see if a steady state would hold in the long run. That this is indeed the case and is demonstrated in the null transient results in Figures 3 through 6 for the core flow, reactor power, system pressure, steam flow, and feedwater flow, respectively.

We conclude that the double-loop iteration algorithm described in Section 2.1 does work well for SBWR.

3.3 Isolation-Condenser Performance

The effectiveness of ICs will be measured by their influence on the frequency of operation of the Safety and Relief Valves (SRVs) for overpressure protection. In the SBWR, the Emergency Core Cooling System (ECCS) has been replaced by a passive system, eliminating the High Pressure Core Injection (HPCI) and Reactor Core Isolation Cooling (RCIC) systems. Thus, the reactor performance, with operating ICs, will be investigated in the absence of these components.

3.3.1 Transient Description

The transient considered here is an ATWS event initiated by the closure of all four MSIVs in four steam lines within 4 seconds with postulated scram failure. This will result in a sharp rise in the vessel pressure, which leads to a large power increase due to void collapse. The SRVs will open at their upper pressure setpoints and will close at their lower pressure setpoints. Thus, after the initial part of the transient, the cyclic operation of the SRVs will control the reactor pressure. Early shutdown of the incoming feedwater flow will cause a decrease in the collapsed water level, which will initiate the HPCI, at the low water level setpoint in the case of regular BWRs. The ICs will be activated by either a 10% closing of the MSIV or exceeding a pressure setpoint of 7.9 MPa.

A regular BWR operating without any isolation condenser has been used as the base case for comparison of the results. Several modifications in the input of the base case have created other significant cases of interest. Table 1 shows the test matrix used to investigate separate effects in each case. Cases 1 and 2 refer to a BWR operating without any IC and with one IC, respectively. Cases 3 and 4 refer to transients with 1 and 3 ICs operating without HPCI respectively. Lastly, cases 5 and 6 study the effect of isolation condenser on a natural circulation system achieved by removing the recirculation pump system. The last two cases refer to a regular BWR operating without any IC and with one IC but in the absence of HPCI.

Table 1. Test Matrix for MSIV Closure

Case No.	Number of ICs	HPCI	Recirc. Pump	Observation
1	0	Active	Active	Base Case
2	1	Active	Active	Effect of IC
3	1	Inactive	Active	Effect of HPCI
4	3	Inactive	Active	Effect of ICs
5	0	Active	Inactive	Natural Circulation
6	1	Active	Inactive	Effect of IC

3.3.2 Results and Discussions

The results will be separated into two parts. In the first part we focus on the forced-circulation system, while the second part is related to the natural circulation system.

Effects on Forced Circulation System

Figure 7(a), 7(b), 7(c) and 7(d) show the transient pressure response for cases 1 through 4, respectively. The MSIV closure results in a rapid increase of the RPV pressure to 8.9 MPa within the first 10 seconds. During this period all the SRV banks have reached their relief pressures, and therefore opened sequentially. Consequent release of steam has resulted in a decrease of reactor pressure after attaining the peak pressure of 8.9 MPa. This peak pressure has remained nearly the same for all four cases analyzed. A periodic behavior of the transient pressure can be observed following the initial peak. According to the SRV pressure setpoints, the SRV bank 3 is periodically opening and closing to produce this behavior. The SRV banks 1 and 2 are open for the entire period of the transient, while the valves in bank 4 has closed within the first 20 seconds.

The cyclic frequency of the SRV operation is reduced when an active isolation condenser is used in case 2, where one IC is operating in the presence of HPCI. However, the effect of

IC is reduced after 90 seconds, as seen from Figure 7 (a) and 7(b). This is due to the actuation of HPCI, as initiated by the low level in the vessel at 45 seconds. From Figure 8(a), we see that the HPCI supplies a constant flow of 369 kg/sec during the rest of the transient. Figure 8(b) shows the combined mass flow rate of the feedwater, HPCI flow, and the condensate flow returning from the IC. The feedwater flow reduces rapidly within the first 5 seconds, as a result of the extraction steam cutoff by the MSIV closure, which has been prescribed here as an input boundary condition. The condensate return from the IC depends on several factors, including the system pressure, IC pressure, IC cooling capacity, and the liquid levels inside the downcomer and IC [3]. The resulting flow of condensate is shown to fluctuate around 30 kg/sec.

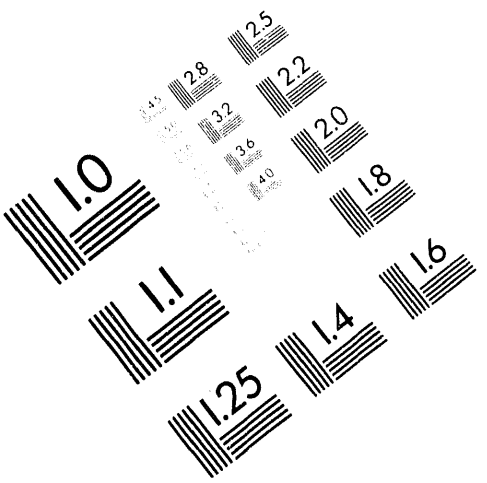
The external makeup water to the reactor vessel is largely dominated by the HPCI flow rate. Therefore, after the activation of the HPCI, the effect of the IC is negligible. According to Figure 8(b), there is no net inflow between 25 to 42 seconds. During this period, the IC activation conditions are satisfied, but the momentum balance between the IC and the condensate return port has prevented any down flow of the liquid. Figure 8(b) shows that the HPCI activation has been delayed by 20 seconds due to the operation of the IC. This delay was caused by the slower drop of the collapsed liquid level during the transient.

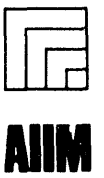
In the new design of SBWR, the ECCS systems are not available in the present form. In order to eliminate the effect of HPCI, cases 3 and 4 are presented, which include one and three active ICs respectively. According to Figures 8(c) and 8(d), the effect of removing the HPCI has resulted in much reduced cycling of the SRVs, although the system pressure is maintained within the same range. It is also observed that increasing the number of ICs has reduced the cycling frequency further.

The periodicity of the pressure behavior is directly related to the steam flow response shown in Figures 8(a) through 11. As a consequence of the pressure rise to 8.9 MPa in the first 5 seconds, there is a core wide collapse of voids. Because of the effect of negative void reactivity feedback, the core thermal power increased during the first 5 seconds. These processes reverse later when the system pressure is reduced, causing the void fraction to increase and resulting in a decrease in the core thermal power within 40 seconds. The periodic behavior during the transient is also evident from the void fraction and thermal power responses. Removal of the HPCI has resulted in much fewer peaks in Case 3 and 4. Therefore, the ICs are more effective in the absence of HPCI, which is the case of the SBWR design.

The effectiveness of the IC as a passive pressure regulating component has thus been demonstrated. The HPCI is initiated by the low collapsed liquid level of -1.485 meter below the entrance of the downcomer. The condensate return flow from the IC changed the transient response of the collapsed liquid level. As seen from Figures 8 and 9, the HPCI initiation by the low level setpoint has been delayed from 42 seconds to 62 seconds by the operating IC.

The condensate return to the reactor vessel from the IC is closely related to the system pressure. After the initial fluctuation in the early transient, the flow rate has stabilized at approximately 30 kg/sec. The periodicity of system pressure has resulted in fluctuation of the liquid return flow by 5 kg/sec.

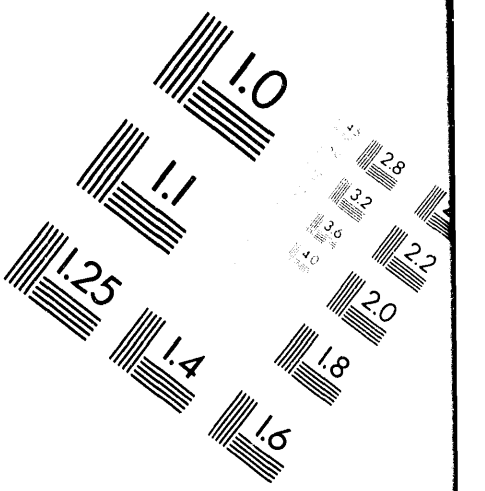


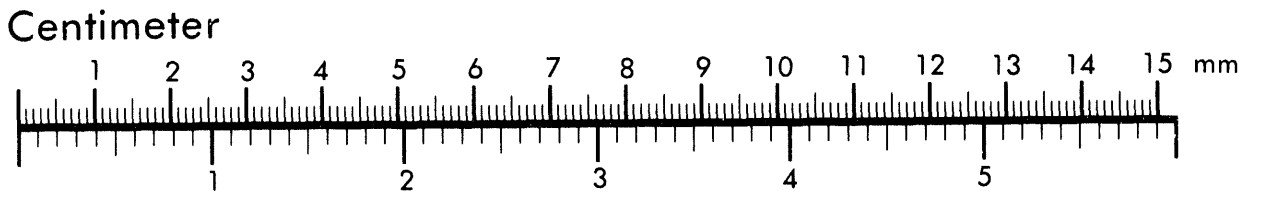


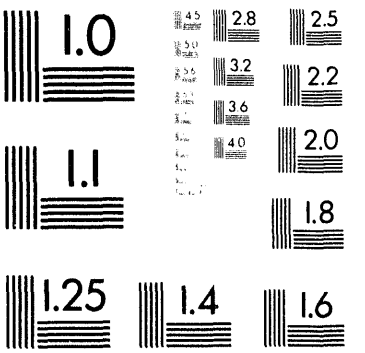
Association for Information and Image Management

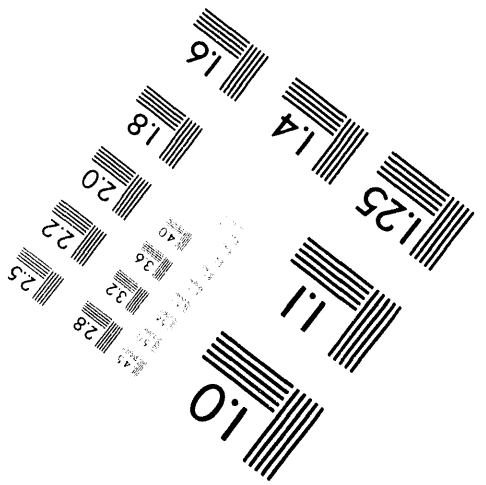
1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910

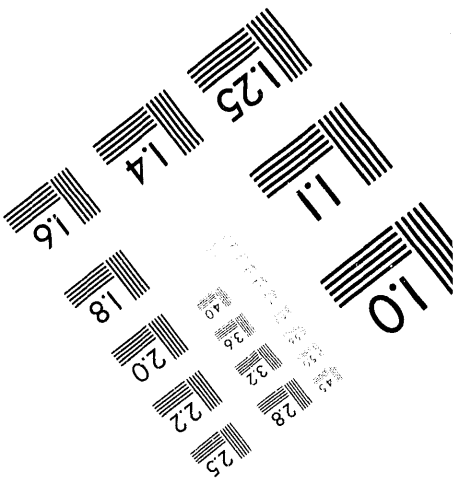
301/587-8202











MANUFACTURED TO AIIM STANDARDS
BY APPLIED IMAGE, INC.

7 of 7

Effects on Natural-Circulation System

The effects of ICs on the forced-circulation system of regular BWRs was presented in the previous section. The overall effect on a natural circulation system is quite similar to that on a forced circulation. Because of the inherent nature of the natural-circulation system, the response time is longer, which results in relatively smoother transient responses for Case 5 and 6. Figures 12(a) and 13(b) show the transient pressure responses for these cases with inactivated recirculation pumps.

The total reactor power for these cases has been reduced to 1600 MW, and the initial core flow rate is 800 kg/sec. The feedwater flow is given as a boundary condition, such that it shuts down in 3.5 seconds, while the HPCI activates on the low water level indicated earlier.

Because of the reduced power in the natural circulation system, the peak pressure observed in this transient is only 7.9 MPa, as compared to 8.9 MPa in the forced circulation cases. This peak pressure is below the operation set points for the SRVs in banks 2 and 4. Therefore, the total number of SRVs active in this natural circulation system is reduced by half. The periodic behavior of the pressure is due to the repeated opening and closing of SRV bank 3, while SRV bank 1 remains open throughout the transient. According to Figures 12 and 13, the cyclic frequency of operation for the SRVs has been reduced significantly by the use of one Isolation Condenser. The steam flow rate in the steam line also shows the periodic behavior. Figures 14 and 15 show the core thermal power during the transient. As compared to the forced circulation cases, the amplitude of oscillations during the first 40 seconds of the transient is higher. The presence of one IC has reduced the thermal fluctuations during the transient as shown in Figure 15.

3.3.3 Conclusions

The effectiveness of ICs as a pressure regulation system has been demonstrated. The cyclic frequency of opening and closing of the SRVs is reduced by the active use of the ICs. In the absence of the HPCI, the SRV operational frequency is further reduced. Hence, the effect of IC is minimal in the case of simultaneous operation of the IC and HPCI. The mass flow rate from HPCI dominates the transient response. This is an important observation for the SBWR since the effectiveness of the IC can not be fully realized in the presence of HPCI. The ECCS of the SBWR uses a passive system operating at low pressure, and high-pressure injection of liquid is prevented. Therefore, the benefit from the ICs as a pressure-regulating device is maximized in this configuration.

In the case of a natural circulation system, simulating a SBWR configuration, the effectiveness of the IC as a pressure-regulating device has also been demonstrated. In this case, the amplitude of pressure oscillations is similar to that for the forced-circulation system, although the initial peak pressure is reduced owing to the lower core thermal power of the natural circulation system. Therefore, the total number of operating SRVs is fewer than for the forced-flow case. The oscillations noted in the transient thermal power are of higher amplitudes than the previous cases. The effect of the IC is to reduce such amplitudes. The response time in the natural-circulation system is, in general, longer than that for the forced-circulation system.

Therefore, the transient events are expected to develop over a more extended time period.

3.4 Instability Due To Recirculation Pump Trip with BOP

To assess the capability of RAMONA-4B to predict thermal-hydraulic instability, a dual-recirculation-pump-trip event was simulated for a BWR4.

3.4.1 Event Description

The scenario selected for the present analysis is a two-recirculation-pump trip initiated from 100% core power and 75% core flow on the Maximum Extended Operating Domain (MEOD) rod line with postulated scram failure (ATWS) as described in Reference 3. This selection was based on the fact that a significant fraction of BWR instability events have resulted from an inadvertent recirculation pump trip (RPT).

The ATWS event initiated from the high-power and low-flow condition by inadvertent trip of both recirculation pumps is ideal for studying the density-wave oscillation characteristics because the dual RPT results in core flow reduction to natural circulation and a corresponding decrease in core power owing to increased vapor generation. This event takes the reactor into the region of power/flow map, which is more susceptible to instability as illustrated in Figure 16. Table 2 summarizes the sequence of events for the dual RPT event as calculated by RAMONA-4B.

Table 2

Sequence of Events for Two-Recirculation-Pump-Trip Event

Time (s)	Event/Action
0.0	Reactor operating at 100% power and 75% flow, both recirculation pump trip, and scram system fails.
30.0	Core flow coasts down to natural circulation, core power decreases to about 48% of rated.
50.0	Density-wave oscillations begin, core flow and core power start to oscillate.
80.0	Core power oscillation reaches limit cycle with peaks of about 150% of rated.
146.0	Core power reaches a maximum of 265% of rated.
200.0	Transient terminated.

The thermal-hydraulic inputs for the present analysis were selected to be similar to the LaSalle-2 instability event [7] of March 9, 1988. However, the initial condition is more bounding at 100% power and 75% flow than that of the LaSalle-2 event (85% power and 75% flow). This initial condition is more susceptible to density wave oscillations, and produced a critical reactor with a bottom-peaked axial power distribution as shown in Figure 17.

Feedwater flow and temperature were imposed as time-dependent boundary conditions. The time-dependent behavior of feedwater flow was taken from the TRACG analysis [8], and that of feedwater temperature was selected in such a way as to match the TRACG calculated core inlet subcooling as close as possible. The time-dependent boundary conditions of the feedwater flow and temperature are presented in Figures 18 and 19, respectively.

3.4.2 Results of Calculations

The event begins with a trip of both recirculation pumps at time zero. The RPT reduces the core flow to natural circulation (about 29% of rated) within 30 seconds as shown in Figure 20. As a result, core power is reduced from its initial rated value to approximately 50% of rated value due to increased vapor generation as shown in Figure 21. The evidence of instability is visible within one minute of the RPT event in the oscillatory behavior of both core flow and core power when the core inlet subcooling has increased beyond 18 °C as shown in Figure 22. The oscillations reached a limit cycle after approximately 80 seconds. Figure 23 presents the oscillatory behavior of core average void fraction, which demonstrates clearly that this is a density-wave oscillation.

The large-amplitude oscillations are often characterized by flow reversal in some coolant channels as is evident in the reversed flow behavior in channel 11 in Figure 24.

The system pressure response and steam flow behavior are shown in Figures 25 and 26, respectively. Because of the rapid reduction of feedwater flow at the beginning of the transient, the system pressure decreases initially and settles at about 6.75 MPa after 20 seconds. The oscillation also appears in both the system pressure and steam flow rate response through the vapor generation.

Figures 27 and 28 show the inlet and outlet flow rates for two hydraulic channels, 17 and 23. These channels represent a single rod bundle. Channel 17 is a low-power channel as it is in the vicinity of a control rod. The inlet and outlet flow rates for this channel are in phase indicating that channel is in stable mode. The high-power channel 23, on the other hand, has inlet and outlet flow rates out-of-phase and, therefore, is in an unstable mode. The parallel-channel phenomena are more evident from Figure 29 which shows that the inlet flow rates for these two channels are out of phase. These results indicate that there are out-of-phase flow oscillations taking place in the reactor core.

3.4.3 Discussion of Results

The limit-cycle oscillations in core flow and core power as calculated by RAMONA-4B exhibit the same characteristics as those calculated by TRACG [8]. However, TRACG predicts higher amplitudes than RAMONA-4B owing to different neutronic conditions and core inlet subcooling. These differences can be deduced from the reactor condition at the time of natural circulation prior to the initiation of the instability as shown in Table 3.

Table 3

Comparison of RAMONA-4B and TRACG Results before the Instability

Item	Time	RAMONA-4B	TRACG
Initial Axial Power Peaking	0 s	1.26	1.34
Core Flow	40 s	29%	30%
Core Power	40 s	50%	60%
Inlet Subcooling	40 s	13 °C	13 °C

The amplitude of the oscillations strongly depends upon the core inlet subcooling. The higher the core inlet subcooling, the stronger is the reactivity feedback. The core inlet subcooling is controlled by the feedwater temperature. The feedwater temperature during the transient was not available from the TRACG report [8]. However, in our calculations, the feedwater temperature was entered as a time-dependent boundary condition and an attempt was made to match the core inlet subcooling with the TRACG prediction as closely as possible. RAMONA-4B predicted an increase in the amplitude of the reactor power with the increase in the subcooling until the feedwater temperature and the core inlet subcooling stabilized.

During the limit-cycle oscillations, TRACG predicted a maximum amplitude of the core power of 400% (See Figure 30, taken from Ref. 8), while RAMONA-4B predicted a maximum amplitude of 265% (See Figure 18). This difference in the amplitude is generally due to the differences in core inlet subcooling, axial power profile and reactivity feedback; especially void feedback. In order to eliminate the effect of core inlet subcooling, the amplitudes from the two calculations were compared at the same inlet subcooling. TRACG predicted a subcooling of 20°C at 110 seconds and the relative power at this time was 160% as shown in Figure 30. RAMONA-4B predicted 20°C subcooling at 100 seconds and the relative power at this time was 155% as shown in Figure 21. Therefore, it is concluded that the differences in the two calculations are due to the parameters in core model such as axial profile and reactivity feedback.

The initial axial power distribution calculated by TRACG is more bottom peaked (1.34) than that by RAMONA-4B (1.26) because of the difference in the initial core conditions. In

general, a more bottom-peaked power shape will produce a higher amplitude of oscillations.

The void coefficients of cross-section sets used by TRACG are probably more negative than those used by RAMONA-4B. This is confirmed from a comparison of relative powers predicted by two codes at 40 seconds as shown in Table 3. While the flow rates and core inlet subcooling are the same, the TRACG predicted higher power than RAMONA-4B. This comparison indicates that the reactivity feedback were higher in the TRACG calculation than in the RAMONA-4B calculation. The TRACG calculation was intended as a bounding calculation to envelope GE's fleet of different BWRs. In RAMONA-4B calculation, we determined the overall void reactivity coefficient by perturbing the void profile alone from two separate steady-state calculations. The estimated void reactivity coefficient for the core used in the present analysis is -0.00055 $\delta k/k/\%$void, or -10¢/%void with an effective delayed-neutron fraction of 0.00546.

Figure 31 shows the maximum clad temperature in the core. The hot spot does exceed 1200 °C at 140 seconds. There is a possibility of clad damage at the hot spot in the core.

There are significant differences in the nodalization detail of the core between the RAMONA-4B and TRACG calculations. RAMONA-4B used 25 thermal-hydraulic channels, while TRACG used only 10 coolant channels. However, TRACG used 40 cells for each channel, placing many more cells between the bottom of the core and the first spacer grid; whereas RAMONA-4B used 24 cells with equal spacing. The effect of such different nodalization schemes is difficult to assess, and can only be resolved by a sensitivity study.

3.4.4 Summary and Conclusions

A two-recirculation-pump-trip event as defined by General Electric for their TRACG calculations has been used to assess the RAMONA-4B capability for predicting the density-wave oscillation induced by thermal-hydraulic instabilities in a BWR. The RAMONA-4B results were similar to those from TRACG calculations.

The results led us to conclude that a high-power and low-flow initial condition will most likely lead to core-wide density-wave oscillations after tripping both recirculation pumps, and that the RAMONA-4B is capable of predicting thermal-hydraulically-induced instabilities in a BWR. Furthermore, as the instability occurred during the natural-circulation mode, the calculation demonstrated the capability of RAMONA-4B code to model the SBWR.

The analysis also indicated that there is a possibility that in some of the nodes in the core, the clad temperature will exceed 1200 °C and will probably lead to some clad damage.

3.5 Loss-of-Feedwater Heating ATWS with FMCRD

3.5.1 Transient Description

The transient selected for this assessment is an ATWS event induced by the loss-of-feedwater heating together with the failure of the normal scram system. The loss-of-feedwater

heating can be caused by either of the two ways: (1) the steam extraction line to the heater is closed, and (2) feedwater is bypassed around the heaters. The total number of unavailable feedwater heaters determines the net loss of heating. In the SBWR the maximum reduction in feedwater temperature is limited to 55.6 °C. The loss of feedwater heating will result in an increase in core inlet subcooling. This will lead to an increase in the reactor power due to the negative void reactivity feedback in the core. The thermal power increases slightly to a new equilibrium value. This transient does not activate any ATWS logic. In order to investigate the effectiveness of the new SBWR feature, fine motion control rod drive (FMCRD) run-in, it is assumed that the FMCRD run-in will be initiated manually after the loss-of-feedwater heating.

The geometric data and the setpoints are specified in accordance with the conceptual design of the GE SBWR. The core represents a regular BWR core with the Browns Ferry Unit 3 cross sections at the end of cycle 5.

3.5.2 Results of Calculations

A feedwater temperature reduction of 55.6°C was initiated at 5 seconds into the transient. As a result, the reactor condition settled to a new steady state after 75 seconds. The temperature reduction of 55.6 °C is conservative since a temperature drop of 16.7 °C indicated by the Feedwater Control System (FWCS) requires the operator to send a signal to the Selected Control Rod Run- In (SCRRI), in order to reduce core power and thereby avoid scram. The loss-of-feedwater heating transient is a slow one which can be assumed to be in quasisteady state. The normal scram system was assumed to have failed during this transient.

The loss-of-feedwater heating transient is followed by the FMCRD run in at 80 seconds, which allows slow insertion of the control rods. The reactor is able to establish a quasisteady axial power shape, and the peak cladding temperature remains within the safety limits.

The results obtained from RAMONA-4B are compared to the TRACG results as reported by GE in the SSAR. The rate of power rise in the core as predicted by RAMONA-4B is higher than that of TRACG, while the system pressure remains constant for both calculations. Figure 32 shows the transient pressure response of RAMONA-4B, where the pressure is unchanged up to 75 seconds. The loss-of-feedwater heating has resulted in an increase of the core inlet subcooling as shown in Figure 33. The inlet subcooling changed from 10.1 to 17.5 °C as shown in Figure 33. Figure 34 shows that the reactor power is raised by 13% within 80 seconds due to the increased inlet subcooling. Figure 35 indicates that the FMCRD insertion begins at 80 seconds and continues until 180 seconds for full insertion. The slow insertion of control rods results in a quasisteady power profile, which is skewed to the top of the core. Figure 32 shows that the steam flow rate has decreased to 7.5% of the rated value within 100 seconds. The pressure also reaches a new equilibrium value within 100 seconds. The time required to reach the new equilibrium is 100 seconds for RAMONA-4B, while it is 60 seconds for TRACG. The feedwater flow was shut down within 10 seconds of the FMCRD initiation, which was imposed as a boundary condition to the calculation. The hottest channel fuel temperature is within the safety limit. The peak cladding temperature was found to be limited to 296°C.

4. CONCLUSIONS

RAMONA-4B code has been upgraded to include the balance of plant and control systems along with components specific to SBWR. The code has also been made operational on workstations. This code is now available to investigate stability issues not only for the current BWRs but also for ABWR and SBWR. RAMONA-4B can also be used for reactivity transients such as a rod-drop accident as well as ATWS events.

ACKNOWLEDGEMENT

This research was performed under the auspices of the U.S. Nuclear Regulatory Commission.

5. REFERENCES

[1] W. Wulff, H. S. Cheng, D. J. Diamond, and M. Khatib-Rahbar, "A Description and Assessment of RAMONA-3B MOD.0 CYCLE 4: A Computer Code with Three-Dimensional Neutron Kinetics for BWR System Transients," NUREG/CR-3664, Brookhaven National Laboratory, Upton, New York (1984).

[2] B. S. Shiralkar, M. Alamgir, and G. M. Andersen, "Thermal Hydraulic Aspects of the SBWR Design."

[3] H. J. Khan and U. S. Rohatgi,"Performance Characterization of an Isolation Condenser of SBWR," Thermal Hydraulics Proceeding for 1992 Winter Annual Meeting of the American Nuclear Society, Chicago. Also in Vol 66, TANSAO 66 1-626 (1992).

[4] W. Wulff, H. S. Cheng, A. N. Mallen, and S. V. Lekach, "The BNL Plant Analyzer," NUREG/CR-3943, BNL-NUREG-51812, Brookhaven National Laboratory, Upton, New York (1984).

[5] L. O. Eisenhart and D. J. Diamond, "Automatic Generation of Cross Section Input for BWR Spatial Dynamics Calculations, "BNL-NUREG-28796, Brookhaven National Laboratory, (1980).

[6] J. F. Carew, D. M. Cokinos, J. G. Guppy, K. Hu, and L. Y. Neymotin, "RAMONA-3B Calculations of BWR Core-Wide and Regional Power/Flow Oscillations," Internal Memo, Brookhaven National Laboratory, December 12 (1988).

[7] W. Wulff, H. S. Cheng, A. N. Mallen, and U. S. Rohatgi, "BWR Stability Analysis with the BNL Engineering Plant Analyzer," NUREG/CR-5816, BNL-NUREG-52312, Brookhaven National Laboratory, October (1992).

[8] "ATWS Rule Issues Relative to BWR Core Thermal-Hydraulic Stability", NEDO-32047, General Electric Co., February (1992).

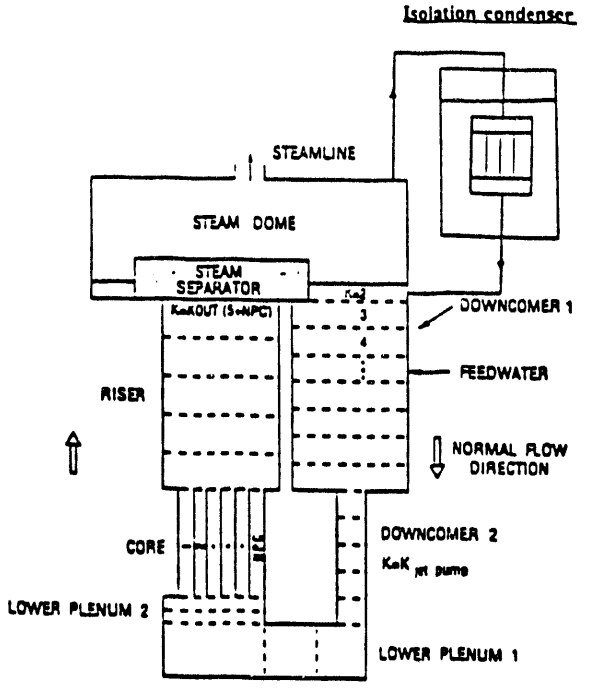


Figure 1. RAMONA-4B Nodalization

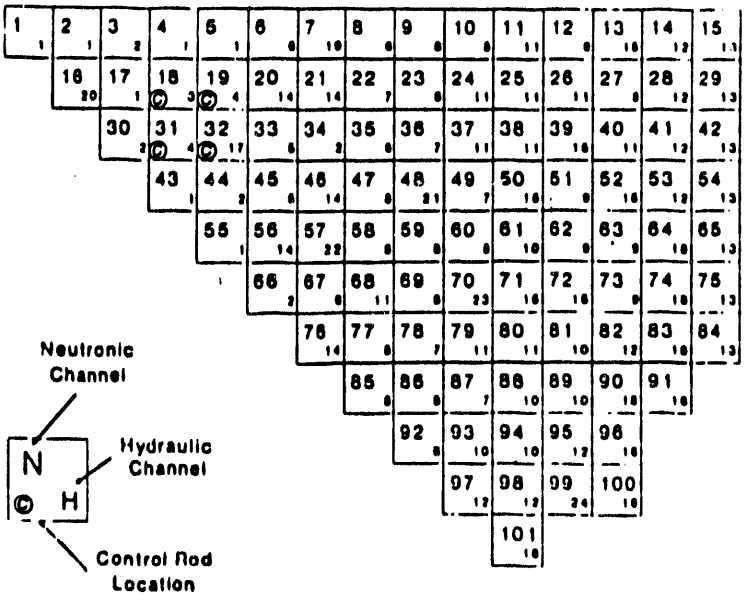


Figure 2. 1/8 Core Model for the Present Analysis

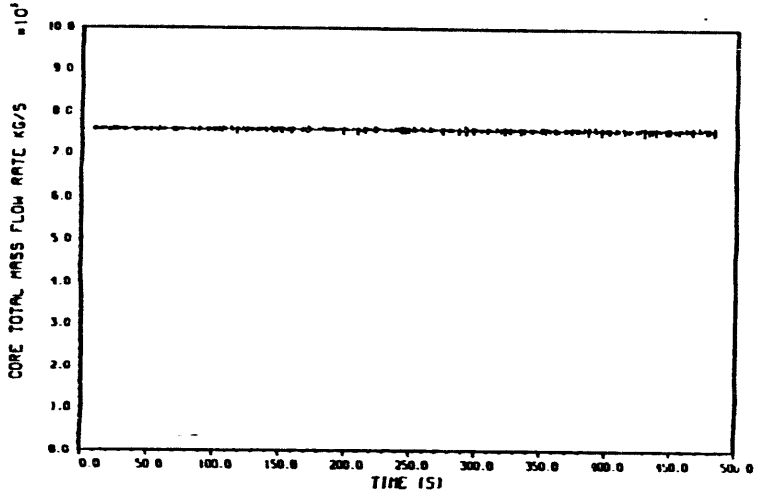


Figure 3. Core Flow Response of the Null Transient.

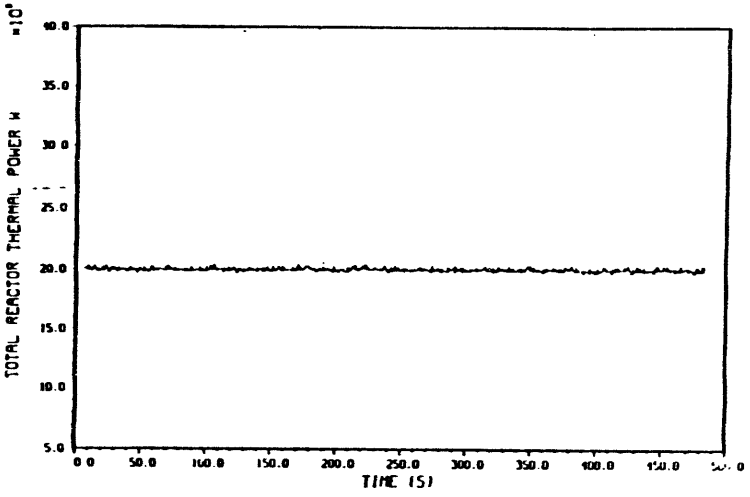


Figure 4. Core Thermal Power Response of the Null Transient.

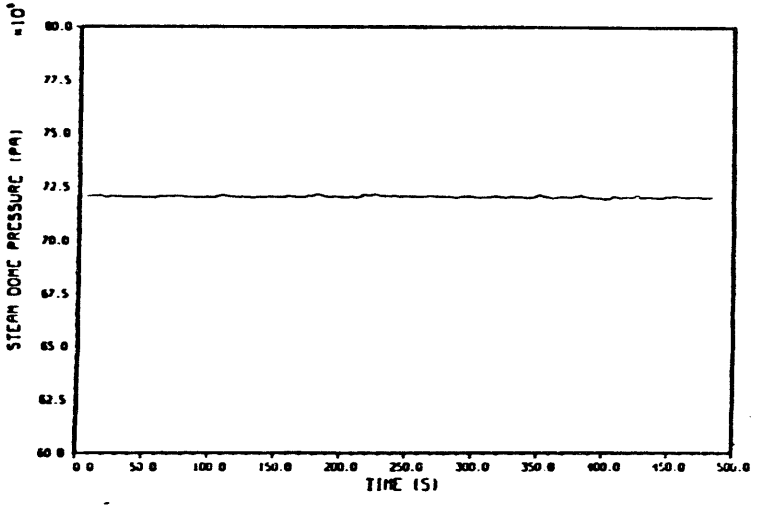


Figure 5. System Pressure Response of the Null Transient.

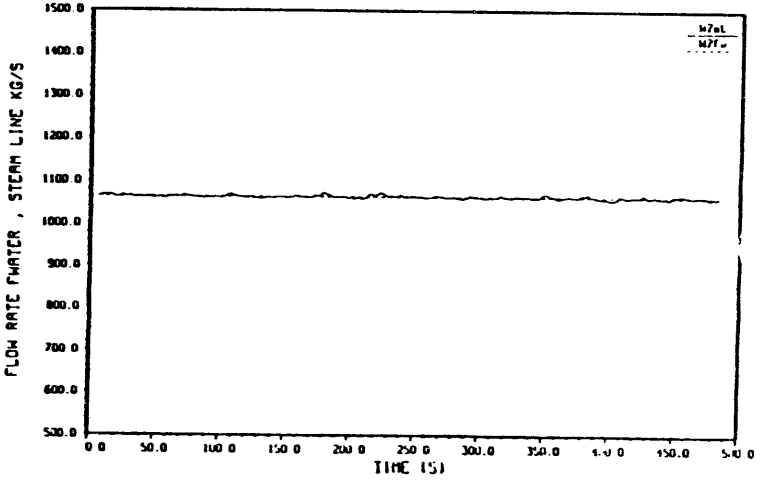


Figure 6. Feedwater and Steam Flow Response of the Null Transient.

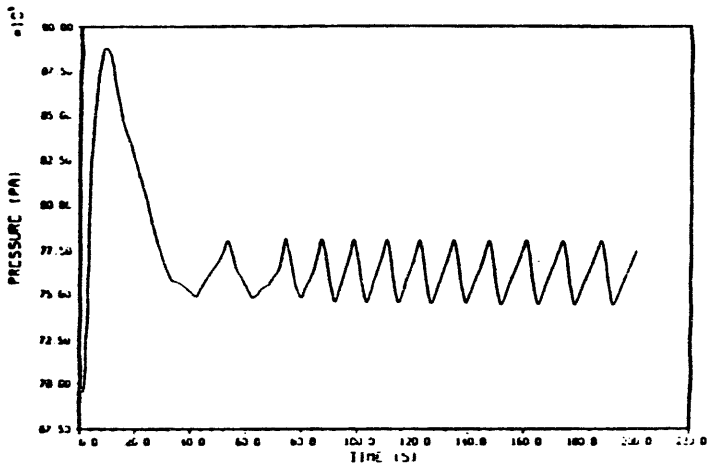


Figure 7(a) Transient Pressure Profile for case 1

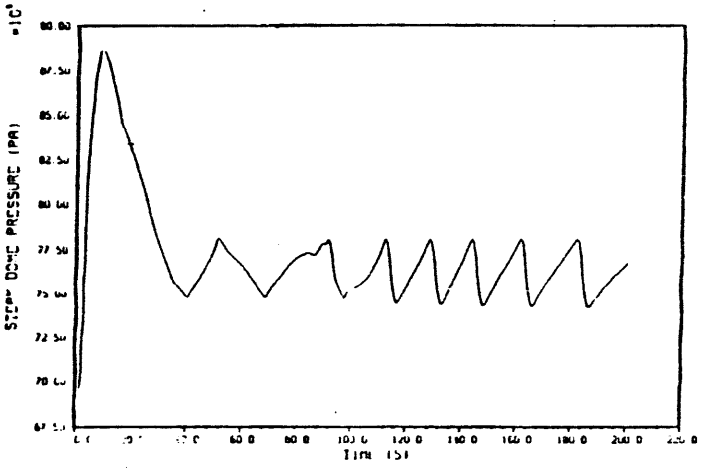


Figure 7(b) Transient Pressure Profile for case 2

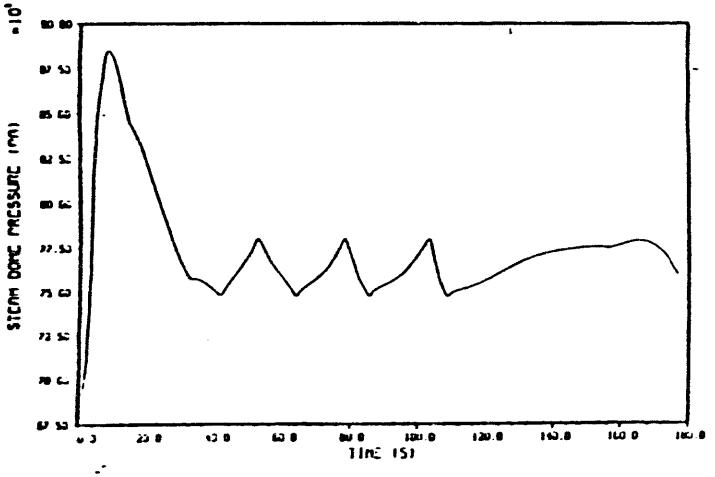


Figure 7(c) Transient Pressure Profile for case 3

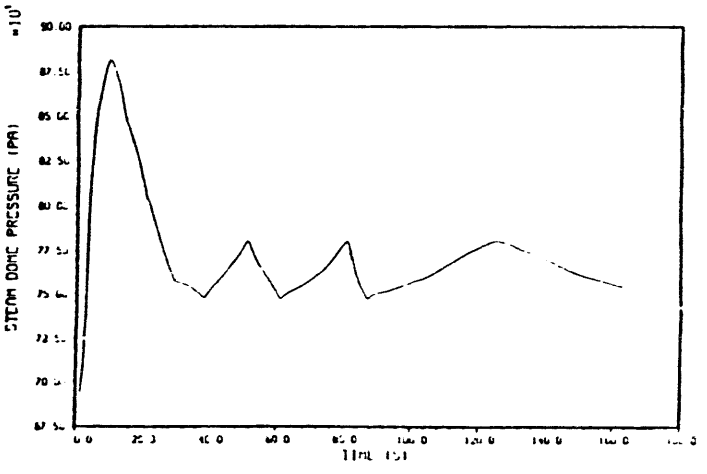


Figure 7(d) Transient Pressure Profile for case 4

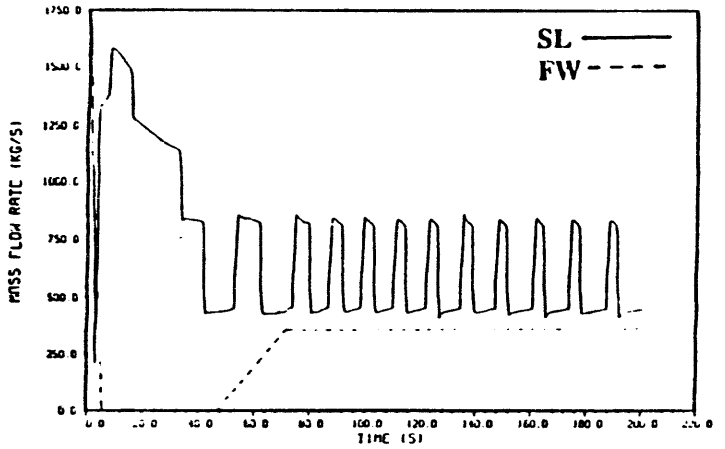


Figure 8 Steam & Feed Water Flow Rate for case 1

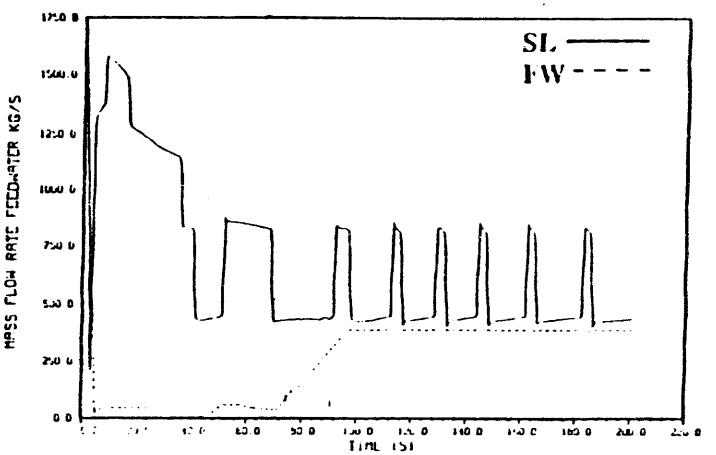


Figure 9 Steam & Feed Water Flow Rate for case 2

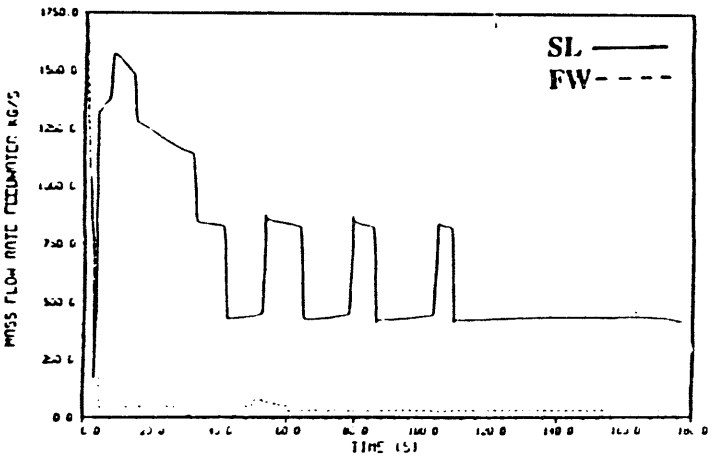


Figure 10 Steam & Feed Water Flow Rate for case 3

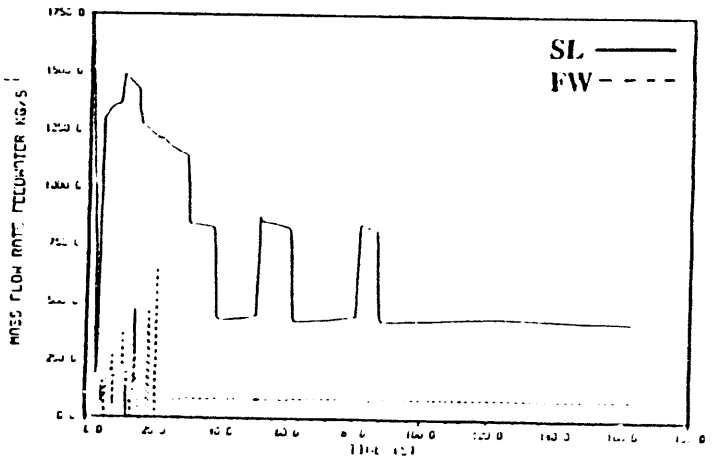


Figure 11 Steam & Feed Water Flow Rate for case 4

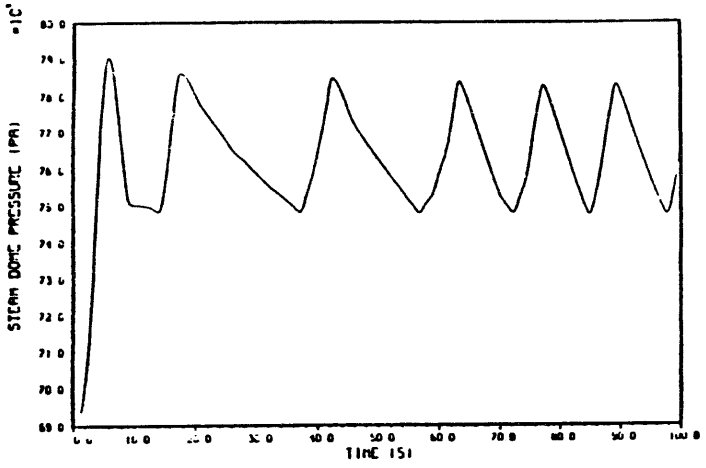


Figure 12 Transient Pressure Profile for Natural Convection Without Isolation Condenser (case 5)

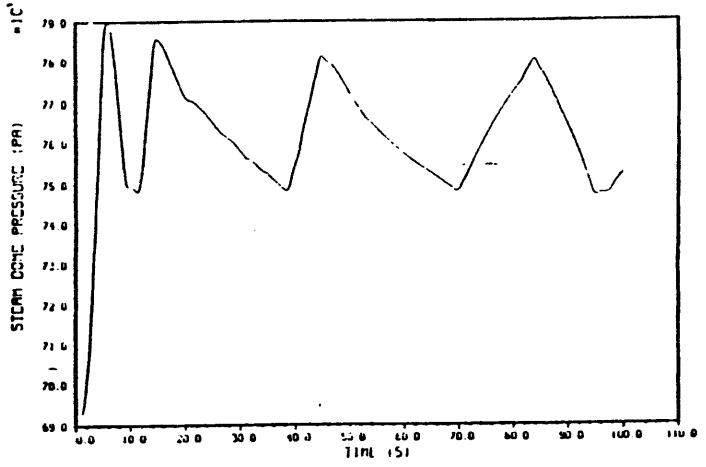


Figure 13 Transient Pressure Profile for Natural Convection With Isolation Condenser (case 6)

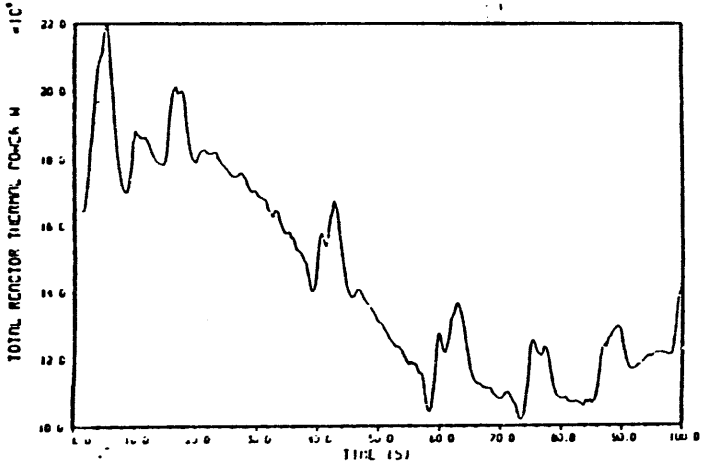


Figure 14 Thermal Power Profile for Natural Convection (case 5)

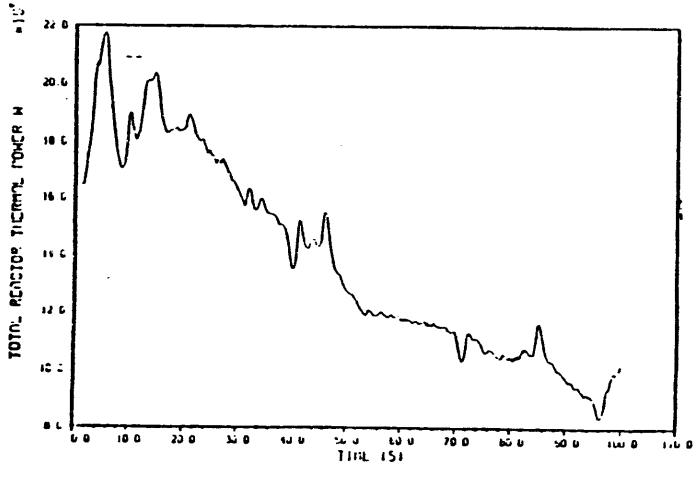


Figure 15 Thermal Power Profile for Natural Convection (case 6)

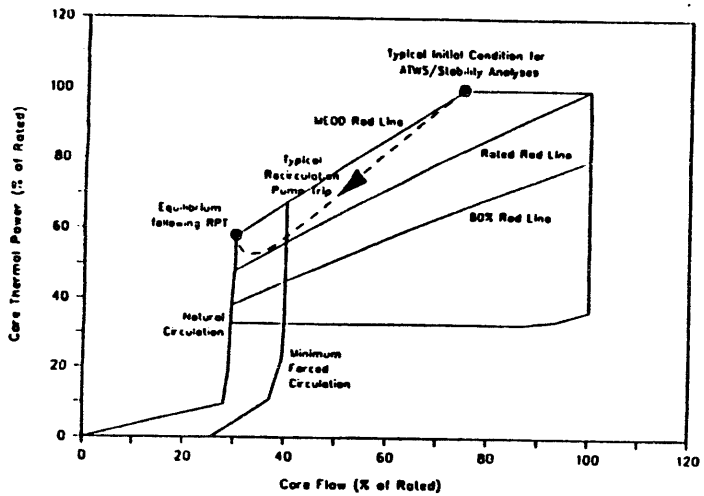


Figure 16. Typical Core Power/Flow Map of a BWR.

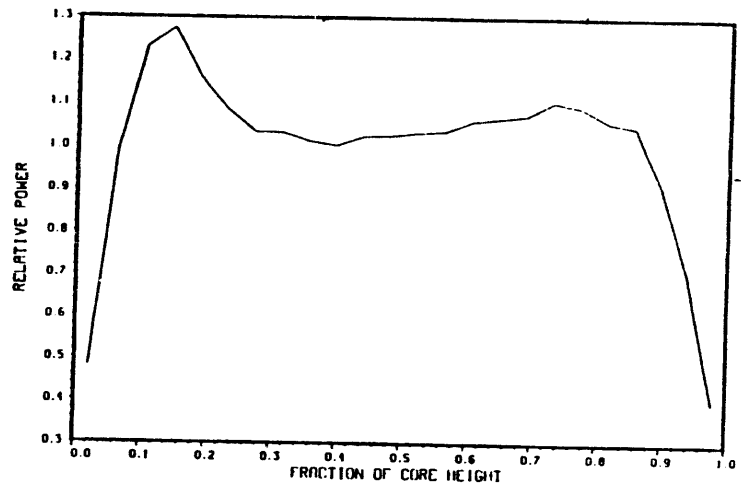


Figure 17. Initial Core Average Axial Power Profile.

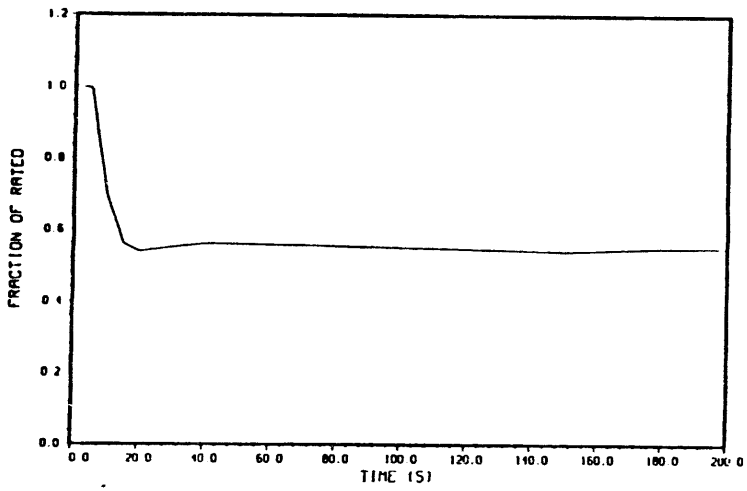


Figure 18. Feedwater Flow Boundary Condition.

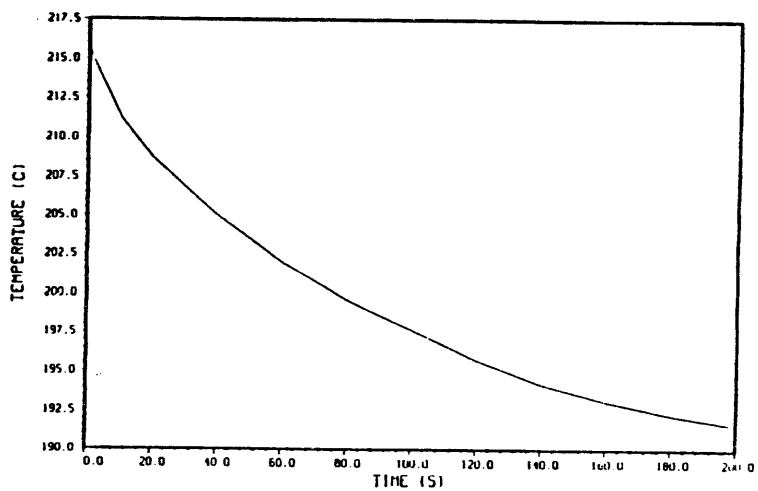


Figure 19. Feedwater Temperature Boundary Condition.

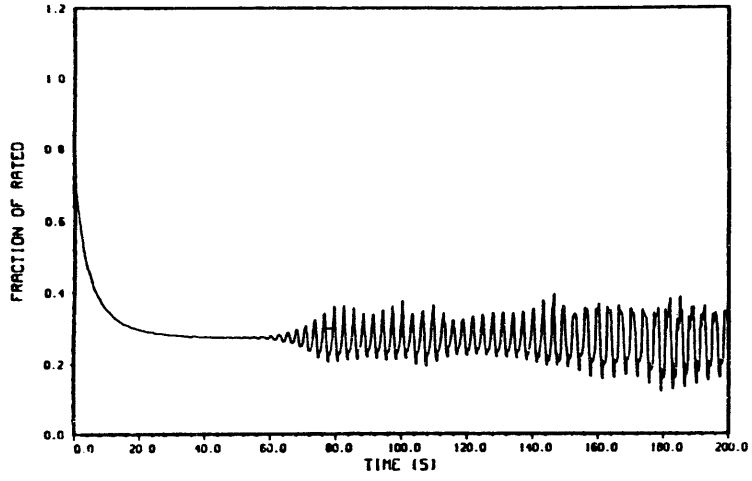


Figure 20. Total Core Inlet Flow Response During the RPT.

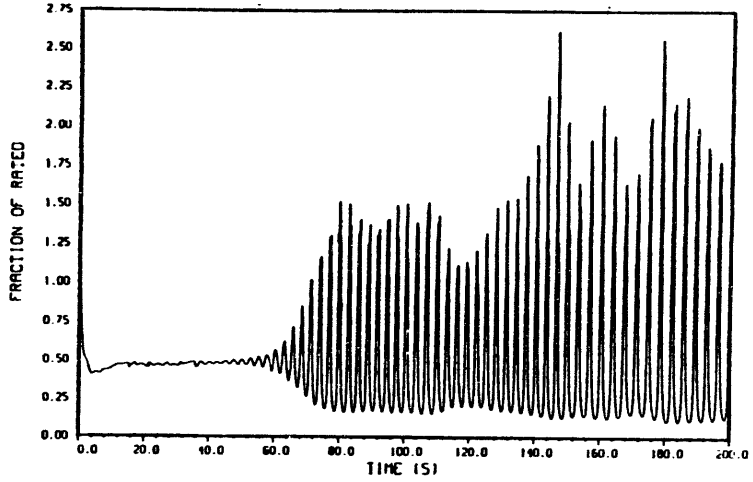


Figure 21. Core Power Response During the RPT.

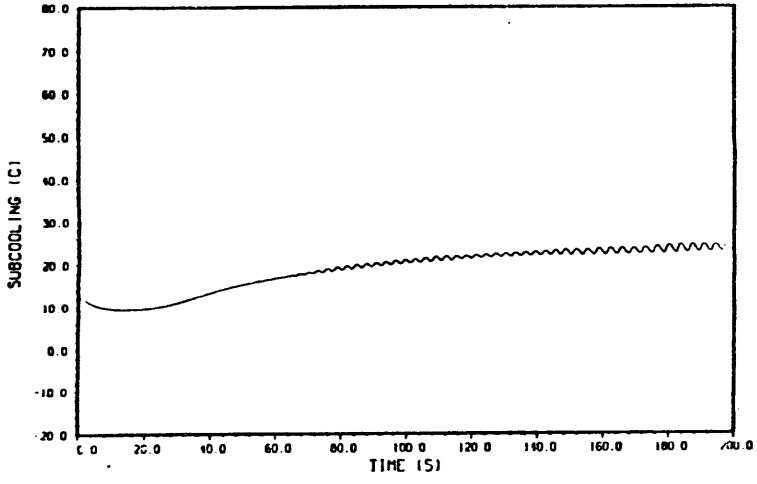


Figure 22. Core Inlet Subcooling During the RPT.

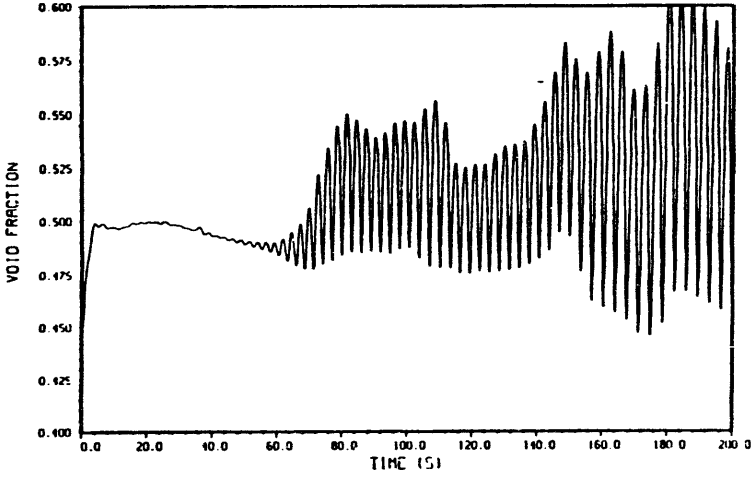


Figure 23. Core Average Void Fraction Response During the RPT.

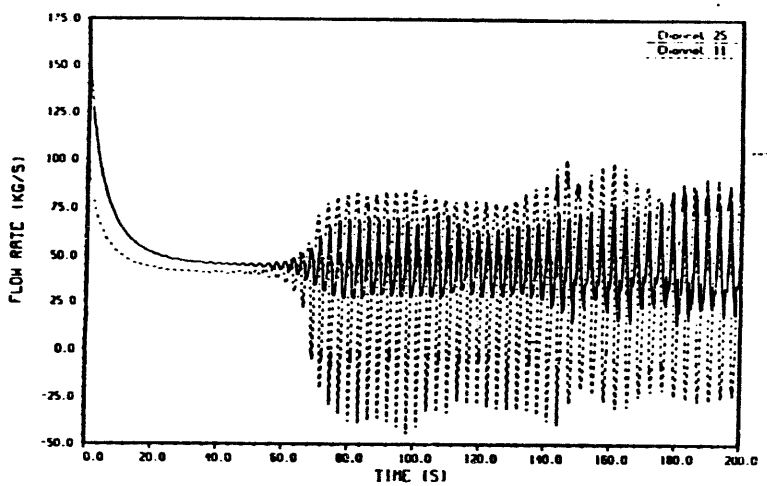


Figure 24. Individual Channel Flow Response During the RPT.

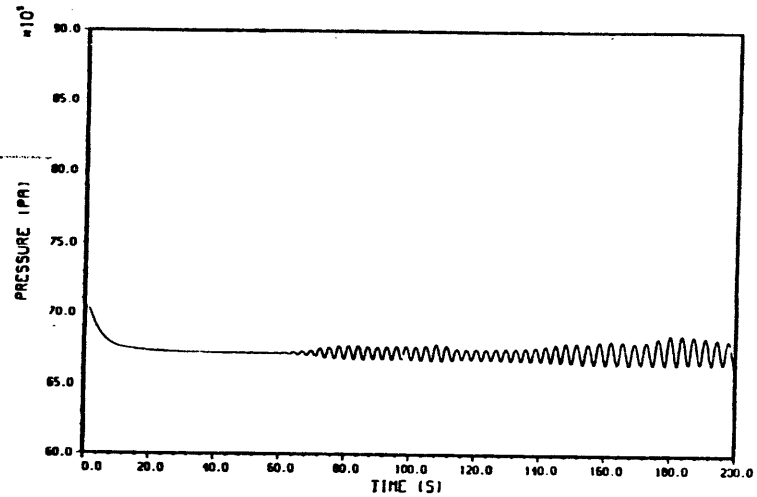


Figure 25. System Pressure Response During the RPT.

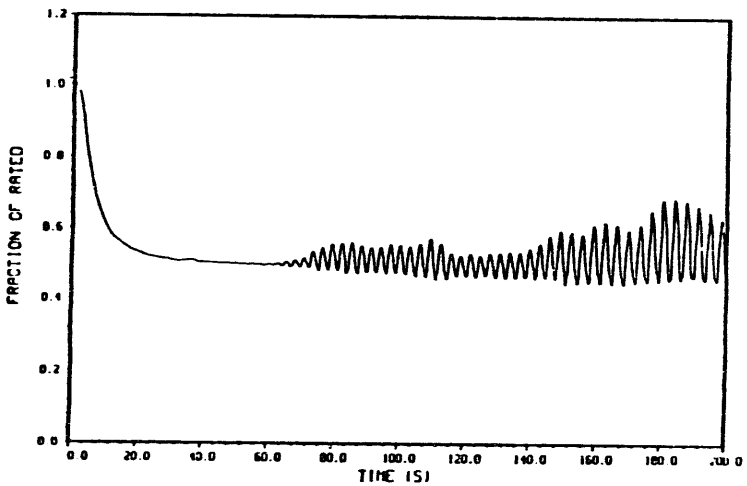


Figure 26. Steam Flow Response During the RPT.

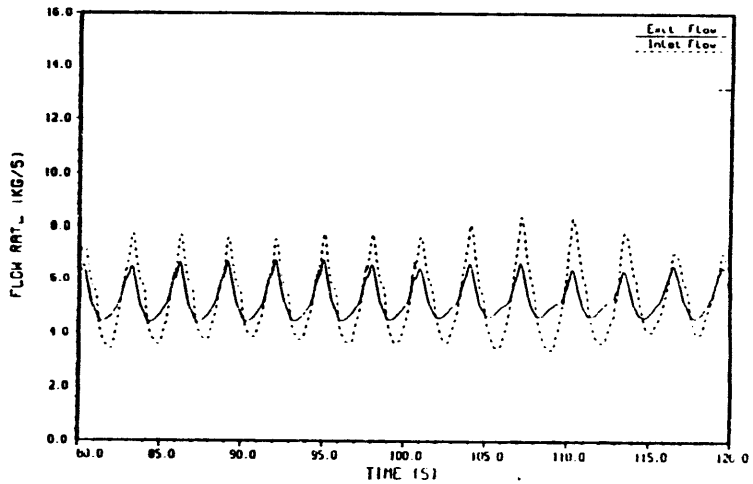


Figure 27. Channel 17, Inlet and Exit Mass Flow Rates.

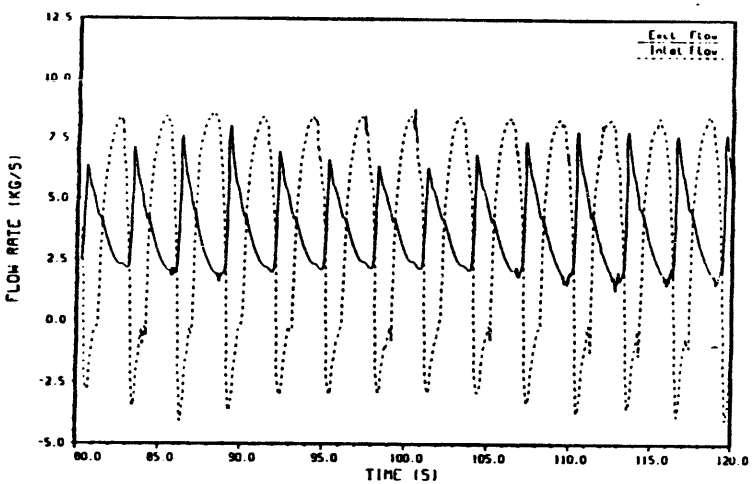


Figure 28. Channel 23, Inlet and Exit Mass Flow Rates.

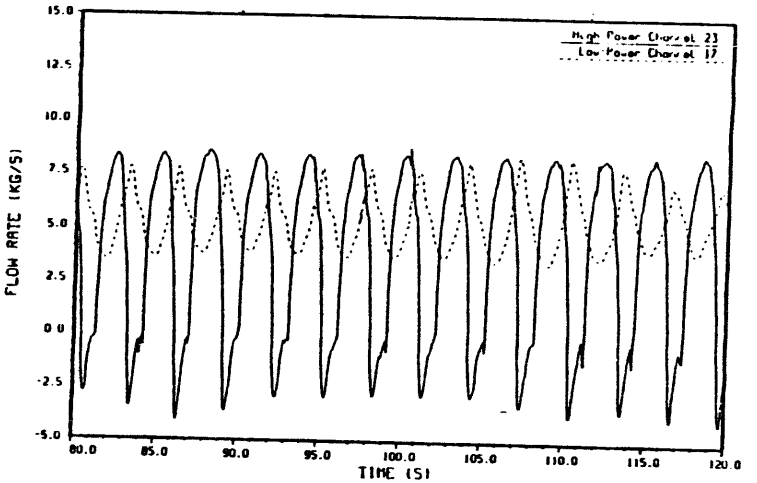


Figure 29. Inlet Flow Rates for Channel 17 and 23.

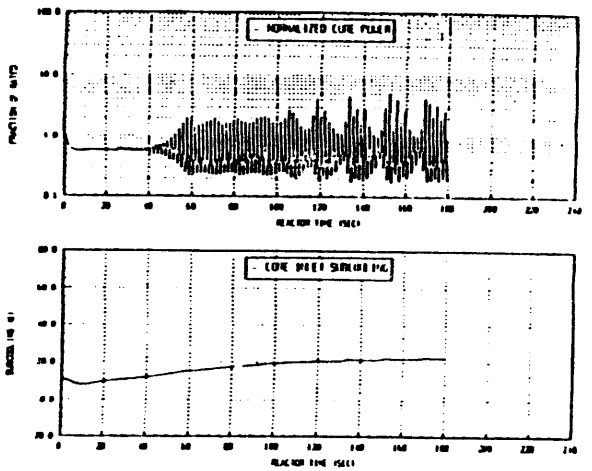


Figure 30. TRACG Results - Core Power and Inlet Subcooling.

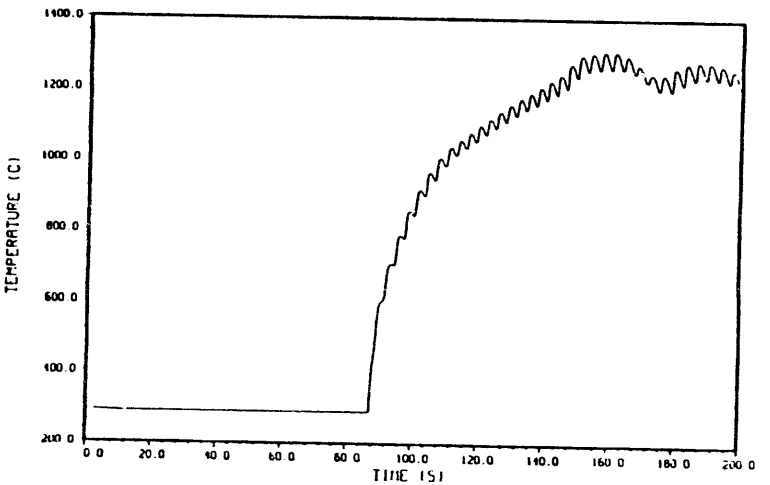


Figure 31. Peak Clad Temperature During the RPT.

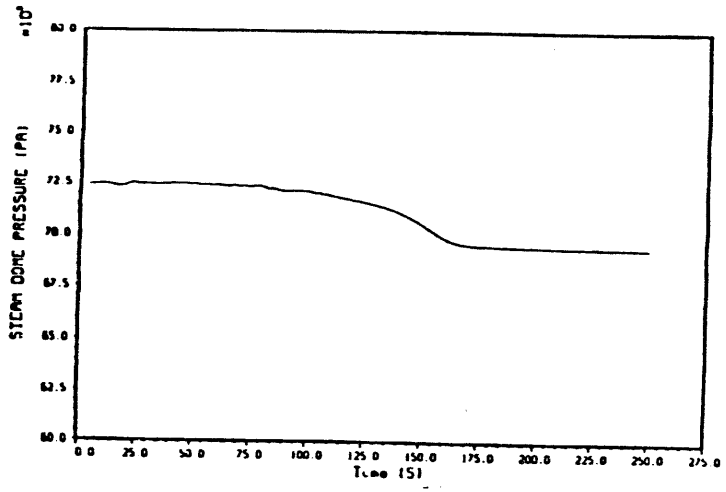


Figure 32. Pressure Profile for Loss of Feed Water Heating ATWS with Fine Motion Control Rod Insertion

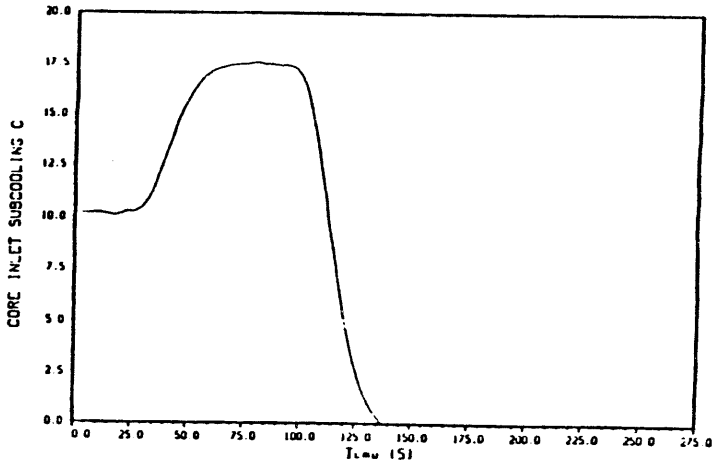


Figure 33. Inlet Subcooling for Loss of Feed Water Heating ATWS with Fine Motion Control Rod Insertion

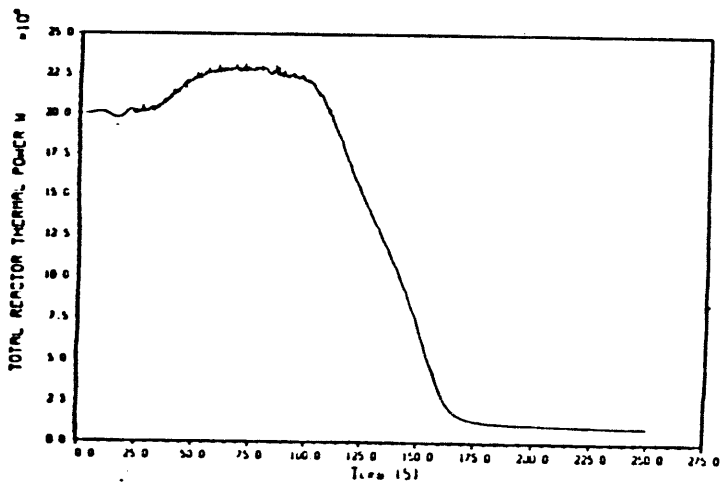


Fig. 34. Thermal Power during Loss of Feed Water Heating ATWS with Fine Motion Control Rod Insertion

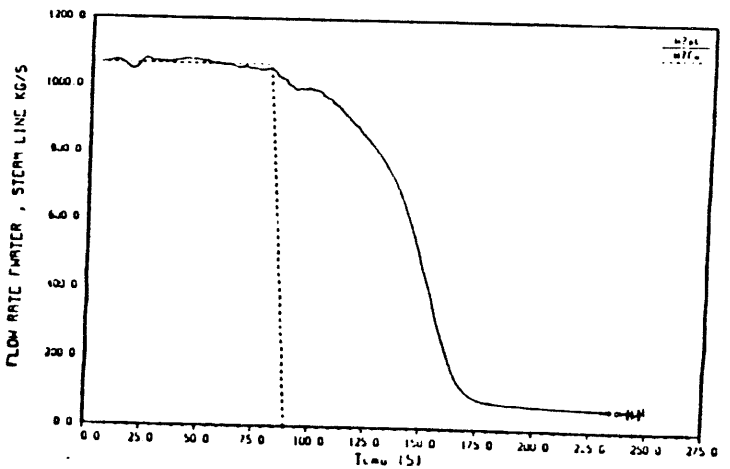


Figure 35. Feed Water and Steam Flow during Loss of Feed Water Heating ATWS with Fine Motion Control Rod Insertion

NRC FORM 335 (2-89) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER (Assigned by NRC. Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG/CP-0133

Vol. 1

2. TITLE AND SUBTITLE

Proceedings of the Twenty-First Water Reactor Safety Information Meeting
Plenary Session; Advanced Reactor Research; Advanced Control System Technology; Advanced Instrumentation & Control Hardware; Human Factors Research; Probabilistic Risk Assessment Topics; Thermal Hydraulics; Thermal Hydraulic Research for Advanced Passive LWRs

3. DATE REPORT PUBLISHED

MONTH	YEAR
April	1994

4. FIN OR GRANT NUMBER

A3988

5. AUTHOR(S)

Compiled by Susan Monteleoné, BNL

6. TYPE OF REPORT

Conference Proceedings

7. PERIOD COVERED *(Inclusive Dates)*

October 25-27, 1993

8. PERFORMING ORGANIZATION – NAME AND ADDRESS *(If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)*

Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington DC 20555-0001

9. SPONSORING ORGANIZATION – NAME AND ADDRESS *(If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)*

Same as Item 8 above

10. SUPPLEMENTARY NOTES

Proceedings prepared by Brookhaven National Laboratory

11. ABSTRACT *(200 words or less)*

This three-volume report contains 90 papers out of the 102 that were presented at the Twenty-First Water Reactor Safety Information Meeting held at the Bethesda Marriott Hotel, Bethesda, Maryland, during the week of October 25-27, 1993. The papers are printed in the order of their presentation in each session and describe progress and results of programs in nuclear safety research conducted in this country and abroad. Foreign participation in the meeting included papers presented by researchers from France, Germany, Japan, Russia, Switzerland, Taiwan, and United Kingdom. The titles of the papers and the names of the authors have been updated and may differ from those that appeared in the final program of the meeting.

12. KEY WORDS/DESCRIPTORS *(List words or phrases that will assist researchers in locating the report.)*

BWR type reactors - reactor safety, PWR type reactors - reactor safety, reactor safety - meetings, research programs - reviews, reactor accidents, reactor components, nuclear power plants - reliability, nuclear power plants - risk assessment, aging, probabilistic estimation, loss of coolant, reactor accidents -management, human factors, containment, systems analysis, leading abstract - proceedings, seismic effects, hydraulics - heat transfer, environmental engineering. International Organizations.

13. AVAILABILITY STATEMENT

Unlimited

14. SECURITY CLASSIFICATION

(This Page)

Unclassified

(This Report)

Unclassified

15. NUMBER OF PAGES

16. PRICE

DATE
FILMED
6/23/94
END