CONF-9410216--Vol. 1

NUREG/CP-0140
Vol. 1

Proceedings of the U.S. Nuclear Regulatory Commission

Twenty-Second Water Reactor Safety Information Meeting

Volume 1
- Plenary Session
- Advanced Instrumentation & Control Hardware & Software
- Human Factors Research
- IPE & PRA

Held at
Bethesda Marriott Hotel
Bethesda, Maryland
October 24–26, 1994

U.S. Nuclear Regulatory Commission

Office of Nuclear Regulatory Research

Proceedings prepared by
Brookhaven National Laboratory

AVAILABILITY NOTICE

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 2120 L Street, NW., Lower Level, Washington, DC 20555-0001

2. The Superintendent of Documents, U.S. Government Printing Office, P. O. Box 37082, Washington, DC 20402-9328

3. The National Technical Information Service, Springfield, VA 22161-0002

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC bulletins, circulars, information notices, inspection and investigation notices; licensee event reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the Government Printing Office: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, international agreement reports, grantee reports, and NRC booklets and brochures. Also available are regulatory guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG-series reports and technical reports prepared by other Federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions. *Federal Register* notices, Federal and State legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Office of Administration, Distribution and Mail Services Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, Two White Flint North, 11545 Rockville Pike, Rockville, MD 20852-2738, for use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018-3308.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

NUREG/CP-0140
Vol. 1

Proceedings of the U.S. Nuclear Regulatory Commission

Twenty-Second Water Reactor Safety Information Meeting

Volume 1

- Plenary Session
- Advanced Instrumentation & Control Hardware & Software
- Human Factors Research
- IPE & PRA

Held at
Bethesda Marriott Hotel
Bethesda, Maryland
October 24–26, 1994

Manuscript Completed: March 1995
Date Published: April 1995

Compiled by: Susan Monteleone

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

Proceedings prepared by
Brookhaven National Laboratory

ABSTRACT

This three-volume report contains papers presented at the Twenty-Second Water Reactor Safety Information Meeting held at the Bethesda Marriott Hotel, Bethesda, Maryland, during the week of October 24-26, 1994. 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 Finland, France, Italy, Japan, Russia, 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
22nd WATER REACTOR SAFETY INFORMATION MEETING

October 24-26, 1994

Published in Three Volumes

GENERAL INDEX

REGISTERED ATTENDEES (NON-NRC)
22ND WATER REACTOR SAFETY INFORMATION MEETING

H. ABE
NUCLEAR POWER ENGINEERING CORP.
3-13 4-CHOME TORANOMON
MINATO-KU TOKYO, 105 JAPAN

S. ADDITON
TENERA (ARSAP)
1901 RESEARCH BLVD., SUITE 100
ROCKVILLE, MD 20850-3184 USA

A. AFZALI
NUS
910 CLOPPER ROAD
GAITHERSBURG, MD 20879 USA

S. AHN
KOREA INSTITUTE OF NUCLEAR SAFETY
PO BOX 114
YUSUNG, TAEJON, 305-600 KOREA

M. ALAMMAR
GPU NUCLEAR CORP.
ONE UPPER POND RD.
PARSIPPANY, NJ 07054 USA

A. ALEMBERTI
ANSALDO
C. 30 PERRONE 25
GENOVA, 16161 ITALY

R. ALLEN
BATTELLE PACIFIC NORTHWEST LABS
PO BOX 999, MS P8-10
RICHLAND, WA 99352 USA

K. ALMENAS
UNIVERSITY OF MARYLAND
MAT. & NUC. ENERGY DEPT.
COLLEGE PARK, MD USA

A. ALONSO
POLYTECHNIC UNIVERSITY OF MADRID
JOSE GUTIERREZ ABASCAL, 2
MADRID, 28006 SPAIN

R. AMADOR
COMISION NACIONAL DE SEGURIDAD NUC. Y SALVAGUARDIA
DR BARRAGAN NO 779, COL NARVARTE
MEXICO D.F., 03020 MEXICO

L. ANDERMO
SWEDISH NUCLEAR POWER INSPECTORATE
BOX 27106
STOCKHOLM, S-102 52 SWEDEN

M. ANDOU
HITACHI WORKS, HITACHI LTD.
1-1, SAIWAI-CHO 3-CHOME
HITACHI-SHI, IBARAKI-KEN 317 JAPAN

J. ANDREWS
B&W FUEL COMPANY
PO BOX 10935
LYNCHBURG, VA 24506-0935 USA

W. ANDREWS
SOUTHERN NUCLEAR OPERATING COMPANY
PO BOX 1295
BIRMINGHAM, AL 35201 USA

S. ASAI
MINISTRY OF INT'L TRADE AND INDUSTRY
1-3-1, KASUMIGASAKI
CHIYODA-KU, TOKYO 100 JAPAN

V. ASMOLOV
RUSSIAN RESEARCH CENTER KURCHATOV INST.
KURCHATOV SQUARE
MOSCOW, 123182 RUSSIA

A. ASRANI
ATOMIC ENERGY REGULATORY BOARD
VIKRAM SARASHAI BHAVAN, ANUSHAKTI NAGAR
BOMBAY, 400 094 INDIA

M. AZARM
BROOKHAVEN NATIONAL LABORATORY
PO BOX 5000, BLDG. 130
UPTON, NY 11973-5000 USA

T. BAKER
SHIFTWORK SYSTEMS, INC.
ONE KENDALL SQUARE, BLDG. 200, 4TH FLOOR
CAMBRIDGE, MA 02139 USA

M. BALE
B&W FUEL COMPANY
3315 OLD FOREST RD., PO BOX 10935
LYNCHBURG, VA 24506 USA

Y. BANG
KOREA INSTITUTE OF NUCLEAR SAFETY
PO BOX 114
YUSUNG, TAEJON, 305-600 KOREA

A. BARATTA
PENN STATE UNIV., NUCLEAR ENGINEERING DEPT.
231 SACKETT BLDG.
UNIVERSITY PARK, PA 16802 USA

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

M. BARRIERE
BROOKHAVEN NATIONAL LABORATORY
PO BOX 5000, BLDG. 130
UPTON, NY 11973-5000 USA

P. BAYLESS
IDAHO NATIONAL ENGINEERING LABORATORY
PO BOX 1625
IDAHO FALLS, ID 83415-3840 USA

L. BELBLIDIA
SCANDPOWER, INC.
101 LAKE FOREST BLVD., STE. 340
GAITHERSBURG, MD 20877 USA

K. BERGERON
SANDIA NATIONAL LABORATORIES
P.O. BOX 5800, MS 0743
ALBUQUERQUE, NM 87185-0743 USA

S. BEUS
WESTINGHOUSE BETTIS
P.O. BOX 79
WEST MIFFLIN, PA 15122 USA

C. BEYER
PACIFIC NORTHWEST LABORATORY
BATTELLE BLVD.
RICHLAND, WA 99352 USA

B. BHASIN
NUCLEAR POWER CORPORATION OF INDIA
TARAPUR ATOMIC POWER STATION
TARAPUR, MAHARASHTRA, INDIA

D. BHATTACHARYA
NUCLEAR POWER CORP. OF INDIA
BOMBAY, INDIA

D. BLEY
BUTTONWOOD CONSULTING INC.
17291 BUTTONWOOD STREET
FOUNTAIN VALLEY, CA 92708 USA

L. BOLSHOV
RUSSIAN ACADEMY OF SCIENCES/NUC. SAFETY INST.
B. TULSKAYA, 52
MOSCOW, 113191 RUSSIA

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

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

R. BOYER
DUKE POWER CO.
8725 HORNWOOD CT.
CHARLOTTE, NC 28215 USA

G. BROWN
AEA TECHNOLOGY
THOMSON HOUSE, RISLEY
WARRINGTON, CHESHIRE WA36AT UK

W. BRUNSON
B&W FUEL COMPANY
PO BOX 10935
LYNCHBURG, VA 24506-0935 USA

R. BUDNITZ
FUTURE RESOURCES ASSOCIATES, INC.
2039 SHATTUCK AVE., SUITE 402
BERKELEY, CA 94704 USA

J. BUTLER
WESTINGHOUSE
P.O. BOX 355
PITTSBURGH, PA 15230 USA

C. CALLAWAY
NUCLEAR ENERGY INSTITUTE - NEI
1776 I ST., N.W., SUITE 400
WASHINGTON, DC 20006-3708 USA

A. CAMP
SANDIA NATIONAL LABORATORIES
PO BOX 5800
ALBUQUERQUE, NM 87185-0747 USA

G. CANAVAN
NEW YORK POWER AUTHORITY
123 MAIN ST.
WHITE PLAINS, NY 10601 USA

F. CARLIN
CIS BIO INTERNATIONAL
BP NO. 32
GIF-SUR-YVETTE CEDEX, F91192 FRANCE

D. CASADA
OAK RIDGE NATIONAL LABORATORY
PO BOX 2009, BLDG. 9102-1
OAK RIDGE, TN 37831-8038 USA

N. CAVLINA
UNIVERSITY OF ZAGREB
FACULTY OF ELEC. ENGINEERING, UNSKA 3
ZAGREB, CRO 41000 CROATIA

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

F-B. CHEUNG
PENNSYLVANIA STATE UNIVERSITY
304 REBER BLDG., PENN STATE U.
UNIVERSITY PARK, PA 16802 USA

B. CHO
ILLINOIS DEPARTMENT OF NUCLEAR SAFETY
1035 OUTER PARK DRIVE
SPRINGFIELD, IL 62704 USA

D. CHO
ARGONNE NATIONAL LABORATORY
BLDG. 208, 9700 S. CASS AVE.
ARGONNE, IL 60439 USA

J. CHOI
KOREA INSTITUTE OF NUCLEAR SAFETY
151 DUKJIN-DONG YUSEONG-GU
TAEJON, KOREA, KOREA

S. CHOI
KOREA INSTITUTE OF NUCLEAR SAFETY
PO BOX 114
YUSUNG, TAEJON, 305-600 KOREA

A. CHRISTOU
MATERIALS & NUCLEAR ENG'G., U. OF MARYLAND
2135 BLDG. 090
COLLEGE PARK, MD 20742-2115 USA

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

T. CHU
SANDIA NATIONAL LABORATORIES
MS 1137, DEPT. 6422
ALBUQUERQUE, NM 87185 USA

N. CHUGO
TOSHIBA CORP.
8, SHINSUGITA-CHO, ISOGO-KU
YOKOHAMA, 235 JAPAN

A. COMBESCURE
CENTRE D'ETUDES DE SACLAY - DRN/DMT/SEMT
CENTRE D'ETUDES DE SACLAY
GIF SUR YVETTE CEDEX, 91191 FRANCE

L. COMES
SCIENCE & ENGINEERING ASSOCIATES, INC.
7918 JONES BRANCH DR., SUITE 500
MC LEAN, VA 22102 USA

L. CONNOR
SOUTHERN TECHNICAL SERVICES, INC.
3 METRO CENTER, SUITE 610
BETHESDA, MD 20814 USA

S. COOPER
SCIENCE APPLICATIONS INT'L. CORP.
11251 ROGER BACON DR., PO BOX 4875
RESTON, VA 22090 USA

R. COPELAND
SIEMENS POWER CORP.
2101 HORN RAPIDS RD.
RICHLAND, WA 99352 USA

B. CORWIN
OAK RIDGE NATIONAL LABORATORY
P.O. BOX 2008
OAK RIDGE, TN 37831-8151 USA

M. COURTAUD
COMMISSARIAT A L'ENERGIE ATOMIQUE
CENTRE D'ETUDES DE GRENOBLE 17, RUE DES MARTYRS
GRENOBLE, 38054 FRANCE

K. COZENS
NUCLEAR ENERGY INSTITUTE - NEI
1776 I ST., N.W., SUITE 400
WASHINGTON, DC 20006-3708 USA

M. CUNNINGHAM
PACIFIC NORTHWEST LABORATORY
PO BOX 999 K8-43
RICHLAND, WA 99352 USA

R. CURTIS
AECL RESEARCH
WHITESHELL LABORATORIES
PINAWA, MB ROE 1LO CANADA

V. DAJI
DUKE POWER COMPANY
9515 PONDSIDE LANE
CHARLOTTE, NC 28213 USA

R. DALLMAN
SCIENTECH, INC.
1700 LOUISIANA BLVD., NE STE. 230
ALBUQUERQUE, NM 87110 USA

J. DANKO
CONSULTANT - UNIVERSITY OF TENNESSEE
15818 SE 35TH ST
VANCOUVER, WA 98684 USA

J. DAVIS
NUCLEAR ENERGY INSTITUTE - NEI
1776 I ST., N.W., SUITE 400
WASHINGTON, DC 20006-3708 USA

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

J. DE BOR
SCIENCE & ENGINEERING ASSOCIATES, INC.
7918 JONES BRANCH DR., SUITE 500
MC LEAN, VA 22102 USA

L. DEITRICH
ARGONNE NATIONAL LABORATORY
9700 SO. CASS AVE., BLDG. 208
ARGONNE, IL 60439 USA

D. DIAMOND
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, PO BOX 5000
UPTON, NY 11973-5000 USA

H. DIAMOND
PELCO ENERGY
965 CHESTERBROOK BLVD.
WAYNE, PA 19087 USA

H. DIETERSHAGEN
KNOLLS ATOMIC POWER LAB., INC. - MARTIN MARIETTA
RIVER ROAD - PO BOX 1072
SCHENECTADY, NY 12301-1072 USA

S. DOROFEEV
KURCHATOV INSTITUTE
KURCHATOV SQUARE 1
MOSCOW, RUSSIA, 123182 RUSSIA

R. DUBOURG
CEA-IPSN DES/SEPRI
BP 6
FONTENAY AUX ROSES, 92265 FRANCE

J. DUCO
INSTITUT DE PROTECTION ET DE SURETE NUCLEAIR
CEA, CEN/FAR 60-68 AVE. DU GENERAL LECLERC
FONTENAY AUX ROSES, 92265 FRANCE

R. DUFFEY
BROOKHAVEN NATIONAL LABORATORY
PO BOX 5000, BLDG. 197C
UPTON, NY 11973-5000 USA

J. EATON
NUCLEAR ENERGY INSTITUTE - NEI
1776 I ST., N.W., SUITE 400
WASHINGTON, DC 20006-3708 USA

R. EBERLE
SIEMENS-KWU
HAMMERBACHERSTRASSE 12+14
ERLANGEN, D-8520 GERMANY

M. ELI
LAWRENCE LIVERMORE NATIONAL LAB.
PO BOX 808, L-126
LIVERMORE, CA 94550 USA

F. ELIA
STONE AND WEBSTER ENG. CORP.
PO BOX 2325
BOSTON, MA 02107 USA

T. ENDO
NUCLEAR POWER ENGINEERING CORP.
FUJITA KANKO TORANOMON BLDG. 5F 17-1, 3-CHOME, TORA
MINATO-KU, TOKYO 105 JAPAN

R. ENNIS
TENERA
1901 RESEARCH BLVD., SUITE 100
ROCKVILLE, MD 20850 USA

T. EURASTO
FINNISH CENTRE FOR RADIATION & NUCLEAR SAFETY
PO BOX 14, FIN-00881
HELSINKI, FINLAND

M. FAKORY
S3 TECHNOLOGIES
8930 STAMFORD BLVD.
COLUMBIA, MD 21045 USA

D. FERETIC
UNIVERSITY OF ZAGREB
FACULTY OF ELEC. ENGINEERING, UNSKA 3
ZAGREB, CRO 41000 CROATIA

F. FERON
DIRECTION DE LA SURETE DES INSTALLATIONS NUCLEAIRES
20 AVENUE DE SEGUR
PARIS CEDEX 07 SP, 75353 FRANCE

A. FERRELI
DIR. FOR NUCLEAR SAFETY & HEALTH PROTECTION
VIA VITALIANO BRANCATI 48
ROME, 00168 ITALY

I. FIERO
ABB COMBUSTION ENGINEERING NUCLEAR FUEL
1000 PROSPECT HILL RD.
WINDSOR, CT 06095-0500 USA

M. FIRNHABER
GRS
SCHWERTNERGASSE 1
COLOGNE, 50667 GERMANY

J. FISHER
UTILITY RESOURCE ASSOCIATES, INC.
51 MONROE ST., SUITE 12000
ROCKVILLE, MD 20850 USA

M. FLETCHER
AECL TECHNOLOGIES INC.
9210 CORPORATE BLVD., SUITE 410
ROCKVILLE, MD 20850 USA

J. FOLSOM
GPU NUCLEAR CORP.
ONE UPPER POND RD.
PARSIPPANY, NJ 07054 USA

J. FORESTER
SANDIA NATIONAL LABORATORIES
DEPT. 6412
ALBUQUERQUE, NM 87185 USA

T. FUJISHIRO
JAPAN ATOMIC ENERGY RESEARCH INSTITUTE
TOKAI-MURA, NAKA-GUN
IBARAKI-KEN 319-11, JAPAN

A. FUKUDA
TOSHIBA CORP., ISOGO NUCLEAR ENGINEERING
8 SHINSUGITA-CHO, ISOGO-KU
YOKOHAMA, KANAGAWA 235 JAPAN

R. GAMBLE
GE NUCLEAR ENERGY
175 CURTNER AVE, M.C. 781
SAN JOSE, CA 95125 USA

R. GAUNTT
SANDIA NATIONAL LABORATORIES
PO BOX 5800, M.S. 1139
ALBUQUERQUE, NM 87185-1139 USA

J. GAUTHIER
COMMISSARIAT A L'ENERGIE ATOMIQUE
CE/FAR BP 6
FONTENAY AUX ROSES, 92265 FRANCE

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

C. GIGGER
BETTIS
P.O. BOX 79
WEST MIFFLIN, PA 15122 USA

R. GILLILAND
OAK RIDGE NATIONAL LABORATORY
P.O. BOX 2009, MS 8051
OAK RIDGE, TN 37831-8051 USA

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

L. GOLDSTEIN
S.M. STOLLER CORP.
485 WASHINGTON AVE.
PLEASANTVILLE, NY 10570 USA

M. GOMOLINSKI
IPSN
321 RUE DE CHARENTON
PARIS, F 75012 FRANCE

A. GOPALAKRISHNAN
ATOMIC ENERGY REGULATORY BOARD
VIKRAM SARASHAI BHAVAN, ANUSHAKTI NAGAR
BOMBAY, 400 094 INDIA

M. GOTO
TOSHIBA CORP., ISOGO NUCLEAR ENGINEERING
8 SHINSUGITA-CHO, ISOGO-KU
YOKOHAMA, KANAGAWA 235 JAPAN

N. GOULDING
B&W NUCLEAR TECHNOLOGIES
PO BOX 10935
LYNCHBURG, VA 24506-0935 USA

M. GRANDAME
ATOMIC ENERGY CONTROL BOARD CANADA
C/O ONTARIO HYDRO, P.O. BOX 160
PICKERING, ONTARIO L1V2r5 CANADA

J. GREEN
UNIVERSITY OF MARYLAND
NUCLEAR ENG'G, 2135 BLDG. 090
COLLEGE PARK, MD 20742 USA

L. GROSSMAN
ABB COMBUSTION ENGINEERING
ADDISON ROAD
WINDSOR, CT 06095 USA

M. GROUNES
STUDSVIK NUCLEAR
S-61182 NYKOPING
NYKOPING, S-61182 SWEDEN

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

G. HACHE
INSTITUT DE PROTECTION ET DE SURETE NUCLEAIRE
CE CADARACHE BAT. 702
ST. PAUL LEZ DURANCE, 13108 FRANCE

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

L. HARROP
NUCLEAR INSTALLATIONS INSPECTORATE
ST. PETER'S HOUSE, BALLIOL RD
BOOTLE, MERSEYSIDE, L20 3LZ UK

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

C. HARWOOD
ATOMIC ENERGY CONTROL BOARD, CANADA
PO BOX 1046 STATION B, 280 SLATER ST.
OTTAWA, ONTARIO K1P 5S9 CANADA

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

M. HASSAN
BROOKHAVEN NATIONAL LABORATORY
PO BOX 5000, BLDG. 130
UPTON, NY 11973-5000 USA

H. HAYDEN
OAK RIDGE NATIONAL LABORATORY
P.O. BOX 2008, BLDG. 4500S
OAK RIDGE, TN 37831-8152 USA

J. HENRY
INSTITUT DE PROTECTION ET DE SURETE NUCLEAIRE
BP6
FONTENAY AUX ROSES, 92265 FRANCE

A. HEYMER
NUCLEAR ENERGY INSTITUTE - NEI
1776 I ST., N.W., SUITE 400
WASHINGTON, DC 20006-3708 USA

D. HIDINGER
MARTIN MARIETTA CORP. (KAPL, INC.)
PO BOX 1072
SCHENECTADY, NY 12302 USA

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

A. HO
SIEMENS POWER CORP., NUCLEAR DIV.
PO BOX 130
RICHLAND, WA 99352 USA

R. HOBBINS
RRH CONSULTING
PO BOX 971
WILSON, WY 83014 USA

L. HOCHREITER
WESTINGHOUSE ELECTRIC COMPANY
P.O. BOX 355
PITTSBURGH, PA 15230 USA

S. HODGE
OAK RIDGE NATIONAL LABORATORY
PO BOX 2009 9104-1, MS 8057
OAK RIDGE, TN 37831-8057 USA

P. HOFMANN
NUCLEAR RESEARCH CENTER KARLSRUHE
PO BOX 3640
KARLSRUHE, D-76021 GERMANY

J. HOHORST
IDAHO NATIONAL ENGINEERING LABORATORY
PO BOX 1625
IDAHO FALLS, ID 83415 USA

H. HOLMSTROM
VTT ENERGY, NUCLEAR ENERGY
PO BOX 1604
ESPOO, 02044 VTT FINLAND

R. HOUSER
BETTIS ATOMIC POWER LABORATORY
173 MONTICELLO DR.
MONROEVILLE, PA 15146 USA

A. HOWARD
TOKYO ELECTRIC POWER CO
1901 L ST., NW
WASHINGTON, DC 20036 USA

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

H-Y HUANG
ATOMIC ENERGY COUNCIL, REP. OF CHINA
67 LANE 144, KEELUNG RD., SEC. 4
TAIPEI, TAIWAN ROC

S. HYTEN
WYLE LABORATORIES
PO BOX 077777
HUNTSVILLE, AL 35807-7777 USA

Y. IBE
NUCLEAR POWER ENGINEERING CORP.
3-13 4-CHOME TORANOMON
MINATO-KU TOKYO, 105 JAPAN

R. IRWIN
UNION ELECTRIC CO.
PO BOX 149, MC 470
ST. LOUIS, MO 63166 USA

H. ISBIN
NSRRC
2815 MONTEREY PKWY
MINNEAPOLIS, MN 55418-3959 USA

M. ISHII
PURDUE UNIVERSITY
SCHOOL OF NUCLEAR ENGINEERING
WEST LAFAYETTE, IN 47907 USA

J. JANSKY
BTB JANSKY GMBH
GERLINGER STR. 151
LEONBERG, 71229 GERMANY

T. JAYAKUMAR
INDIRA GANDHI CENTRE FOR ATOMIC RESEARCH
KALPAKKAM, INDIA

M. JIMINEZ
FLORIDA POWER & LIGHT
700 UNIVERSITY BLVD.
JUNO BEACH, FL 33407 USA

Y. JIN
KOREA ATOMIC ENERGY RESEARCH INST.
PO BOX 105, YUSEONG
TAEJON, 305-353 KOREA

J. JO
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, P.O. BOX 5000
UPTON, NY 11973-5000 USA

G. JOHNSEN
IDAHO NATIONAL ENGINEERING LAB
PO BOX 1625
IDAHO FALLS, ID 83415-3880 USA

R. JOHNSON
PACIFIC GAS & ELECTRIC CO.
333 MARKET ST., RM. 1061
SAN FRANCISCO, CA 94177 USA

A. KAKODKAR
BHABHA ATOMIC RESEARCH CENTRE
REACTOR DESIGN & DEV. GROUP
TROMBAY, INDIA

F. KAM
OAK RIDGE NATIONAL LABORATORY
PO BOX 2009
OAK RIDGE, TN 37831-8250 USA

S-P KAO
SIMULATION EXPERT SYSTEMS
23 HARBOR CLOSE
NEW HAVEN, CT 06519 USA

Y. KARINO
TOSHIBA CORP. (GE NUCLEAR ENERGY)
970 ST. ANDREWS DR., APT. 102
WILMINGTON, NC 28412 USA

H. KARWAT
TECHNISCHE UNIVERSITAT MUNCHEN
FORSCHUNGSGELANDE, D-85748 GARCHING
GARCHING, GARCHING D-85748 GERMANY

H. KASHIMA
MITSUBISHI HEAVY INDUSTRIES, LTD.
3-1, MINATOMIRA1 3CHOME, NISHI-KU
YOKOHAMA, 220 JAPAN

T. KATSUSHIGE
JAPAN POWER ENG'G & INSPECTION CORP.
SHIN-URAYASU BLDG., 9-2, MIHAMA 1 CHOME
URAYASU-SHI, CHIBA-KEN, 279 JAPAN

J. KAVANAGH
ATOMIC ENERGY CONTROL BOARD
280 SLATER ST
OTTAWA, ONTARIO K1P 5S9 CANADA

J. KELLY
SANDIA NATIONAL LABORATORIES
PO BOX 5800, MS 0742
ALBUQUERQUE, NM 87185-0742 USA

S. KERCEL
OAK RIDGE NATIONAL LABORATORY
PO BOX 2008, BLDG. 3508/MS 6318
OAK RIDGE, TN 37831-6318 USA

R. KERN
NETCORP
9 BANNISTER CT.
GAITHERSBURG, MD 20879 USA

B. KIM
KOREA INSTITUTE OF NUCLEAR SAFETY
PO BOX 114
YUSUNG, TAEJON, 305-600 KOREA

H. KIM
KOREA INSTITUTE OF NUCLEAR SAFETY
PO BOX 114
YUSUNG, TAEJON, 305-600 KOREA

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

I. KIM
KOREA ATOMIC ENERGY RESEARCH INSTITUTE
PO BOX 105, YUSEONG
TAEJON, 305-600 KOREA

K. KIM
KOREA INSTITUTE OF NUCLEAR SAFETY
151 DUKJIN-DONG YUSEONG-GU
TAEJON, KOREA, KOREA

S. KIM
KOREA INSTITUTE OF NUCLEAR SAFETY
PO BOX 114
YUSUNG, TAEJON, 305-600 KOREA

W. KIM
KOREA INSTITUTE OF NUCLEAR SAFETY
PO BOX 114
YUSUNG, TAEJON, 305-600 KOREA

S. KINNERSLY
AEA TECHNOLOGY
WINFRITH TECHNOLOGY CENTRE
DORCHESTER, DORSET DT2 8DH UK

J. KLAPPROTH
GE NUCLEAR
PO BOX 780, MC J26
WILMINGTON, NC 28402 USA

P. KLOEG
KEMA
UTRECHTSEWEG 310
ARNHEM, 6812 AR NETHERLANDS

Y. KOBAYASHI
NUCLEAR POWER ENGINEERING CORP.
FUJITA KANKO TORANOMON BLDG. 5F 17-1, 3-CHOME, TORA
MINATO-KU, TOKYO 105 JAPAN

K. KORSAH
OAK RIDGE NATIONAL LABORATORY
PO BOX 2008, BLDG. 3500, MS 6010
OAK RIDGE, TN 37831 USA

M. KOYAMA
JAPAN POWER ENG'G & INSPECTION CORP.
SHIN-URAYASU BLDG., 9-2, MIHAMA 1 CHOME
URAYASU-SHI, CHIBA-KEN, 279 JAPAN

P. KRISHNASWAMY
BATTELLE PACIFIC NORTHWEST LABORATORY
505 KING AVE.
COLUMBUS, OH 43201 USA

B. KUCZERA
KERNFORSCHUNGSZENTRUM NUC. RESEARCH CENTER
PO BOX 3640
KARLSRUHE, D76021 GERMANY

Y. KUKITA
JAPAN ATOMIC ENERGY RESEARCH INSTITUTE
TOKAI, IBARAKI, IBARAKI 319-11 JAPAN

K. KUSSMAUL
MPA STUTTGART
PFAFFENWALDRING 32
STUTTGART, 70569 GERMANY

P. LACY
URA
51 MONROE STREET, SUITE 1600
ROCKVILLE, MD 20850 USA

J. LAKE
IDAHO NATIONAL ENGINEERING LABORATORY
PO BOX 1625
IDAHO FALLS, ID 83415-3895 USA

D. LAMPE
UTILITY RESOURCE ASSOCIATES, INC.
51 MONROE ST., SUITE 1600
ROCKVILLE, MD 20814 USA

P. LANG
U.S. DEPT. OF ENERGY
NE-451
WASHINGTON, DC 20585 USA

S. LANGENBUCH
GESELLSCHAFT FUR ANLAGEN U. REAKTORSICHERHEIT
FORSCHUNGSGELANDE
GARCHING, 85748 GERMANY

V. LANGMAN
ONTARIO HYDRO
700 UNIVERSITY AVE.
TORONTO, ONT M5G1X6 CANADA

D. LANNING
BATTELLE PACIFIC NORTHWEST LAB.
809 W. 22ND AVE.
KENNEWISK, WA 99337 USA

E. LANNING
NEBRASKA PUBLIC POWER DISTRICT
PO BOX 499
COLUMBUS, NE 68602-0499 USA

E. LANNING
NEBRASKA PUBLIC POWER DISTRICT
P.O. BOX 499
COLUMBUS, NE 68602-0499 USA

C. LECOMTE
INSTITUT DE PROTECTION ET DE SURETE NUCLEAIR
CEA, CEN/FAR 60-68 AVE. DU GENERAL LECLERC
FONTENAY AUX ROSES, 92265 FRANCE

C. LEE
KOREA ATOMIC ENERGY RESEARCH INSTITUTE
PO BOX 105, YUSONG
TAEJON, 305-606 KOREA

D. LEE
KOREA ELECTRIC POWER CORPORATION
103-16 MUNJI-DONG, YUSEONG-KU
TAEJEON, KOREA

J. LEE
KOREA INSTITUTE OF NUCLEAR SAFETY
P.O. BOX 114, YUSONG
TAEJON, KOREA, 305-600 KOREA

S. LEE
KOREA ATOMIC ENERGY RESEARCH INST.
PO BOX 105, YUSONG
TAEJON, 305-353 KOREA

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

M. LIVOLANT
INSTITUT DE PROTECTION ET DE SURETE NUCLEAIRE
CE/FAR BP M 6
FONTENAY-AUX-ROSES CEDEX, 92265 FRANCE

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

F. LOSS
MEA
9700-B M.L. KING JR. HWY.
LANHAM, MD 20706 USA

S. LU
LAWRENCE LIVERMORE NATIONAL LAB.
7000 EAST AVE.
LIVERMORE, CA 94550 USA

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

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

D. MAGALLON
CED-JRD ISPRA
JRC-EURATOM
ISPRA, VARESE 21020 ITALY

C. MANUEL
CEA-IPSN DES/SEPRI
BP 6
FONTENAY AUX ROSES, 92265 FRANCE

J. MARCON
FRAMATOME NUCLEAR FUEL
10, RUE JULIETTE RECAMIER
LYON, 69456 FRANCE

Y. MARUYAMA
JAPAN ATOMIC ENERGY RESEARCH INSTITUTE
2-4 SHIRANE, SHIRAKATA
NAKA-GUN, IBARAKI-KEN, 319-11 JAPAN

S. MASAMORI
MITSUBISHI HEAVYINDUSTRIES, LTD.
1-1-1 WADASAKI-CHO, HYOGO-KU
KOBE, 654 JAPAN

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

B. MAVKO
J. STEFAN INSTITUTE
JAMOVA 39
LJUBLJANA, SLOV. 61111 SLOVENIA

R. McCARDELL
EG&G IDAHO, INC.
187 NORTH 4200 EAST
RIGBY, ID 83442 USA

D. McCULLOUGH
KAPL, INC., MARTIN MARIETTA
RIVER ROAD
SCHENECTADY, NY 12301 USA

K. McDONOUGH
KNOLLS ATOMIC POWER LAB., INC. - MARTIN MARIETTA
RIVER ROAD - PO BOX 1072
SCHENECTADY, NY USA

T. McINTYRE
GE NUCLEAR ENERGY
175 CURTNER AVE, M.C. 781
SAN JOSE, CA 95125 USA

R. McMILLAN
AEA TECHNOLOGY
THOMSON HOUSE, RISLEY
WARRINGTON, CHESHIRE WA38AT UK

K. McMINN
AEA TECNOLOGY
WINFRITH TECHNOLOGY CENTER, DORCHESTER
DORSET, DT28DH UK

C. MEDICH
SOCIETA INFORMAZIONI EXPERIENZE TERMOIDRAULICHE
VIA N. BIXIO 27
PIACENZA, 29100 ITALY

N. MESHKATI
UNIVERSITY OF SOUTHERN CALIFORNIA
INST. OF SAFETY & SYSTEMS MGT, USC
LOS ANGELES, CA 90089-0021 USA

G. MEYER
B&W FUEL COMPANY
PO BOX 10935
LYNCHBURG, VA 24506-0935 USA

A. MEYER-HEINE
INSTITUT DE PROTECTION ET DE SURETE NUCLEAIRE
CE CADARACHE BAT. 702
ST. PAUL LEZ DURANCE, 13108 FRANCE

A. MIAO
CHARLES RIVER ANALYTICS, INC.
55 WHEELER ST.
CAMBRIDGE, MA 02138 USA

M. MILLER
DUKE POWER COMPANY
PO BOX 1439, MS ON01ES
SENECA, SC 29679 USA

R. MILLER
WESTINGHOUSE ELECTRIC CORP.
4350 NORTHERN PIKE WEC W 316
MONROEVILLE, PA 15146-2888 USA

S. MIRSKY
SCIENCE APPLICATIONS INT'L. CORP.
20201 CENTURY BLVD.
GERMANTOWN, MD 20874 USA

D. MITCHELL
B&W FUEL COMPANY
PO BOX 10935
LYNCHBURG, VA 24506-0935 USA

D. MODEEN
NUCLEAR ENERGY INSTITUTE - NEI
1776 I ST., N.W., SUITE 400
WASHINGTON, DC 20006-3708 USA

S. MODRO
INEL LOCKHEED IDAHO TECHNOLOGIES CO.
PO BOX 1625, MS 3890
IDAHO FALLS, ID 83415-3890 USA

D. MONHARDT
FRAMATOME
1 PLACE DE LA COUPOLE
COURBEVOIE, 92400 FRANCE

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

F. MOODY
GE NUCLEAR ENERGY
175 CURTNER AVE, M.C. 781
SAN JOSE, CA 95125 USA

D. MORRISON
THE MITRE CORPORATION
7525 COLSHIRE DR., MS W766
MCLEAN, VA 22102 USA

A. MOTTA
PENN STATE UNIV., NUCLEAR ENGINEERING DEPT.
231 SACKETT BLDG.
UNIVERSITY PARK, PA 16802 USA

K. MURAYAMA
HITACHI LTD.
1-1, SAIWAI-CHO 3-CHOME, HITACHI-SHI, IBARAKI-KEN
HITACHI-SHI, JAPAN

T. NAGAO
NUCLEAR POWER ENGINEERING CORP.
17-1, 3-CHOME TORANOMON
TOKYO, 105 JAPAN

D. NAUS
OAK RIDGE NATIONAL LABORATORY
PO BOX 2009, BLDG. 9204-1
OAK RIDGW, TN 37831-8056 USA

R. NG
NUCLEAR ENERGY INSTITUTE - NEI
1776 I ST., N.W., SUITE 400
WASHINGTON, DC 20006-3708 USA

M-S NI
ATOMIC ENERGY COUNCIL, REP. OF CHINA
67 LANE 144, KEELUNG RD., SEC. 4
TAIPEI, TAIWAN ROC

G. NIEDERAUER
LOS ALAMOS NATIONAL LABORATORY
M.S. K575
LOS ALAMOS, NM 87545 USA

L. NILSSON
STUDSVIK ECO & SAFETY AB
S-61182 NYKOPING
NYKOPING, S-61182 SWEDEN

S. NOWLEN
SANDIA NATIONAL LABORATORIES
MS/0737, PO BOX 5800
ALBUQUERQUE, NM 87185 USA

A. NUNEZ
COMISION NACIONAL DE SEGURIDAD NUC. Y SALVAGUARDIA
DR BARRAGAN NO 779, COL NARVARTE
MEXICO D.F., 03020 MEXICO

N. ORTIZ
SANDIA NATIONAL LABORATORIES
PO BOX 5800, MS 0738
ALBUQUERQUE, NM 87185-0738 USA

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

L. OSTROM
IDAHO NATIONAL ENGINEERING LABORATORY
P.O. BOX 1625
IDAHO FALLS, ID 83415-3855 USA

O. OZER
ELECTRIC POWER RESEARCH INSTITUTE
3412 HILLVIEW AVE.
PALO ALTO, CA 94304-1395 USA

B. PALAGI
COM ED COMPANY
P.O. BOX 767
CHICAGO, IL 60601 USA

J. PAPIN
INSTITUT DE PROTECTION ET DE SURETE NUCLEAIRE
CE CADARACHE BAT. 702
ST. PAUL LEZ DURANCE, 13108 FRANCE

B. PARK
KOREA NUCLEAR FUEL COMPANY
DAEJEON, 300 KOREA

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

M. PARKER
ILLINOIS DEPARTMENT OF NUCLEAR SAFETY
1035 OUTER PARK DRIVE
SPRINGFIELD, IL 62704 USA

J. PATE
OAK RIDGE NATIONAL LABORATORY
PO BOX 2008
OAK RIDGE, TN 37831-6158 USA

J. PELTIER
COMMISSARIAT A L'ENERGIE ATOMIQUE
BP 6
FONTENAY-AUX-ROSES-CEDEX, 92265 FRANCE

W. PENNELL
AMERICAN SOCIETY OF MECHANICAL ENGINEERS
PO BOX 2009, BLDG. 9204-1, MS-8056
OAK RIDGE, TN 37831-8056 USA

P. PERMEZEL
ELECT. DE FRANCE, SER. ETUDES ET PROJETS THERMIQUES
12-14 AV. DUTRIEVOZ
VILLEURBANNE, LYON 69628 FRANCE

M. PETRASKE
ABB COMBUSTION ENGINEERING
1000 PROSPECT HILL RD.
WINDSOR, CT 06095 USA

M. PEZZILLI
VIA ANGUILLARESO 301
S. MARIA DI GALERIA
ROMA, 60 ITALY

H. PFEFFERLEN
GENERAL ELECTRIC
175 CURTNER AVE, M.C. 781
SAN JOSE, CA 95125 USA

T. PIETRANGELO
NUCLEAR ENERGY INSTITUTE - NEI
1776 I ST., N.W., SUITE 400
WASHINGTON, DC 20006-3708 USA

B. PIKUL
THE MITRE CORPORATION
7525 COLSHIRE DR.
MC LEAN, VA 22102 USA

E. PILAT
YANKEE ATOMIC
580 MAIN ST.
BOLTON, MA 01740 USA

M. PILCH
SANDIA NATIONAL LABORATORIES
PO BOX 5800
ALBUQUERQUE, NM 87185-1137 USA

E. PIPLICA
WESTINGHOUSE
P.O. BOX 355
PITTSBURGH, PA 15230 USA

M. PODOWSKI
RPI
DEPT. OF NUCL. ENG. & ENG. PHYSICS
TROY, NY 12180 USA

S. POPE
SCIENTECH, INC.
11140 ROCKVILLE PIKE
ROCKVILLE, MD 20852 USA

G. POTTS
GE NUCLEAR
PO BOX 780, MC K05
WILMINGTON, NC 28402 USA

R. PRAKASH
EMBASSY OF INDIA
WASHINGTON, DC USA

W. PRATT
BROOKHAVEN NATIONAL LABORATORY
BUILDING 130
UPTON, NY 11973 USA

R. PROEBSTLE
GE NUCLEAR
PO BOX 780, MC A01
WILMINGTON, NC 28402 USA

V. PROKLOV
RRC KURCHATOV INSTITUTE
KURCHATOV SQUARE 1
MOSCOW, RUSSIA, 123182 RUSSIA

J. PUGA
UNESA
FRANCISCO GERVAS 3
MADRID, 28020 SPAIN

C. PUGH
OAK RIDGE NATIONAL LABORATORY
P.O. BOX 2009, MS 8063
OAK RIDGE, TN 37831 USA

T. RAJALA
ABB ATOM
FINNSLATTEN
VASTERAS, SWEDEN

D. RAPP
WESTINGHOUSE BETTIS LAB
P.O. BOX 79
WEST MIFFLIN, PA 15102 USA

J. RASHID
ANATECH RESEARCH CORP.
5435 OBERLIN DR.
SAN DIEGO, CA 92037 USA

S. RAY
WESTINGHOUSE ELECTRIC CORP.
PO BOX 355
PITTSBURGH, PA 15230 USA

K. REIL
SANDIA NATIONAL LABORATORIES
PO BOX 5800, M.S. 1139
ALBUQUERQUE, NM 87185-1139 USA

W. RETTIG
U.S. DOE, IDAHO OFFICE
850 ENERGY DRIVE
IDAHO FALLS, ID 83402 USA

J. RHODE
HEAD, SEVERE ACCIDENTS DEPT., GRS
SCHWERTNERGASSE 1
COLOGNE, 50667 GERMANY

L. RIB
AECL TECHNOLOGIES INC.
9210 CORPORATE BLVD., SUITE 410
ROCKVILLE, MD 20850 USA

A. RODRIGUEZ
COMISION NACIONAL DE SEGURIDAD NUC.Y SALVAGUARDIA
DR BARRAGAN NO 779, COL NARVARTE
MEXICO D.F., 03020 MEXICO

U. ROHATGI
BROOKHAVEN NATIONAL LABORATORY
BLDG. 475B, PO BOX 5000
UPTON, NY 11973-5000 USA

A. ROSCIOLI
PENNSYLVANIA POWER & LIGHT CO.
2 NORTH 9TH ST.
ALLENTOWN, PA 18101 USA

T. ROSS
PSE&G
PO BOX 236, MC n20
HANCOCKS BRIDGE, NJ 08038 USA

P. ROTHWELL
NUCLEAR INSTALLATIONS INSPECTORATE
ROOM 908 ST. PETER'S HOUSE, BALLIOL RD.
BOOTLE, MERSEYSIDE, L20 3LZ UK

T. ROWELL
WESTINGHOUSE ELECTRIC CORP.
PO BOX 353
PITTSBURGH, PA 15230 USA

J. ROYEN
OECD NUCLEAR ENERGY AGENCY
12 BLVD. DES ILES
ISSY-LES-MOULINEAUX, F92130 FRANCE

H. RYU
NUCLEAR POWER ENGINEERING CORP.
8F FUJITAKANKO TORANOMON BLDG. 17-1, 3-CHOME
MINATO-KU, TOKYO, 105 JAPAN

K. SAITO
NUCLEAR POWER ENGINEERING CORP.
17-1, 3-CHOME TORANOMON
TOKYO, 105 JAPAN

O. SANDERVAG
SWEDISH NUCLEAR POWER INSPECTORATE
SEHLSTEDT GT 11
STOCKHOLM, SWEDEN

M. SARRAM
NUCLEAR ENERGY INSTITUTE - NEI
1776 I ST., N.W., SUITE 400
WASHINGTON, DC 20006-3708 USA

K. SATO
HITACHI, LTD
3-1-1 SAIWAI-CHO
HITACHI-SHI, IBARAKI 317 JAPAN

K. SATO
MITSUBISHI ATOMIC POWER INDUSTRIES, INC.
3-3-1, MINATO MIRAI, NISHI-KU
YOKOHAMA-SHI, 220 JAPAN

M. SATO
TOSHIBA NUCLEAR MARKETING DEPT.
1-1-6, UCHISAIWAI-CHO
CHIYODA-KU, TOKYO 100 JAPAN

S. SAVOLAINEN
IMATRAN VOIMA OY/LOVIISA POWER PLANT
PO BOX 23
LOVIISA, FIN-07901 FINLAND

C. SAYLES
SOUTHERN CALIFORNIA EDISON
PO BOX 128
SAN CLEMENTE, CA 92672 USA

P. SCHEINERT
BETTIS ATOMIC POWER LABORATORY
PO BOX 79
WEST MIFFLIN, PA 15122 USA

F. SCHMITZ
CEA/IPSN
F-13108 ST. PAUL LEZ DURANCE CEDEX
FRANCE

R. SCHULTZ
IDAHO NATIONAL ENGINEERING LABORATORY
P.O. BOX 1625
IDAHO FALLS, ID 83415 USA

A. SEKRI
ELECT. DE FRANCE, SER. ETUDES ET PROJETS THERMIQUES
12-14 AV. DUTRIEVOZ
VILLEURBANNE, LYON 69628 FRANCE

C. SEOK
300, CHUN-CHUN-DONG
SUWON, KOREA, 440-748 KOREA

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

W. SHA
ARGONNE NATIONAL LABORATORY
9700 SOUTH CASS AVENUE
ARGONNE, IL 60439 USA

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

J. SHIN
RAYTHEON E&C
2 WORLD TRADE CENTER, 87 FL.
NEW YORK, NY 10048 USA

D. SHURBERG
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, PO BOX 5000
UPTON, NY 11973-5000 USA

E. SILVER
OAK RIDGE NATIONAL LAB
BLDG. 9201-3, MS 8065, PO BOX 2009
OAK RIDGE, TN 37831-8065 USA

B. SINGH
JUPITER CORP.
2730 UNIVERSITY BLVD. W, STE. 900
WHEATON, MD 20902 USA

S. SNIDER
TU ELECTRIC COMPANY
400 NORTH OLIVE, L.B. 81/24SLIC
DALLAS, TX 75201 USA

M. SONG
KOREA INSTITUTE OF NUCLEAR SAFETY
PO BOX 114
YUSUNG, TAEJON, 305-600 KOREA

B. SOUBIES
INSTITUT DE PROTECTION ET DE SURETE NUCLEAIRE
B.P. 6
FONTENAY AUX ROSES, 92265 FRANCE

G. SRINIVASAN
NUCLEAR POWER CORPORATION OF INDIA
TARAPUR ATOMIC POWER STATION
TARAPUR, MAHARASHTRA, INDIA

K. ST. JOHN
YANKEE ATOMIC ELECTRIC CO.
580 MAIN ST
BOLTON, MA 01740 USA

W. STADTMULLER
MPA STUTTGART
PFAFFENWALDRING 32
STUTTGART, D-70569 GERMANY

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

R. STEELE JR.
IDAHO NATIONAL ENGINEERING LABORATORY
P.O. BOX 1625
IDAHO FALLS, ID 83415 USA

R. STIRN
GE NUCLEAR
PO BOX 780, MC F24
WILMINGTON, NC 28402 USA

J. STONE
MPR ASSOCIATES, INC.
320 KING ST.
ALEXANDRIA, VA 22314-3238 USA

P. STOREY
HSE/NSD
BROADLANE
SHEFFIELD, S37HQ UK

V. STRIZHOU
NSI RHS
B. TULSKAYA, 52
MOSCOW, RUSSIA, 113191 RUSSIA

E. STUBBE
TRACTEBEL INGENIERIE
AVE. ARIANE 7, BTE 1
BRUSSELS, 1200 BELGIUM

R. SUMMERS
SANDIA NATIONAL LABORATORIES
P.O. BOX 5800, MS 0745
ALBUQUERQUE, NM 87185-0745 USA

B. SUN
SUNUTECH, INC.
PO BOX 978
LOS ALTOS, CA 94023 USA

J. SUN
ARGONNE NATIONAL LABORATORY
9700 SOUTH CASS AVENUE
ARGONNE, IL 60439 USA

A. SUSLOV
RRC KURCHATOV INSTITUTE
KURCHATOV SQUARE 1
MOSCOW, RUSSIA, 123182 RUSSIA

E. SWANSON
B&W NUCLEAR TECHNOLOGIES
PO BOX 10935
LYNCHBURG, VA 24506-0935 USA

I. SZABO
COMMISSARIAT L'ENERGIE ATOMIQUE
C.E. CADARACHE
ST. PAUL LES DURANCE, 13108 FRANCE

K. TAKIGUCHI
2-12-1 OH-OKAYAMA, MEGURO-KU
TOKYO, TOKYO 152 JAPAN

P. TALARICO
GILBERT/COMMONWEALTH, INC.
PO BOX 1498
READING, PA 19603 USA

T. TANAKA
SANDIA NATIONAL LABORATORIES
MS/0737, PO BOX 5800
ALBUQUERQUE, NM 87185 USA

P. TANGUY
ELECTRICITE DE FRANCE
32 RUE DE MONCEAU
PARIS, 75008 FRANCE

Z. TECHY
VEIKI
ZRINYI U. 1.
BUDAPEST, 1051 HUNGARY

C. THIBAULT
WYLE LABORATORIES
PO BOX 077777
HUNTSVILLE, AL USA

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

J. TOLY
CEA-IPSN DES/SEPRI
BP 6
FONTENAY AUX ROSES, 92265 FRANCE

A. TURRIAN
HSK SWISS FEDERAL NUC.SAFETY INSPECTORATE
WURENLINGEN
VILLIGEN-HSK, CH 5232 SWITZERLAND

R. VAN HOUTEN
JUPITER CORP.
2730 UNIVERSITY BLVD., STE 900
WHEATON, MD 20902 USA

W. VESELY
SCIENCE APPLICATIONS INT'L CORP.
655 METRO PLACE SOUTH
DUBLIN, OH 43017 USA

D. WALTERS
NUCLEAR ENERGY INSTITUTE - NEI
1776 I ST., N.W., SUITE 400
WASHINGTON, DC 20006-3708 USA

A. WARE
IDAHO NATIONAL ENGINEERING LABORATORY
PO BOX 1625
IDAHO FALLS, ID 83415-3750 USA

D. WHITEHEAD
SANDIA NATIONAL LABORATORIES
PO BOX 5800, MS 0747
ALBUQUERQUE, NM 87185-0747 USA

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

K. WOLFERT
GESELLSCHAFT FUR ANLAGEN & REAKTORSICHERHEIT MBH
FORSCHUNGSGELANDE, D-85748 GARCHING
DEUTSCHLAND, GARCHING D-85748 GERMANY

G. WROBEL
ROCHESTER GAS & ELECTRIC CORP.
49 EAST AVE.
ROCHESTER, NY 14649 USA

L. YEGOZOVA
RRC KURCHATOV INSTITUTE
ROGOV ST. 16, AP. 35
MOSCOW, RUSSIA

M. TORCIVIA
KNOLLS ATOMIC POWER LAB.
PO BOX 1072
SCHENECTADY, NY 12301-1072 USA

W. URKO
ABB/COMBUSTION ENGINEERING
1000 PROSPECT HILL RD., DEPT. 9341-0421
WINDSOR, CT 06095 USA

L. VANDEN HEUVEL
OAK RIDGE NATIONAL LABORATORY
PO BOX 2009, BLDG. 9201-3
OAK RIDGE, TN 37831-8065 USA

J. WADE
ARIZONA PUBLIC SERVICE
P.O. BOX 52034
PHOENIX, AZ 85072-2034 USA

S-F WANG
INSTITUTE OF NUCLEAR ENERGY RESEARCH
1000 WENHUA RD., CHIAAN VILLAGE
LUNG-TAN, TAIWAN 325 ROC

P. WEBSTER
ATOMIC ENERGYCONTROL BOARD, CANADA
280 SLATER ST.
OTTAWA, ONTARIO K1P 5S9 CANADA

K. WHITT
SOUTHERN NUCLEAR
40 INVERNESS CENTER PARKWAY
BIRMINGHAM, AL 35201 USA

M. WILLIS
WESTINGHOUSE ELECTRIC CORP.
PO BOX 353
PITTSBURGH, PA 15230 USA

J. WREATHALL
JOHN WREATHALL & CO.
4157 MACDUFF WAY
DUBLIN, OH 43017 USA

G. WU
NUCLEAR ENERGY INSTITUTE - NEI
1776 I ST., N.W., SUITE 400
WASHINGTON, DC 20006-3708 USA

K. YOO
KOREA ATOMIC ENERGY RESEARCH INSTITUTE
PO BOX 105, YUSONG
TAEJON, 305-600 KOREA

N. TRIKOUROS
GPU NUCLEAR CORP.
ONE UPPER POND RD.
PARSIPPANY, NJ 07054 USA

K. VALTONEN
FINNISH CENTRE FOR RADIATION & NUCLEAR SAFETY
P.O. BOX 14
FIN-00881-HELSINKI, FINLAND

O. VESCOVI
SOCIETA INFORMAZIONI EXPERIENZE TERMOIDRAULICHE
VIA N. BIXIO 27
PIACENZA, 29100 ITALY

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

W. WANG
STONE & WEBSTER ENG. CO.
P.O. BOX 5200
CHERRY HILL, NJ 08034 USA

J. WHITCRAFT
BECHTEL POWER CORP.
9801 WASHINGTONIAN BLVD.
GAITHERSBURG, MD 20878 USA

G. WILKOWSKI
BATTELLE PACIFIC NORTHWEST LABORATORY
505 KING AVE.
COLUMBUS, OH 43201 USA

L. WOLF
UNIV. OF MARYLAND, DEPT. MATERIALS & NUCLEAR ENG'G
2135 BLDG. 090
COLLEGE PARK, MD 20742-2115 USA

S. WRIGHT
SANDIA NATIONAL LABORATORIES
PO BOX 5800, MS 1145
ALBUQUERQUE, NM 87185-1145 USA

M. YAMAGISHI
MITSUBISHI ATOMIC POWER INDUSTRIES, INC.
3-1, MINATOMIRAI 3-CHOME, NISHI-KU
YOKOHAMA, KANAGAWA 220 JAPAN

Y. YOSHIZAWA
TOKYO INSTITUTE OF TECHNOLOGY
2-12-1 OH-OKAYAMA, MEGURO-KU
TOKYO, TOKYO 152 JAPAN

D. YU
KOREA ATOMIC ENERGY RESEARCH INST.
PO BOX 105, YUSONG
TAEJON, 305-353 KOREA

Y. YUNE
KOREA INSTITUTE OF NUCLEAR SAFETY
PO BOX 114
YUSUNG, TAEJON, 305-600 KOREA

G. ZACHARIAS
CHARLES RIVER ANALYTICS, INC.
55 WHEELER ST.
CAMBRIDGE, MA 02138 USA

D. ZANOBETTI
UNIVERSITY OF BOLOGNA
VIALE RISORGIMENTO 2
BOLOGNA, 40138 ITALY

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

PROCEEDINGS OF THE
TWENTY-SECOND WATER REACTOR SAFETY INFORMATION MEETING
October 24-26, 1994

CONTENTS - VOLUME 1

CONTENTS - VOLUME 1 (Cont'd)

CONTENTS - VOLUME 1 (Cont'd)

OPENING REMARKS

of

James M. Taylor
Executive Director for Operations
U.S. Nuclear Regulatory Commission

22nd Water Reactor Safety Information Meeting
Bethesda, MD

October 24, 1994

Good morning!

It is a pleasure to welcome so many of our colleagues from the United States and abroad to this twenty-second in the series of annual Water Reactor Safety Information Meetings.

This meeting is about research. Nuclear safety research has an integral and important place in our agency's approach to accomplish its safety regulatory mission. Research results provide critical information for assessing risks and the risk-reduction values of regulatory responses. We are moving towards safety regulation that is more clearly and directly risk based -- regulation that provides protection against significant risks but avoids imposition of resource burdens for risks that are not really there or are unimportant. Research results are major building blocks for the information base to support sound risk-based regulation.

This meeting includes papers and discussions covering the status of research being done both in the U.S. and abroad. It includes participants from U.S. Government laboratories, various research firms and independent laboratories, reactor vendors, utilities, universities. Seven foreign countries are represented on the author list; nineteen countries are among the over 100 foreign registered attendees at last count.

The meeting will feature new and different work this year on the subject of high burn-up fuel behavior, as well as results and techniques for research on severe accidents, primary system integrity, structural and seismic engineering, advanced instrumentation and controls, aging, human factors, thermal hydraulic characteristics of advanced passive light-water reactors, Individual Plant Examinations, and probabilistic risk assessment.

International relationships in nuclear safety research are becoming increasingly important. Nuclear safety is a world-wide need, increasingly so recognized. Much of the research is relevant to reactors in many countries. International cooperative arrangements and international dissemination of knowledge of nuclear safety offer safety benefits of international scope as well as economies through utilization of results from colleagues abroad.

Efforts are under way by Western nations to share nuclear safety practices with the successor states of the former Soviet Union and other states in Eastern Europe and Asia. The USNRC is continuing to work with Russia and Ukraine on nuclear safety research activities under the auspices of the Joint Coordinating Committee for Civilian Nuclear Reactor Safety (JCCCNRS) for which I serve as U.S. Co-Chairman. For example, Working Group 3, initiated in 1989, is continuing to examine the effects of neutron irradiation on the integrity of reactor pressure vessels. Under this Working Group, the U.S. obtained useful engineering information on the thermal annealing of VVER-440s, and has benefited from embrittlement prediction techniques developed by the Russians for their plants. Working Group 12, chartered in 1990, deals with the technical issues related to nuclear power plant aging and life extension. This Working Group provides opportunities to both sides to participate and

interact on a broad spectrum of issues of interest to the utilities, the designers and builders, and the regulators.

In addition, we are providing these countries computer software and hardware plus training so that they can apply NRC-developed safety analysis codes to Russian-designed power reactors. These projects are proceeding under the Lisbon Initiative, which calls for providing assistance in the application of analytical techniques to be used by the safety regulatory agencies of these countries. The NRC has been very active in the planning of the OECD sponsored RASPLAV Program, which is designed to study nuclear reactor core melt/pressure vessel interactions during a severe accident. The experimental program is being conducted in Russia by the Kurchatov Institute under an OECD consortium which includes the NRC.

A number of new bilateral agreements for information exchange and test facility sharing have been signed during the past year -- with Canada, the Czech Republic, Finland, Japan, Korea, Lithuania, the Russian Federation, the Slovak Republic, Slovenia, Sweden, Switzerland, Taiwan, and the United Kingdom. In addition, we have participated in a number of advisory groups within the OECD and the IAEA.

Several of our current reviews for design certification have also involved us directly with foreign research organizations.

Westinghouse's AP600 testing program is conducting thermal-hydraulic loop tests at the SPES facility in Piacenza, in Italy, and automatic depressurization system tests at the VAPORE facility near Rome. Independently of Westinghouse and with Japan's cooperation we have modified the ROSA facility in Japan to conduct our own confirmatory series of AP600 loop tests.

General Electric likewise has international involvement in its SBWR testing program. The PANTHER facility in Piacenza is testing the heat exchangers and isolation condenser for the passive containment cooling system. A similar test series has been completed at the GIRAFFE facility near Tokyo. And SBWR loop tests are now underway in the PANDA facility in Switzerland.

With the recent formal submittal requesting NRC's review and certification of the CANDU 3 design, we have a reactor of foreign design under review for the first time. This obviously brings us into further contact with international research, although the distances are not great here, as most of the supporting experimental work has been done in Canada and will continue there.

We are not only interacting with an international research community in reviewing the experimental test data for the AP600, SBWR, and CANDU 3 designs, but we are also undertaking the analysis of those tests with our own codes to help assess the validity of the vendors' design calculations and supporting data bases.

International cooperation in research offers the significant benefit of bringing the best people to the tasks and the best ideas to bear on the issues addressed. It provides cost sharing and the quickest way to transmit new knowledge. The TMI-2 Vessel Investigation Project, successfully completed last year, is a good example of such a program and its benefits. This project was begun by the NRC in 1988 in cooperation with ten other countries under the auspices of the OECD Nuclear Energy Agency. The project included the recovery of samples from the lower head of the reactor vessel, examinations of the samples, and analyses of results. The results of the TMI-2 VIP significantly increased our understanding of the extent of damage to the reactor vessel lower head and the margin of structural integrity that remained in the vessel during the TMI-2 accident, as well as lower vessel head behavior during severe accidents in general.

The French/Internation PHEBUS-FP Program [FP = Fission Product] of which the U.S. is a member includes severe fuel damage experiments and study of the behavior of fission products during their transport in the reactor and containment systems. This well designed experimental program will provide better information on radioactive-material-release source terms under severe accident conditions. There was good collaboration in planning this research and the experimental work is now well underway. We are enthusiastic about this program and we admire the fine job that our French colleagues are doing.

Our cooperative agreement with the French Atomic Energy Commission (CEA) covering testing of cables for effects of age-related degradation, including testing each other's cables, has been a highly successful program of cooperation in testing and information exchange.

And we are entering a new era of cooperation with research on reactivity transient efforts on high burnup fuel with the CEA in France, JAERI in Japan, and the Russian Research Center. We will, in fact, be hearing papers from all three of these organizations at this conference on Wednesday afternoon.

Our cooperation with Electricité de France in information exchange from operating experience with nuclear power plant equipment is a good example of the value that such exchanges have. We have profited from our discussions with Electricité de France concerning steam generator operating experience at French nuclear power plants, particularly with respect to management of degradation and hydrostatic test data on primary-to-secondary leakage at pressure differentials exceeding design-basis-accident levels.

In summary, I am pleased with the international participation of our research partners at this conference. As Executive Director, I support research with international partners as being both cost effective and safety effective. Further, I consider this meeting to be very important to reactor safety technology research and development, and an excellent opportunity to discuss and disseminate the results. I am particularly happy to welcome Mr. Pierre Tanguy, the Inspector General of Electricité de France for Nuclear Safety, whose work I have admired for years. It is very appropriate for him to be an invited keynote speaker.

22nd Water Reactor Safety Meeting
October 24, 1994
Bethesda Marriott Hotel, Bethesda, MD

Some views on nuclear reactor safety

by Pierre Y. TANGUY[1]
Électricité de France, Paris, France

Introduction

When I came for the first time in this country, I was told that it was a tradition to start any speech with a joke, even when the speaker is supposed to talk about a very serious topic. I was also told that it did not have to be a good one, fortunately. I attended a meeting, not in this country, but in another English-speaking country, where the head of a national nuclear regulatory board, addressing representatives of nuclear operating organizations, began his speech with those words: I am here to help you! Everybody in the audience thought he was just following the tradition, and although they did not think it was a very good joke, there was anyway a polite laugh. When this reaction seemed to come as a surprise for the speaker, the laugh became quite bigger. If the speaker did mean it, then it was a good joke.

Here I am today, speaking at a meeting organized by the world largest nuclear regulatory agency, and I do belong to a nuclear operating organization, Électricité de France, EDF. I will not start by telling you that I am here to help you, or to ask for your help, or anything of this kind. Operating organizations and regulatory bodies have both an essential role in insuring a satisfactory safety level in operating NPP's. They have no other choice than work together, in a more or less conflicting way. It is to be expected that their views may differ on several issues. Today I will give my own views, based on my experience, in EDF and in various international organizations. But first, some words about EDF and my position within the company.

Nuclear power at EDF

EDF, as you probably know, is today the world largest nuclear operator, with 56 PWR's in operation, that have produced last year slightly more than 350 billions kilo-Watt-hours, representing about 78% of the French

[1] General Inspector for Nuclear Safety.

total electricity production. Four more PWR's are under construction, and will be connected to the grid between 1995 and 1998. EDF is also operating a large breeder, Superphenix, that has been the subject of a lengthy debate in France. Because or this high involvement in nuclear power, the cost of electricity in France is one of the cheapest in Europe, and EDF is exporting more than 15 % of its production. The part of national resources in French energy mix is now slightly over 50% when it was around 20% 15 years ago. The CO2 release per capita is the lowest of all industrialized countries. All these arguments are well recognized by the French public, thanks to the advertisement campaigns sponsored by EDF in the past few years. Public opinion polls show that nearly 60 % of all French citizens support the present nuclear development. But of course, any serious threat on the safety of our plants would have tremendous consequences on EDF's image and activities.

No surprise therefore if the safety of its nuclear installations is deemed a key issue for the company. Within EDF, I am General Inspector for Nuclear Safety. I don't think that there are similar posts in other nuclear utilities. My mission is to report to our Chief Executive Officer on the nuclear safety status in our installations. I publish an annual report, where I underline the safety deficiencies I have noticed, and suggest the actions that, in my opinion, would enhance safety. Since the press and the media love hearing about weaknesses, they pay more attention to my report than they do to the many other EDF documents that present our good results, in terms of availability and costs for instance. That does not always make myself very popular inside the company. Nevertheless, at the end of a 10 years mission in EDF, I hope that there are some managers in our organization that consider that my reports have been of some assistance to them. But that might be the same joke again...

Part 1 - EDF nuclear safety status

I will first present some of the key features of my 1993 report. In that report, I gave a rather positive statement about the results obtained by EDF in its nuclear safety policy. I wrote that it had demonstrated its effectiveness in three areas that were in my opinion critically important:

- the implementation throughout the managerial chain of a real safety culture within the teams in charge of building and running EDF nuclear power units,

- a common Franco-German approach for the future, based on the same assessment of safety related questions, and achieving some significant progress on the safety level,

- and finally an effective collaboration with the Chinese agencies responsible for the Daya Bay power plant, with the aim of setting up safety conditions in keeping with international standards.

Since time is limited, I will mainly develop the first aspect, focussing on operational safety, that is our first priority in EDF.

The EDF operational safety results

Efforts have been made in EDF to set up within organizations, teams and individuals, a strong *safety culture.* I think that this phrase is not as commonly used in this country as it is in Europe. You may be aware that it was used for the first time in the International post-Chernobyl meeting that took place in Vienna in August 1986. Two years later, it was identified as one of the most important fundamental principles in the *Basic safety principles for nuclear power plants,* published by the IAEA under the reference INSAG-3. And finally, it was the subject of INSAG-4, another IAEA document elaborated by the INSAG expert group, published in 1991. In its introduction, INSAG-4 states that it is especially directed to the senior management of all organizations whose activities affect nuclear plant safety. This message was well received in EDF. The INSAG-4 report was translated into French. Clear directives have been issued by top management commanding all the staff to give safety its due importance. The message has become louder and clearer with time and has been applied in the field into unequivocal requirements for all staff levels, and with noteworthy progress in 1993.

The progress in the implementation of an efficient safety culture on nuclear sites, and the progress in operational safety, have been simultaneous, even if it cannot be demonstrated that the second is a consequence of the first. The overall balance sheet of nuclear safety at EDF has always been satisfactory: after more than 500 reactor-years experience, EDF modern plants have never suffered a nuclear accident. But it is from the analysis of all incidents that one can try to get an evaluation of the safety level. We have been using in EDF for several years a severity scale for ranking the safety significance of all operational events. It is very similar to the international INES scale. There has been one level 3 incident, in 1989, that clearly indicated that we had to improve the quality in maintenance activities. There used to be in previous years half a dozen level 2 incidents each year; only one was reported in 1993, and I hope that there will not be more than two in 1994. This reduction in safety significant events is in my opinion a valuable indication.

Usual WANO indicators show also clear progress in 1993 and 1994. This is particularly true of availability, more than 80% in 1993, probably around 81% in 1994, when it was only around 71% in 1992. The average collective dose per reactor went down, 2 man-Sievert in 1993 compared to 2.4 in 1992. The frequency of automatic shutdown went also down: 2 per year and per unit in 1993 versus 2.2 in 1992. We are still far from being the best in the world on these two indicators and we have to make more progress; for scrams for instance our aim is to come down to around 1 per unit-year.

The progress on average plant availability factor is also due to good anticipatory actions. They have enabled EDF to avoid in 1993 and 1994 the incidents that had marked the years 1989 to 1991 (maintenance errors on pressurizer relief valves, bad quality control on containment venting circuits, and Inconel stress corrosion phenomena on steam generator tubes and pressure vessel head penetrations). Decisions have been taken concerning early replacements of vessel heads and steam generators. They illustrate our determination to maintain the safety level of our installations throughout their life time. We are certainly not totally protected from unforeseen events in the future, but we have moved forward.

The operational experience worldwide

My annual report specifically addresses EDF plants. When foreign NPP's are mentioned, it is because I consider that the lessons learnt from their experience can be useful to enhance safety in EDF units. After some of my past reports, I received complaints from foreign utilities: excerpts had been incorrectly quoted by their national press, and has hampered their image. Consequently my last report does not mention any names when talking about non-EDF nuclear power plants. And of course, it has been always quite clear that I do not intend to bear any kind of judgment on nuclear safety outside EDF.

Nevertheless, in front of this audience, I wish to say that I am convinced that the optimistic views I have on the safety of EDF plants are also valid for most of the nuclear power plants in operation in Western countries. I have visited many countries during the past ten years. In 1994 I spent two weeks in an American plant, following INPO's invitation. I consider that modern Western plants today are safely operated. Our EDF plants are not the only good ones, and they are certainly not the best of all. Many peer reviews of various types took place around the world in the recent years, and their results confirm my optimistic statement.

Does that mean that we can relax and don't have to worry any more about operational safety, at least in the West? Of course not, and in the second part of my talk I am going to give you my views on what can be done in the future in the field of operational safety.

Part 2 - Actions aimed at enhancing safety in the future

Thinking of EDF plants, we should be attentive to three aspects:

- We must insure that in all operating situations, "As an overriding priority, nuclear plant safety issues do receive the attention warranted by their significance."[2] Such directive should look obvious to all managers, since experience has shown that efforts directed towards safety enhancement are also helpful in getting a more cost-efficient electricity production. Nevertheless, we must recognize that in the daily operation of a nuclear power plant, operators have to make decisions that affect safety and availability in opposite directions. Since nuclear plants are complex machines, it is not so easy for operators to have a full conscience of the potential safety impact of their decisions. In 1994, we experienced two incidents classified on the 2nd level of the INES scale. Both of them were related to inappropriate actions from operators in specific operating phases: plant shut-down with primary water at the mid-loop level, and load following. In each case, long-term potential safety consequences were overlooked. I consider that these incidents indicate that we must remain vigilant if we want to keep *a proper balance between safety and production.* We have to be sure that safety is always present in the mind of all staff.

  Daily experience is very efficient in making clear at all levels that an inappropriate action can have immediate detrimental consequences on operation. But it needs an in-depth analysis to appreciate their delayed safety consequences. Therefore one has to analyze carefully, with the operators involved, all abnormal events that occur in a plant, extending the analysis to the potential risks related to possible development of the accidental sequence. In this way, the operators learn how to look beyond the facts and they get a concrete feeling of potential safety degradations associated with deficiencies in operation. In EDF we have published a specific guide for this task. The most significant events will be used for training operators on simulators. The evaluations of the corresponding severe accident's conditional probabilities will constitute the bases for a precursor study, similar to the NRC study. I consider that this emphasis put on

[2] INSAG-4, definition of safety culture.

experience feedback, accompanied by improvements in the working organization and with a significant increase of the time allocated for simulator training, is the most efficient action that can be done for enhancing the daily safety culture of all staff.

Plant managers have of course a special responsibility in keeping a proper balance between safety and other concerns, such as economics. We all realize the vital importance of the operating costs and availability for the future of nuclear energy. I know that in this country, some utilities have embarked on re-engineering exercises, officially aiming at simultaneously enhancing safety and reducing costs. Many people are thinking of more on-line maintenance to reduce the duration of periodic outages. Clearly these actions can be consistent with the present safety level, and can even improve safety, but only if all operational activities have been carefully analyzed from a risk perspective. When in a plant all responsible managers have a detailed knowledge of the ways in which their task could impact safety, positively or negatively, performance improvements will automatically lead to safety enhancements. But this knowledge is not easy to acquire and has to be periodically refreshed, with the support of all operational experience available worldwide. Retraining of managers at all levels is required.

- The second aspect is related to plant aging. French plants are young, an average of 12 years old for the 900 MW and 6 years for the 1300 MW. When you want to operate a nuclear power plant for a long time, 35 to 40 years, and maybe even more, the objective is not just to insure that its safety does not deteriorate. This is a prerequisite of course, and it justifies early replacements for large components affected by inconel corrosion. Maintaining a constant safety level does also imply an in-depth surveillance programme on all components and systems that are important for safety. In EDF, the long shut-down required by the regulatory authorities after each 10 years of operation is used to have a look at all systems that are not part of the usual inspection programme. The standardized design is of course favorable for such an extensive review.

  But we are also required to proceed every 10 years to a safety re-assessment of each standard, taking into account operational experience worldwide as well as new knowledge obtained in research centers. The ultimate goal of these periodic reassessments is to make sure that when a plant has been operated for a long time, its safety has been improved, thanks to an effective implementation of lessons learnt from experience. There is of course an economic limitation to the backfitting process. We hope we will agree with the regulatory

authorities, that significant modifications will always have to be justified according to their safety merits.

The third aspect is *severe accidents*, that, in my opinion, will always have to be considered as a standing safety issue. Since TMI, we know that so-called *beyond-design accidents* can occur and that such accident, if the sequence is not properly managed in order to be stopped early, can jeopardize the entire nuclear industry. Since Chernobyl, we are aware that if the containment fails completely in case of a severe accident, it is practically impossible to limit its consequences to a level tolerable for the people and their representatives. Probabilistic evaluations demonstrate that we should be well protected against accidents with large radioactive releases off-site. Nevertheless, we also know that our studies are not fully exhaustive. There are also significant uncertainties linked with common mode failures and human factors. Therefore I consider that we must work still more on both aspects: validate on experience the *severe accident management* provisions that have been implemented in our plants, and improve our knowledge on all phenomena that can influence the size of any possible off-site radioactive release. EDF is supporting for instance a research programme performed by the French C.E.A. in the test facility called PHEBUS, in the Research Center of Cadarache.

The importance of improving our basic knowledge

This leads me to mention breifly the safety research programme that EDF considers as a necessary complement to the operation of nuclear power plants. EDF is performing R&D activities inside the company, within its research division. It also sponsors research performed by the C.E.A., either on a bilateral basis, or in the framework of a tripartite agreement with FRAMATOME. Concerning research related only to PWR's, EDF is presently spending each year nearly 500 Million French Francs, more than 90 Million US $, 1/3 in EDF and 2/3 in the CEA. A large part of these research actions is devoted to safety.

I already mentioned the PHEBUS programme that aims at getting a better knowledge of radioactive aerosol releases in case of a core-degraded accident. Many programmes are directly related to the analysis of accidental plant operation. One of them is quite important for us today: called CABRI-REP, it deals with the behaviour of high burn-up fuel during a fast reactivity transient, and its results will be used to get from the regulatory authorities the authorization we need to move to higher burn-ups.

*

* *

Before concluding this talk, I will review the two other aspects mentioned earlier in my presentation.

The safety of future nuclear reactors

On July 1993, the French and German safety authorities published a joint declaration "on a common safety approach for PWR reactors of the future". It refers to the design of power plants that may be in operation at the start of the next decade. I will quote a short excerpt from the introduction:

> "A significant improvement in the safety of the next generation of nuclear power plant appears necessary, compared to existing plants. (...) It is considered that significant progress at the design stage is possible along an evolutionary path, giving appropriate consideration to the lessons learnt from operating experience and probabilistic studies performed for existing power plants"

The level of safety aimed at can be summarized in three points:

- the overall probability of a core meltdown accident must be less than one in a hundred thousand per reactor per operating year, *taking into account all uncertainties and all types of failure and hazards;*

- radioactive substances released in the event of an accident must be limited: if there is no core meltdown, it should not be necessary to provide protective measures for neighbouring populations; in the hypothesis of a *low pressure* meltdown the measures should be very limited in space and in time; the other types of severe accidents should be eliminated by design

- during normal running, the doses of radiation received by the staff, the quantities of radioactive waste and effluents, and the possibilities of incidents occurring as a result of human error, must be kept to a minimum.

On September 1993, the main options selected for the nuclear island of the project known as EPR (European Pressurized Water Reactor) were presented by three partners: EDF, a consortium bringing together nine German producers of electricity, and a consortium of constructors made up of Siemens/KWU, Framatome, and their joint subsidiary Nuclear Power International. Detailed discussions with the safety authorities of both countries started soon after and went on during the year 1994. Their outcome is foreseen for next December. I am confident it will

confirm that the options are in keeping with the safety objectives. This will be an important step towards a European safety harmonization.

Efforts are under way to come now to some common bases between Europe and USA. On the utility side, we intend to proceed to a detailed comparison between the Utility Requirements for Advanced Light Water Reactors published by EPRI a few years ago, and the European Utility Requirements presently in an early stage of elaboration. There are obviously many similarities, since EDF and other European utilities had been associated to the EPRI action. On the regulatory side, I hope that a consensus could be reached at least on safety targets, and on some fundamental technical issues. The results achieved already between France and Germany is a good sign for a future success.

EDF cooperation with Chinese utility on Daya Bay

The startup of the first unit of the Chinese Daya Bay power station was in my opinion an important event in 1993. Clearly the responsibility for the safety of this power plant rests with the Chinese utility, controlled by the national Chinese safety authority. The safety of Daya Bay nevertheless is of interest to EDF on two counts: the nuclear island is that of a 900 MW plant series, and EDF, who carried out the overall engineering work, has been helping the utility during construction and commissioning.

I had the occasion a year ago to spend several days on the site and to talk with the Chinese utility and with the EDF staff who are helping them. The Chinese authorities are determined to show to the world nuclear community their capacity to run a power plant *in strict compliance with international safety standards*. They have already demonstrated that they are opened to the outside world, by calling on foreign consultants to check the quality of the work and by asking the IAEA for regular OSART mission visits. The two units have been now operating for some time at full power, with satisfactory operational results, and it seems as if all Chinese organizations were maintaining their policy of transparence.

When thinking about the safety difficulties encountered by nuclear power plants operated in the Eastern Europe, the Western cooperation with these countries could aim at achieving the same type of result that is looked for in Daya Bay. Of course, there are specific problems related to the design and to the construction quality in Eastern nuclear power plants, either VVERs or RBMKs. But cooperation on operational safety will contribute significantly to the enhancement of their safety.

CONCLUSION

Even when their overall results are good, all nuclear power plants expect to encounter some kind of difficulties in the future. Past experience gives us some clues for the right way to get over them. I wish to emphasize three orientations:

- consolidate safety culture, everybody being deeply aware of the way in which his task is related to plant safety,

- try to take more into account the risks involved, thanks in particular to improvements in knowledge, from research and from experience,

- stay open to other viewpoints, internally and internationally.

Prospects for Nuclear Safety Research

Eric S. Beckjord, Director
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission

22nd Water Reactor Safety Information Meeting
Bethesda, MD
October 26, 1994

NOTE: The views expressed in this talk are mine and they do not necessarily represent the NRC.

Introduction

I am pleased to speak at this luncheon of the 22nd Water Reactor Safety Meeting in your presence as important members of the U.S. and international safety community. This is the 9th such meeting since I became Director of Research at NRC, and an appropriate occasion to talk about reactor safety, the contribution of reactor safety research, and prospects for safety research in the years to come.

Reactor Safety 1979-1994

The Three Mile Island Unit 2 accident raised major concerns about nuclear reactor safety in this country and abroad, and led to a widespread review of plant performance and safety requirements by NRC. As a result there were many improvements made to emergency safety systems, control rooms and instrumentation, and operator qualifications and training. There is no question that plant safety has improved as a consequence.

Plant owner/operators have made safety improvements. One example is the reduction of the number of automatic reactor trips. They accomplished this by
SLIDE 1 systematic review of plant conditions at the time of the trip, determination of the root cause, and, if the trip was not needed for safety, correction so that the condition will not reoccur. Unnecessary trips are a challenge to safety systems, and reducing unnecessary challenges is a safety improvement. This bar chart from the INPO 1993 Annual Report shows the record of progress in reactor trips.

Reactor safety research conducted by the NRC has also made important contributions to safety over the same period of time. There is, however, no simple measure, such as a numerical performance indicator, to show the improvement. Nevertheless it is possible to explain causes of safety improvement in meaningful terms. Here are four examples which have made a difference.

1. Reactor Vessel Research

Reactor vessels are vital not only in normal operation, but also in accidents wherein they must retain water for the purpose of core cooling to prevent fuel melting. Exposure of the vessel to neutrons throughout its life causes changes in the vessel steel. The most important changes are the increase of the nil ductility transition temperature or embrittlement, and the decrease in the ductile fracture toughness of the vessel and exposed welds. As vessels age, the effects of these changes become greater. Pressurized Thermal Shock (PTS) is an important safety issue arising from these changes. An example of PTS would be the actuation of a PWR safety injection system during a small break LOCA, as a result of which the reactor vessel temperature could drop quickly while the system is still pressurized: hence the term PTS. Reactor vessel research has concentrated on understanding the changes in order to establish safe limits to operation, and on the effectiveness of reactor vessel annealing when a vessel reaches the limits in order to restore the properties it had when it was new.

Had this research not been carried out, knowledge of these limiting conditions on reactor vessel operation would not be known, and it would have been necessary to shut plants down on the basis of conservative estimates. Because of this research plants will be able to operate safely longer. I am talking about years of additional operation. Also, when the time comes, plants should be able to take advantage of reactor vessel annealing.

2. Probabilistic Risk Assessment

Probabilistic Risk Assessment, an idea proposed by Dr. Reginald Farmer in 1958, came to fruition in the 1975 Reactor Safety Study (WASH-1400). Unfortunately at that time its usefulness was not widely appreciated. Confidence in PRA increased gradually as a result of improvements and application to 30 or more plants. In 1990 NRC completed a 6 year study with major improvement of methods in the report on Severe Accident Risks (NUREG-1150). The Individual Plant Examination program using NUREG-1150 methods and now approaching completion will provide a PRA study of every plant in the U.S. (except 1). In the course of the IPE every plant has made safety improvements as a result of discovery of accident vulnerabilities. This achievement is the direct result of NRC research and development of PRA, and its application by U.S. nuclear utilities. This is the first point I wish to make on PRA.

The second point is that we can use PRA to measure the effectiveness of safety research.

SLIDE 2 This slide shows the core damage frequencies (CDF) for PWRs from three sources: WASH-1400 (Surry), NUREG-1150 (Sequoyah, Surry, and Zion),and the Individual Plant Examination (IPE) PWRs (42 plants). I want to compare first WASH-1400 and NUREG-1150 CDFs, and second NUREG-1150 and the IPE. The WASH-1400 and NUREG-1150 values are almost the same, but major changes took place during the intervening 15 years between the studies: the NUREG-1150 analysis included many accident sequences not considered in WASH-1400, and many improvements were carried out on plant equipment as vulnerabilities were discovered. The NUREG-1150 CDF incorporates both. Consequently the comparison with WASH-1400 is not valid, and I assert that a reanalysis of the Surry CDF as it was at the time of WASH-1400 would in fact be substantially greater than the WASH-1400 value of 6×10^{-5} per reactor year. The difference between a revised value and the NUREG-1150 value would be a measure of the benefits attributable to the changes put into effect in large part due to the PRAs, and also to post TMI fixes. Doing this task today would take a lot of digging into records, and is perhaps not worthwhile, but I believe this kind of analysis should be done in the future, because it can measure the effectiveness of safety improvements derived from research. It will be helpful in budget justification.

The second comparison, i.e., of NUREG-1150 and the average of the IPE PWR CDFs is valid, because the IPE methods were based on NUREG-1150 methods, and because most of the IPEs submitted by the plant owners are of high quality. I conclude from the comparison that the IPE and the changes resulting from it have been very beneficial from the point of view of safety, confirming the first point on PRA that I made.

3. Severe Accident Research - Direct Containment Heating (DCH)

Direct Containment Heating is the challenge to a containment building of high pressure melt ejection from the reactor vessel of a PWR during the station blackout sequence. Research took two approaches to this issue. The first was in NUREG-1150, a probabilistic approach. The conclusion was that the risk of this sequence is low, because it is very unlikely that the primary system would be at high pressure at the time of reactor vessel failure, for the reason that the pressurizer surge line or the hot leg would fail early in the sequence because of very hot gas flowing through the relief valve, causing pipe failure on the way.

The second approach to resolution of this issue was to perform tests of the DCH phenomena and sequence in 3 facilities: 1/6, 1/10, and 1/40 scale tests. The tests and their analyses showed that the likelihood of containment failure, given the event itself, is very low for PWRs such as Zion (6 plants) and Surry (10 plants), because most of the melt is caught in the compartments along the path and does not reach the containment free volume. The conclusion of this research is that the existing Westinghouse large, dry PWR containment building plants have adequate margin in their design basis to withstand the challenge of this unlikely beyond design basis accident. As a result of this finding, there is no need for additional measures to protect against DCH.

4. Advanced LWR Research

In 1990 General Electric and Westinghouse initiated applications for certification of their advanced passive LWR concepts, the SBWR and the AP600. Because of novel features of the passive ECCS systems for these plants, for which there were no performance data available, the NRC initiated confirmatory research of these systems in order to provide assurance that they would operate effectively in accident conditions. The research programs are now underway, with construction of a scale model test facility for the SBWR at Purdue University, and the conversion of the LSTF thermal-hydraulic test facility at the Japan Atomic Energy Research Institute to provide a scale model of the AP600. Testing began in January of this year at the latter facility. The AP600 tests in Japan have already provided important data on the AP600 scale model, making it possible to test the thermal hydraulic codes that will be used for licensing the AP600. The AP600 scale model tests, though not yet complete, are a major contribution, along with separate tests by Westinghouse to proof of safety, and thus an important safety research accomplishment.

These few examples, I think, illustrate clearly major contributions of research to reactor safety.

I have been talking mostly about NRC research accomplishments, and now I want to talk about the broad prospect ahead for nuclear safety research, and not just NRC research. Because the demand for this research is linked to the general prospect for nuclear energy in the U.S., it is helpful to see how it might evolve, and specifically whether it will decline, remain stationary, or grow. I do not predict but rather look at certain indicators, which taken together can point out a favorable trend, or the contrary.

Nuclear Energy Prospects in the U.S.

SLIDE 3 The indicators selected are shown on Slide 3, and I define them briefly as follows:

Resource Base:	domestic uranium resources
Policy:	totality of local, state, and national requirements to build and operate a plant
Economics:	competition with other energy generation sources
Environment:	effect of plant operation on air quality and atmospheric carbon dioxide

For nuclear energy these four indicators are not controversial and for the most part factual. The remaining four also have a factual basis, but are more controversial, and public perception of them, which may differ from fact, is more important. The definitions of these are as follow:

Waste Disposal:	public acceptance of nuclear waste disposal
Nuclear Proliferation:	perception of link between nuclear fuel cycle and weapons
Health and Safety:	public concern about health and safety of nuclear plants
Renewable Energy:	perception of abundant sources just around the corner

Although public perception is generally slow to change in a direction favorable to nuclear energy, it can change suddenly in an unfavorable direction, as in the case of Health and Safety after Three Mile Island.

SLIDE 4 I now compare these indicators as perceived 15 years ago, today, and how they might be over the coming 15 years. In 1979 after Three Mile Island there were just two that were favorable: Resource Base and Economics. Plant capital and operating costs were under reasonable control, and nuclear electricity was competitive with the alternatives. Renewable Energy was a nascent issue then. All other indicators were unfavorable to nuclear generation, and especially Health and Safety because of the TMI accident. So too was Nuclear Proliferation, until the public recognized that the LWR once-through fuel cycle was not prone, in the absence of clandestine reprocessing plants, to proliferation. As is evident from the tally, the totality of indicators did not favor nuclear energy in 1979, with 5 out of 8 unfavorable.

Today the tally components differ somewhat from 1979. Health and Safety is a non-issue, that is to say neither favorable nor unfavorable, because of improved plant performance, and the passage of time since TMI. Economics has

turned unfavorable for several reasons. Increasing operating costs of nuclear plants make them less competitive, and cheap natural gas is available on 10 year contracts for low capital cost gas turbines, or combined cycle plants. Also, it is a fact that base load plant construction of any kind is at a standstill. The bottom line of the 1994 tally is little changed from 1979 and unfavorable to new construction.

What about the future? Watch the indicators. It is important to look ahead and see what the future may bring. Both the nuclear industry and the regulators must plan for future needs. My view is that major changes in the indicators could occur in the coming 10-15 years. The test for Renewable Energy will be cost competition with base loaded thermal plants for new construction. The question will be how much of a premium will the public be willing to pay for Renewable Energy. With the advent of advanced passive LWRs, Health and Safety could become favorable to Nuclear Plants. I do not expect Waste Disposal to turn favorable to nuclear power in this period, but it is possible that it could become less controversial or a non-issue, if the development of the Yucca Mountain repository or an alternative shows success. The Environment, in the event of resolution of the effects of carbon dioxide release, will favor nuclear energy. Policy also could shift: plants can be constructed in 6 years, and policy changes could reduce the long lead times; the NRC's Part 52 Rule for Standard Design Certification is important in this respect.

Economics is a big question mark primarily because of the future availability of cheap natural gas. We know that gas price is inelastic for increasing demand beyond transmission capability. Furthermore, conventional wisdom looks to a continuation of technology improvement in searching for and developing new resources. If conventional wisdom is wrong and gas prices rise, Economics could swing in favor of nuclear energy. Finally, the Resource Base could become a more decisive consideration than it is today, particularly if natural gas imports from Canada and Mexico rise: In that event, the large U.S. resource of uranium is likely to be recognized.

So, watch the indicators!

Future Nuclear Safety Research

What research is likely to make a difference in years to come? Here I refer to research again broadly, not simply NRC research. One way to answer the question is in terms of the indicators. In this context the eight again can
SLIDE 5 be separated in 2 groups, as shown in Slide 5.

The first five, i.e. Resource Base, Policy, Environment, Renewable Energy, and Nuclear Proliferation, are externalities, because developments and changes in whether they will be favorable or unfavorable will take place without strong linkage to LWR development. The last three are linked to technology development, and are the areas where research can make a difference.

1. Economics. This is the province of nuclear development which the nuclear industry supports. Although it is not in a strict sense nuclear safety research, I mention it, because I believe that performance

improvement can never be completely separated from safety, and it should be carried out in the context of meeting recognized safety goals. Performance improvement means increasing availability, controlling operation and maintenance cost, and fuel cycle improvement. For advanced design extending the design life of systems and components, and reducing capital cost are also important. Improvements in any one or all of these factors can improve the evaluation of nuclear plants in comparison with competitors.

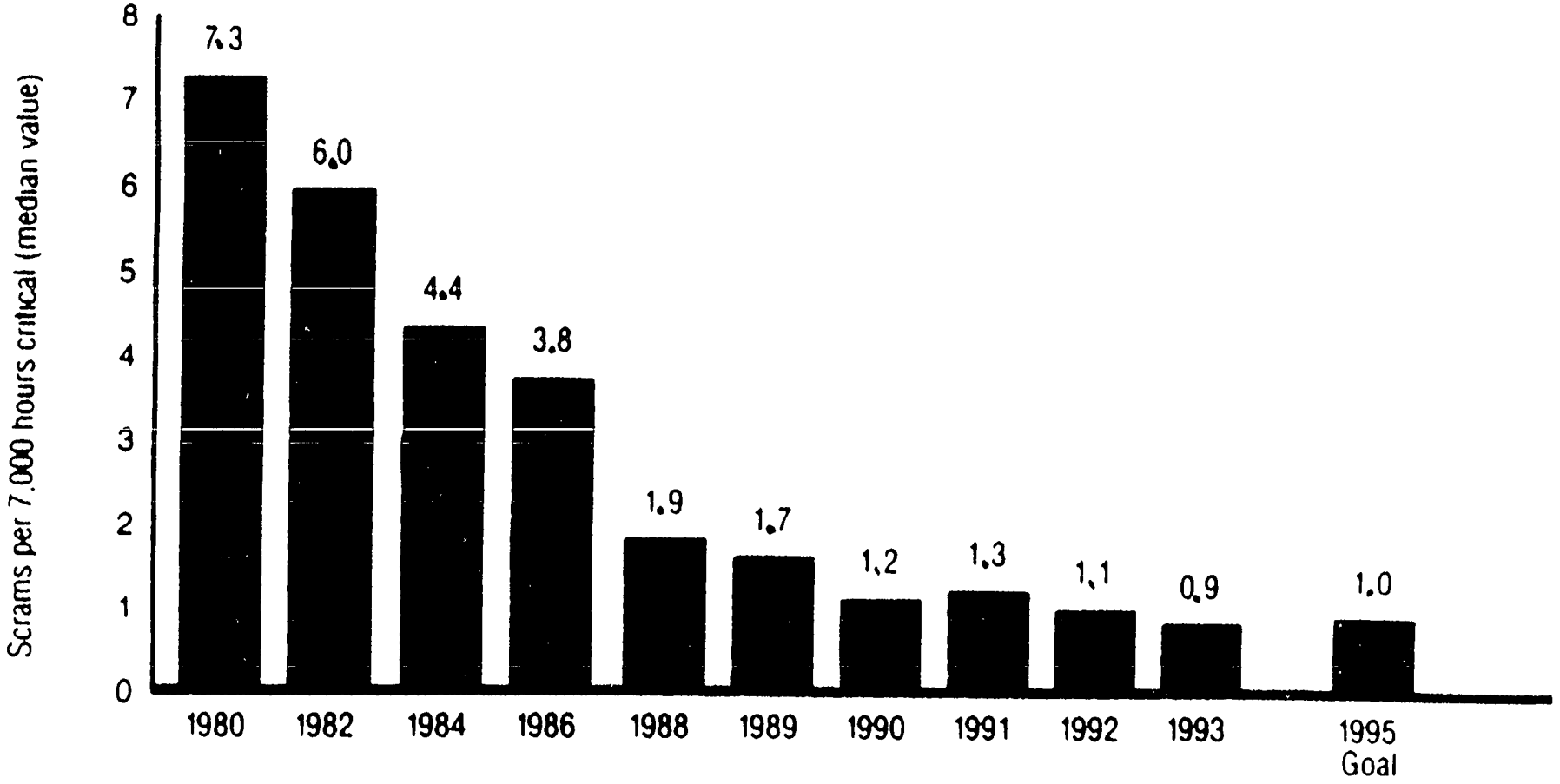
2. Waste Disposal. The policy change that set LWRs on the course away from reprocessing and toward the once-through fuel cycle took place 20 years ago. I do not think that anybody anticipated in 1975 that it would take 20 years and more to resolve the issue of spent fuel storage, and the issue is far more pressing today than it was then. The issue is in part amenable to resolution by science and technology, and in part depends on a change in public perception: the NIMBY syndrome. Science and technology are at work on deep geologic storage, and on development of enduring encapsulation. My position is that there should be enough flexibility in the process leading to actual storage of spent fuel, so that there is room for trial, error, and correction, an essential step in all of science and engineering, without which we may have a Catch 22: to do a job, you first have to prove it; you cannot prove it if you cannot try it.

3. Health and Safety. Operating reactors are demonstrably safer than they were 15 years ago, through the effort of reactor operators, the NRC, through research by the industry and NRC, and through international connections in all these activities. It is important to maintain safety of operating reactors, through their remaining life, including license renewal. That is likely to be 30 to 50 years or more into the future. We have learned much about aging mechanisms and managing them, but important tasks remain, such as improved non-destructive testing to detect flaws and to indicate the remaining life of primary system components, steam generator tubes, and safety related electromechanical equipment, such as pumps and valves. We should understand that the 1500 reactor years of operation now behind us came from new and middle aged plants, but little or none from plants near the end of their design lives. Therefore, we should be ready for surprises as operating plants reach the end of their life. Doing this requires that we maintain an active aging phenomena and management program.

The ALWR developments and reviews are preparation for tomorrow: they lead to new and improved standard designs. When the process is complete I think the PRAs of these advanced designs will show significantly lower CDFs and risks than the currently operating plants. On the systems side the research is not yet complete, and there is more to do on passive ECCS performance, containment cooling during accidents, and instrumentation and controls. There is also a need for more work on human decision making and reliability, and on the effect of organization and management on safety. It is important now to carry through and complete the work so that all important safety issues for these new

plants are resolved, and so that there are no big questions left on the table that could hang over licensing and operations for the future.

So I say to you there is plenty of important nuclear safety research to be carried out. There are 109 operating plants in the U.S., and there are many nuclear power plants operating in countries where rapid societal changes are taking place and the institutions responsible for nuclear safety need strengthening. Research has a role to play in this activity. For these reasons I believe nuclear safety research is justifiable, although full funding for it will be harder to obtain than in the past. It will be the responsibility of those who plan and lead the research to make the case for it effective, and, with the researchers, to see to it that the research produces useful results.



(INPO 1993 ANNUAL REPORT DATA)

SLIDE 1

CORE DAMAGE FREQUENCY (EVENTS PER REACTOR YEAR)

	WASH-1400 (1975)	NUREG-1150 (1990)	IPE (1994)
PWR	6×10^{-5}	5×10^{-5}	8.4×10^{-5}

Nuclear Energy Climate Indicators

Mostly matter of fact:

- Resource Base
- Policy
- Economics
- Environment

Highly perceptual:

- Waste Disposal
- Nuclear Proliferation
- Health and Safety
- Renewable Energy

SLIDE 3

Factors in Nuclear Energy Decision-Making

	1979	1994	2000-2009
Resource Base	F	F	F
Policy	U	U	F*
Economics	F	U	
Environment	U	U	F*
Waste Disposal	U	U	N*
Nuclear Proliferation	U	N	N
Health & Safety	U	N	F*
Renewable Energy	N	U	F*

F FAVORABLE TO NUCLEAR ENERGY
U UNFAVORABLE TO NUCLEAR ENERGY
N NON-ISSUE FOR LWR ONCE-THROUGH FUEL CYCLE
* POTENTIAL OR POSSIBLE SHIFT OVER NEXT 10-15 YEARS

INDICATORS

EXTERNALITIES

- RESOURCE BASE
- POLICY
- ENVIRONMENT
- RENEWABLE ENERGY
- NUCLEAR PROLIFERATION

AMENABLE TO IMPROVEMENT

- ECONOMICS
- WASTE DISPOSAL
- HEALTH AND SAFETY

SLIDE 5

A CONFIRMATORY RESEARCH APPROACH TO THE MEASUREMENT OF EMI/RFI IN COMMERCIAL NUCLEAR POWER PLANTS*

Stephen W. Kercel
Oak Ridge National Laboratory
Oak Ridge TN 37831-6318

ABSTRACT

The Oak Ridge National Laboratory (ORNL) is conducting confirmatory research on the measurement of electromagnetic/radio frequency interference (EMI/RFI) in nuclear power plants. While it makes a good beginning, the currently available research data are not sufficient to characterize the EMI/RFI environment of the typical nuclear plant. Data collected over several weeks at each of several observation points are required to meet this need. To collect the required data, several approaches are examined, the most promising of which is the relatively new technology of application specific spectral receivers. While several spectral receiver designs have been described in the literature, none is well suited for nuclear power plant EMI/RFI surveys. This paper describes the development of two receivers specifically designed for nuclear power plant EMI/RFI surveys. One receiver surveys electric fields between 5 MHz and 8 GHz, while the other surveys magnetic fields between 305 Hz and 5 MHz. The results of field tests at TVA's Bull Run Fossil Plant are reported.

1. INTRODUCTION

Electromagnetic and radio frequency interference (EMI/RFI) are known to cause upsets and malfunctions in safety related instrumentation and control (I&C) systems [Cir 86, Ewi 94]. Systems can be designed to withstand exposure to EMI/RFI, but the cost of a system can increase rapidly as its EMI/RFI immunity increases [Ott 88]. Thus, the designer of I&C systems is faced with the difficulty of hardening the system enough to withstand any EMI/RFI effects that the system is likely to encounter. At the same time, it is undesirable to include more EMI/RFI immunity than is really needed, as this can lead to dramatic and unnecessary increases in the cost, complexity, and size of the system.

EMI/RFI becomes a particular concern as nuclear plant I&C systems designers begin to use digital circuitry [Ewi 92]. As the digital state of the art progresses, clock rates become faster and logic levels become lower. In practical terms, the more modern the digital system, the smaller is the logic pulse, in both the time and voltage dimensions, and consequently, the greater the likelihood that a pulse can be corrupted by EMI/RFI. To minimize the effects of EMI/RFI, good electromagnetic compatibility (EMC) design and installation procedures must be used. However, what is good EMC design?

*Research sponsored by the Nuclear Regulatory Commission and work performed at Oak Ridge National Laboratory, Oak Ridge, Tennessee, managed by Martin Marietta Energy Systems, Inc., under contract DE-AC05-84OR21400 with the U.S. Department of Energy.

In several recent instances, utilities have conducted an EMI/RFI survey of the proposed location of digital equipment to demonstrate to the Nuclear Regulatory Commission (NRC) that ambient levels are substantially below the withstand level of the digital system upgrade [EPR 94]. Many within the industry consider it unnecessary and prohibitively expensive to perform an EMI/RFI survey for each instance and location where a digital system is to be added. Hence, there is considerable interest in establishing a technically well founded design guideline that will eliminate the need for these surveys.

To assist in the process of establishing good EMC engineering practices, EMI acceptance criteria should be determined for the nuclear industry. The Oak Ridge National Laboratory (ORNL) is currently helping NRC to establish a technical basis for acceptance criteria. This assistance consists of both an exhaustive survey of existing standards and practices, as summarized by Ewing et al., and confirmatory experimental research as the need arises [Ewi 92].

Good EMC engineering practice for safety related I&C systems in nuclear power plants is dominated by the question, what field levels should the system be able to withstand? Trying to answer this question leads to another, what are the ambient field levels typically found in a nuclear power plant? This leads to further questions. How is EMI/RFI distributed as a function of frequency? How often do significant EMI/RFI effects occur? How are they distributed in time? Are they roughly evenly spread, or do they occur in isolated clusters in time? Do these distributions vary significantly among plants? As NUREG/CR-5941 states, insufficient data are available to answer these questions from the existing literature [Ewi 94].

This paper examines the present state of research, and what is needed to supplement the currently available data. It considers the alternative techniques for monitoring EMI/RFI in safety related environments, and determines that application specific spectral receivers are best suited for nuclear power plant monitoring. It describes the development and field testing of two devices, one to monitor electric fields, and another to monitor magnetic fields.

2. CURRENT STATE OF RESEARCH

2.1 EMI Measurements in Nuclear Plants

The Electric Power Research Institute (EPRI) recently completed the only systematic and extensive study of EMI/RFI levels in nuclear power plants that has ever been undertaken [EPR 94]. The investigators developed a generic test procedure consisting of six types of measurements based on military standards [MIL 93]. They did the generic measurements in various locations at six different nuclear power plants. The data are reported as a set of "worst case" observations. The implicit assumption throughout the EPRI report is that EMI/RFI levels at each location do not vary significantly over an extended period. While not explicitly stated in the report, the actual test data seem to consist primarily of short duration (on the order of hours) spectrum analyzer readings for various combinations of the six generic tests at each location.

The EPRI study led to several major findings. EMI/RFI levels vary sensitively with location, and consequently, the measurements should be taken at the location of the digital equipment. Above 60 Hz, worst case low frequency conducted emissions at all six plants were at least 20 dB below the EPRI recommended susceptibility level of 142 dBμA. Worst case high frequency conducted emissions at all six plants were at least 10 dB below the EPRI recommended susceptibility level of 103 dBμA. Worst case low frequency radiated emissions at all six plants were at least 12 dB below the EPRI recommended susceptibility level that declines logarithmically from 180 dBpT at 30 Hz to 116 dBpT at 40 kHz. Worst case high frequency conducted emissions at all six plants were at least 42 dB below the EPRI recommended susceptibility level of 140 dBμV/m. Worst case transient conducted emissions at all six plants were at least 25 dB below the EPRI recommended susceptibility level of 158 dBμA. The study provides a systematic body of data urgently needed by the industry, and not previously available.

There is a need to confirm that the results determined by industry studies completely characterize the EMI environment in NPP. The existing data consists of a series of spot checks of limited duration which are assumed to have captured the worst case values. Industry studies do not provide information on how EMI/RFI varies over an extended period, and they do not address the issues of the rate and distribution of EMI/RFI occurrences raised in Section 1 of this paper. To answer these questions, supplemental information is needed.

2.2 Measurement Techniques

As in the EPRI study, safety related EMI/RFI measurements in other industries are frequently done with a spectrum analyzer. EMI/RFI effects can be especially crucial in hospital operating rooms, where an EMI/RFI induced failure can directly lead to the loss of life, and electric fields emanating from medical equipment can be very high, as much as 44 Volts/meter (V/m) [Nel 94]. Similarly, the operation of high speed railroads is highly automated, depends critically on reliable communications, and occurs in an extremely noisy EMI environment [Gra 94]. An EMI/RFI induced train wreck can lead to extensive loss of life and massive property damage.

In the EPRI study, the hospital study, and the railroad study, a spectrum analyzer was used. Data collection for all three studies required elaborate experimental setups, with many accessories needed to process the EMI/RFI emanations into a form acceptable to the spectrum analyzer, and other accessories to capture the spectrum analyzer output. All three studies required an operator to be present throughout the course of the data collection, and each produced a torrent of raw data that required extensive post-processing.

While this kind of observation may provide a complete picture of EMI/RFI in a surgical operating room or a railroad locomotive, it is unlikely to do so for a nuclear power plant. Both a surgical procedure and a train trip between New York and Washington have in common the fact that either can be completed in a few hours. Consequently, it is practical to keep the experimenter on hand throughout the trip. Both have in common the fact that possibly disruptive levels of EMI/RFI occur almost continuously throughout the duration of the trip. Thus, it is desirable to keep a detailed record of all the occurrences of EMI/RFI for subsequent analysis. Finally, both have in common the fact that

in neither setting is human error a major cause of EMI/RFI occurrences. Therefore, the mere presence of an outside observer does not reduce EMI/RFI.

Contrast this with the situation in a nuclear plant control room. The operating cycle lasts for months rather than hours, and continues around the clock. It would be extremely expensive to have three shifts of experimenters to collect many weeks of EMI/RFI data with a spectrum analyzer at each observation point. In addition, EMI/RFI events in nuclear plant control rooms are rare and intermittent. Most of the time, the EMI/RFI levels are below the noise floor of the monitoring equipment. To hold the recorded data to a reasonable volume, the monitoring equipment must be set up to recognize and discard the "zero" readings, merely noting how many occurred. Finally, it must be recalled that a cause of EMI/RFI in nuclear power plants is human error, such as the unauthorized operation of a handheld transceiver; the mere presence of an outside observer induces the power plant staff to be on its best behavior, and thus reduces the number of EMI/RFI events. (Note: Our experience at power plant sites suggests that an unattended and unadorned gray box quickly fades from the notice of power plant staff, who go on about their business as if it were not there.)

A spectrum analyzer is designed to be used as a diagnostic or troubleshooting device. Given that a disruptive EMI/RFI level is known to exist, a spectrum analyzer in the hands of a skilled operator is the ideal tool to track down the source. However, when utilized for ambient surveys, the spectrum analyzer is awkward and unwieldy, requiring an elaborate hardware setup and a human attendant. While better than no tool at all, it is not the right tool for the job. It is reasonable to ask if another tool might not be better suited to the job of observing EMI/RFI effects over the long term.

Dosimetry might seem a possibility. A dosimeter is a broadband electromagnetic monitoring device designed to measure the exposure of humans or equipment to electromagnetic energy. For example, the Personal RF Dosimeter developed at ORNL measures the exposure of sailors on an aircraft carrier deck to RF fields over an extreme bandwidth [Roc 90]. Similar devices, operating over a narrower bandwidth, measure exposure to near field effects by considering electric fields and magnetic fields simultaneously [Bab 86, Asl 87]. Dosimeters typically are concerned with the total energy resulting from the exposure; in effect, they measure average rather than peak effects. Magnetic field measurement techniques use a shielded loop antenna and rudimentary processing circuitry [Mis 93]. In dosimetry, for both electric and magnetic effects, detection (usually by a hot carrier diode acting as a rectifier) takes place directly at the antenna, and frequency information is thereby discarded before the signal arrives at the processing circuitry.

There are alternatives to the antenna-rectifier scheme for observing electric fields. A recent development in electric field detection is the photonic probe [Mas 89]. These devices depend on phenomena such as the Pockels effect to change the optical properties of dielectric materials as a function of electric field. Typically these have a noise floor at 7 V/m, and are therefore only suitable for observing strong field effects such as electromagnetic pulses that result from nuclear explosions. They are not suitable for power plant ambient monitoring, where the field strengths are usually far less than 10 V/m.

Similarly, there are alternatives to loop-rectifier schemes for observing magnetic fields. Active magnetic sensor elements, featuring wide bandwidth and high dynamic range are being explored [Eum 93]. The technology does not appear to be sufficiently mature for power plant monitoring.

Research in broadband monitoring has recently been done by Gassmann and Furrer [Gas 93]. Their system was designed to measure extremely strong fields (up to 1500 V/m and 6 Amps/meter) in the presence of high powered transmitters. While the system has excellent bandwidth and dynamic range, it does not preserve frequency information.

Dosimeters are fast and cheap. They are useful if the frequency of the EMI/RFI signal is already known, or if the knowledge of frequency does not matter. Dosimeter designs are frequently reported in the literature. Commercial models are much cheaper than spectrum analyzers. Most dosimeters respond to average effects rather than peak effects. However, a digital system is disrupted by the *peak* value rather than the total energy of an EMI/RFI event. Thus, the data produced by dosimeters are not a good predictor of whether or not the observed event is likely to disrupt a digital system. Often, dosimeters respond only to a very strong field; they are typically not sensitive enough to measure ambient EMI/RFI effects in a power plant control room, and there is no practical way to increase their sensitivity.

If neither the spectrum analyzer nor the dosimeter is well suited for long term ambient EMI/RFI surveys, is there another instrument that can serve this purpose? The EMI/RFI (or spectral) receiver is the right tool for the job, but available commercial models are not quite suited to this particular task. Hewlett Packard has released specifications for the HP 8546A EMI/RFI Receiver [Hew 93]. The system costs about $65,000, excluding antennas. The specification sheet suggests that it is designed primarily for testing of personal computers for compliance with EMI/RFI regulations issued by various licensing authorities. Because the system features many external controls and several fascinating displays, it is not well suited for long term unattended monitoring in a nuclear plant control room environment. Very recently, Electro-Metrics of Amsterdam NY has published the principles of design of EMI/RFI receivers, but their paper does not include the description of a specific product [Sik 94].

A spectral receiver, customized for long term unattended operation, is the right tool for the job of nuclear power plant EMI/RFI ambient monitoring. Unlike dosimetry, it can preserve frequency information and be made sensitive to low field strengths. Unlike the spectrum analyzer, it does not require an elaborate setup, and can be designed to operate unattended for an extended period. The practicality of using spectral receivers to do the job, the unavailability of suitable devices in the commercial market, and need to collect long term nuclear plant site data, have led ORNL to develop and construct two different kinds spectral receivers, one for high frequency electric fields, and the other for low frequency magnetic fields.

3. SPECTRAL RECEIVER DESIGN REQUIREMENTS

The spectral receivers, or monitors, constructed by ORNL for NRC, are being deployed for automatic, unattended recording of EMI/RFI levels at nuclear plant sites. They are unattended in the sense that no human operator is required while the monitor is making its observations. They operate in the presence and plain view of nuclear plant employees; to reduce the temptation of tampering or mischief, the monitors are unadorned gray boxes, with no external displays, and no external controls except a key lock "off/on" switch whose key can be removed in either setting. The areas to be monitored include turbine rooms, and the monitors must be physically robust enough to withstand extended exposure to an industrial environment.

The monitors must be unobtrusive. Other than sensing the ambient levels of electromagnetic fields, and taking operating power from the plant power system, they do not interact with the nuclear plant environment. They are EMI/RFI hardened; no radiated energy should enter the monitors except through the antenna, and no signals generated by the monitors should escape. The monitors are not intended to be connected to the plant data acquisition system.

While it would be desirable for the monitors to be battery powered, and independent of the plant power system, they require several continuously running active analog elements. To run completely unattended for several months would require enormous (roughly several hundred pounds) batteries with capacities of hundreds of ampere-hours. For a practical system, the tradeoff is between two alternatives. One is to have the monitor battery powered, isolated from the plant power system, but requiring the battery to be replaced every day. The other is to have the monitor powered from the plant power system by a well shielded power supply, and show with test data that the monitor does not interfere with the operation of plant equipment.

The ORNL monitors are capable of unattended operation for several months. They include an onboard uninterruptible power supply, and can withstand a power interruption of up to 20 minutes. In addition, the recorded data are stored on an onboard floppy disk every six hours. Thus, even in case of a major failure, most of the recorded data would be preserved.

The frequency range to be covered is 305 Hz to 8 GHz. This range is determined primarily by MIL-STD-461C, Requirement RS01 (low end) and RS03 (high end) [MIL 93]. As an example of the real-world EMI/RFI environment in an electric utility, consider that the Tennessee Valley Authority (TVA) uses power line carrier (PLC) communications in the 30-300 kHz band, and some PLC below 30 kHz. TVA uses microwave intersite communications in the 7-8.2 GHz band. In addition, there is a risk of EMI/RFI from other low frequency sources such as video monitors [Nic 93]. It was found to be impractical to build a single device to cover the desired frequency range. Two monitors, the magnetic spectral receiver covering 305 Hz to 5 MHz, and the electric spectral receiver covering 5 MHz to 8 GHz, were developed.

No attempt is made to obtain isotropic antenna response, since to do so would require three orthogonal antennas and processing circuitry for each [Nov 93]. Since this is intended as a survey type system, it is not considered that the

improved precision of an isotropic response is worth the expense and the resulting unwieldiness of the equipment.

The output of each of the monitors is a two dimensional matrixed histogram. One dimension is bands (or bins) of frequency. The other dimension is bands (or bins) of peak field strength. The entries in the histogram matrix are the running totals of the number of times (i.e., number of sampling intervals) that the ambient EMI/RFI level falls within the intersection of a strength bin and a frequency bin. Resolution is coarse, being limited by the bin width. The histograms and their time tags are stored to disk every six hours. Thus, the counts for any observation period can be determined by subtracting the running total counts through the previous period from the running total counts through the period of interest.

Typical operation of each monitor is as follows. The monitor is placed in the environment to be observed, and a VGA video monitor and personal computer keyboard are temporarily connected. The monitoring program starts with the histogram counters zeroed. The VGA video monitor and keyboard are disconnected, and the EMI/RFI shielded interface port is sealed. The system is left unattended, and it counts events for up to several months. At the end of the monitoring interval, the interface port is unsealed and the VGA video monitor and keyboard are temporarily reconnected, and the monitoring program is stopped. The running total histogram for each six hour interval is an ASCII file. Data retrieval consists of removing the floppy disk from its drive, and copying the files.

To provide automatic, long term unattended monitoring of EMI/RFI signals of unknown frequency and bandwidth requires circuitry capable of handling extreme bandwidths. The low band of the electric spectral receiver covers an input bandwidth of 5 MHz to 1000 MHz, or 200:1, and an intermediate frequency (IF) bandwidth of 12.5 to 37.5 MHz, or 3:1. The magnetic spectral receiver covers a bandwidth of 305 Hz to 5 MHz, or 16393:1, and can examine the entire 14 octave bandwidth in a single glance. It is noteworthy that in current EMI/RFI practice, a signal with a 2:1 bandwidth is considered ultrawideband [Eng 93]. In view of this, it is not surprising that a device similar to these monitors is not available commercially, and that the design of these monitors includes considerable novelty.

4. ELECTRIC SPECTRAL RECEIVER

One monitor assembled for this research is configured to observe high frequency electric fields. Frequency coverage is from 5 MHz to 8 GHz. The monitor uses two resistive taper antennas as broadband electric field probes. The antennas are connected to independent processing circuits; one covers 20 bands of equal width from 5 to 1000 MHz, and the other covers a single band from 1 to 8 GHz. The conceptual diagram is shown in Figure 1. A photograph of the processing electronics is shown in Figure 2. A photograph of the completed prototype receiver is shown in Figure 3.

Microwave (1-8 GHz) signals are treated as a single band. The microwave antenna output is coupled through a 1 GHz high pass filter to an amplifier having a flat response from 1-8 GHz. In the interest of holding down cost, a relatively high noise figure (6-8 dB) is tolerable. Since the objective is to

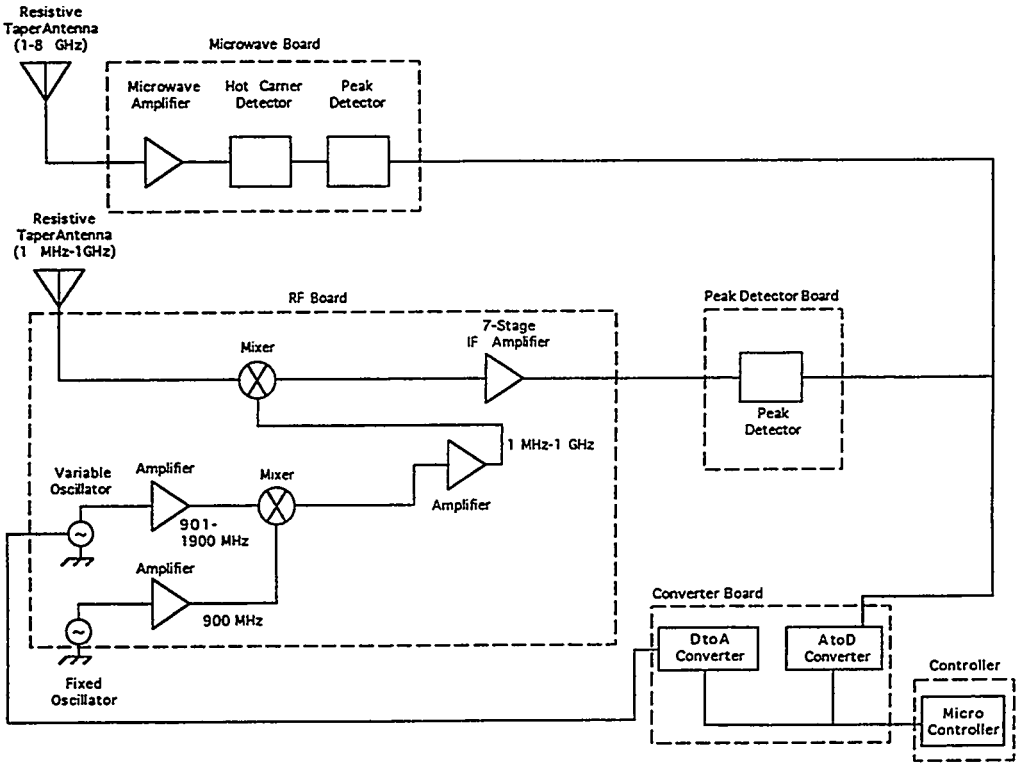


Figure 1. Block Diagram of Electric Receiver.

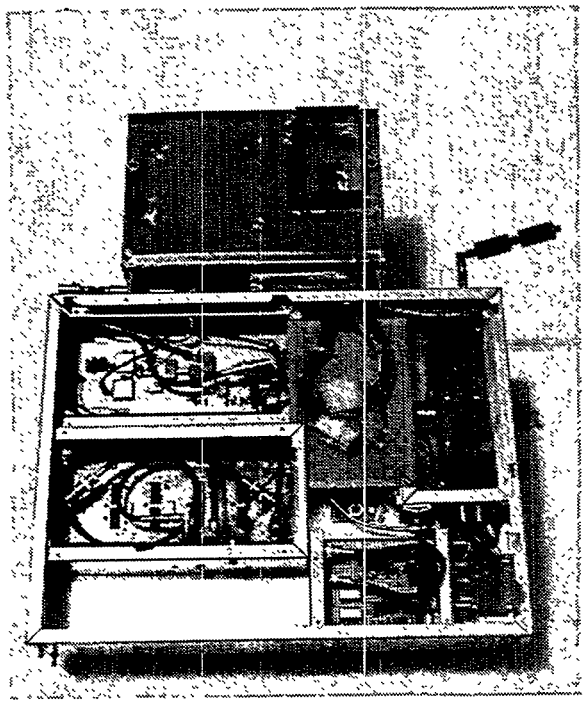


Figure 2. Photo of Electric Receiver Electronics.

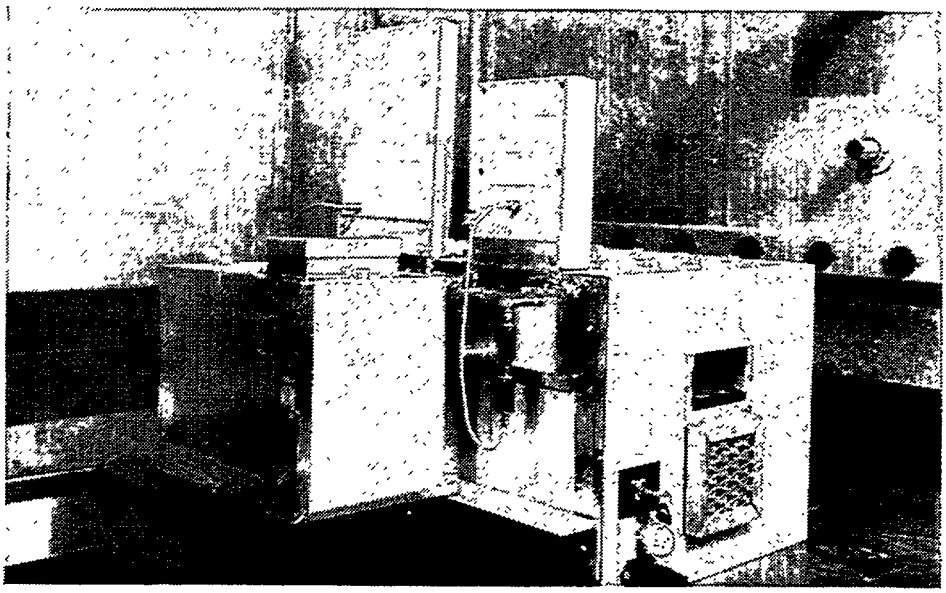


Figure 3. Photo of Electric Receiver.

detect the presence of relatively strong electric fields, going to great expense to obtain a low noise figure is not necessary.

The amplified output is processed by pseudo-peak detection, using a video detector based on a hot carrier diode. This produces a 6 MHz bandwidth signal that is a replica of the modulation envelope of the original microwave signal. The video detector output is then fed to a peak detector, which takes the envelope input and produces a DC output that is correlated with the peak value of the original microwave signal.

Signals below 1 GHz are processed through a heterodyning scheme. The purpose of the local oscillator (LO) chain is to produce a voltage controlled local oscillator that sweeps from 5 MHz to 1 GHz in a single sweep as the control voltage sweeps from 0 to 20 Volts DC. To obtain this performance, a variable oscillator whose output can be swept from 905 to 1900 MHz is mixed with a fixed oscillator at 900 MHz. The difference at the first mixer output is thus 5 to 1000 MHz. The first mixer also produces a sum signal at 1805 to 2800 MHz. A low pass filter with a 1 GHz cutoff suppresses the sum.

The second mixer mixes the broadband (5 MHz to 1 GHz) output of the antenna, and the swept output of the LO chain. The output of the mixer is two sets of broadband signals, the sum of the splitter output and the LO, and the absolute difference of the splitter output and the LO. The absolute difference is the desired product. By following the second mixer with a low pass filter (LPF), a folded window looking into the RF spectrum is realized. For instance, with a

LPF of 37.5 MHz, the intermediate frequency (IF) is limited to DC-37.5 MHz. For a given LO frequency, the RF window includes:

$$(LO - 37.5\ MHz) \leq RF \leq (LO + 37.5\ MHz)$$

The mixer output is amplified by a circuit with a 37.5 MHz cutoff low pass characteristic. Therefore, when the local oscillator sweeps from 42.5 to 962.5 MHz, the amplifier output is a 75 MHz wide window sweeping from 5 MHz to 1000 MHz. The signal is amplified and applied to a peak detector, which produces a DC voltage proportional to the peak value of the signal in the window during the sampling time interval.

The control microprocessor operates on a 35 second sampling sweep, capturing the peak electric field strength observed during each sweep. The 35 second sweep samples each of the 21 individual bands within the spectrum for about 1.5 seconds. A signal must be present for at least 35 seconds to assure that it will be captured; signals of less than 35 second duration will be captured only if the system is looking at that particular band at the time the signal occurs.

The controller carries out the operating cycle as follows. It selects the next local oscillator frequency and the corresponding peak detector, zeroes out the detector, waits 1.5 seconds, reads the peak detector voltage level (which is proportional to the peak field observed during the last second of the 1.5 second wait), and increments the appropriate histogram bin in random access memory (RAM). It moves to the next local oscillator frequency and repeats the process, and so on until the entire range is swept. It repeats the cycle indefinitely until interrupted by a command from the outside world.

5. MAGNETIC SPECTRAL RECEIVER

The other monitor assembled for this research is configured to observe low frequency magnetic fields. Frequency coverage is from 305 Hz to 5 MHz. The monitor uses a passive loop antenna as a broadband magnetic field probe. The conceptual diagram is shown in Figure 4. A photograph of the processing electronics is shown in Figure 5. A photograph of the completed prototype receiver is shown in Figure 6. The 305 Hz to 5 MHz coverage spans 14 octaves. The magnetic monitor captures peak magnetic field strength in each octave during each sampling cycle.

The magnetic spectral receiver repeatedly cycles through the 14 octaves every ½-second. The monitor takes 128K samples at a sampling rate of 10 million samples per second, thus filling the queue in 12800 microseconds. At a processing duty cycle of about 3%, it takes the five digital signal processing (DSP) chips a little more than 30 times as long to extract the information from the data as it does to collect it. Thus, the whole process will take about 30 times 12800 microseconds, or 384000 microseconds. At the conclusion of the processing, the octave registers are updated, and the cycle repeats. Any signal that occurs while the queue is filling will be captured. Since the queue fills for only 12800 microseconds out of each half second cycle, only signals lasting more than a ½-second are certain to be captured.

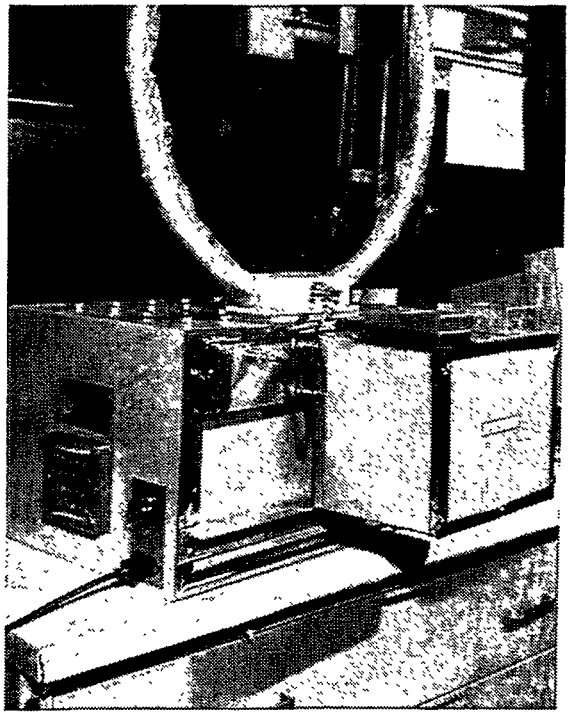


Figure 6. Photo of Magnetic Receiver.

The low frequency magnetic spectral receiver uses a minimal hardware configuration, consisting of an antenna, a preprocessing filter, broadband amplifier, analog-to-digital converter, digital processor, and controller. Due to the extreme bandwidth (14 octaves), the desirability to minimize hardware complexity, and the desirability to maximize the amount of time each octave is observed, all signal processing is done digitally.

The analog part of the system operates as follows. The antenna produces a current proportional to the incident magnetic field in the band of 20 Hz to 5 MHz. A passive 7-pole analog Butterworth high pass filter is used to suppress the power frequency, its third harmonic, and any other undesired signals below 305 HZ. An analog low pass filter is used to prevent aliasing of signals above 5 MHz. A DC to 5 MHz amplifier is used to scale and translate the signal to a level suitable for input to the analog-to-digital (A/D) converter.

Eight bit A/D conversion is done with a self contained chip. While this imposes an upper limit of about 36 dB on the useful dynamic range, it is sufficient for this application. A sampling rate of 10 M-samples per second provides the Nyquist limit at the highest input frequency.

The processing is done on a sample and hold basis. The A/D converter is enabled until the queue fills. Then the A/D converter is disabled, and the queue is processed by DSP0. DSP0 strips out the upper octave and notes the peak value. DSP0 also strips out the lower 13 octaves and feeds the filtered signal to DSP2. DSP2 obtains the peak value for the next highest octave,

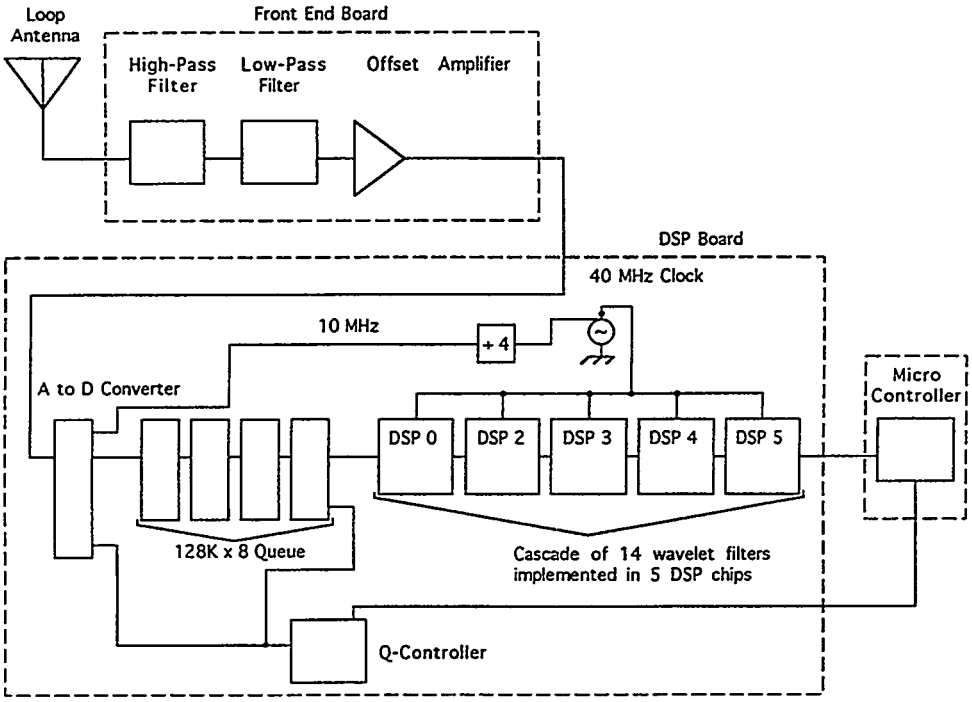


Figure 4. Block Diagram of Magnetic Receiver.

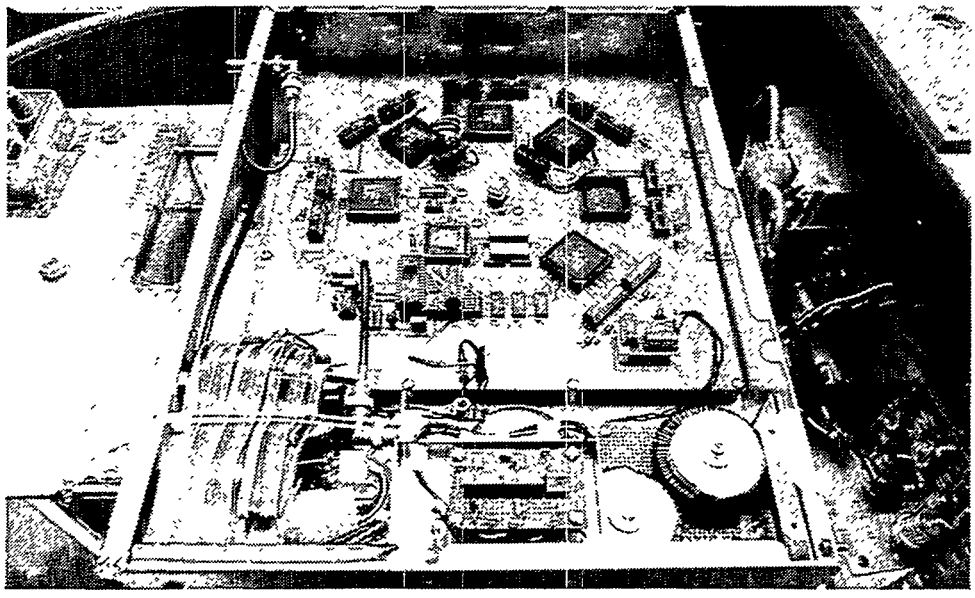


Figure 5. Photo of Magnetic Receiver Electronics.

strips out the bottom 12 octaves, and feeds the filtered signal to DSP3. DSP3 obtains the peak value for the two next highest octaves, strips out the bottom 10 octaves, and feeds the filtered signal to DSP4. DSP4 obtains the peak value for the four next highest octaves, strips out the bottom six octaves, and feeds the filtered signal to DSP5. DSP5 obtains the peak value for the last six octaves, and feeds all the peak readings to the controller.

6. FIELD TESTING

Prior to deployment at a nuclear site, about 10 weeks of observations were made with the electric spectral receiver in the control room and a switchgear room at TVA's Bull Run Fossil Plant. Bull Run is the world's largest single unit fossil plant. At 980 MW, it is comparable in size to a typical nuclear unit. The primary objective of these observations was to assess the performance of the receiver under conditions similar to those that might be encountered in a nuclear plant. Assessing the state of EMI/RFI ambient conditions in the Bull Run control room was of secondary interest.

ORNL employees were present only at setup, and to copy the recorded data at the end of the collecting periods. Otherwise, the receiver operated completely unattended. The captured data are the result of normal operations at Bull Run. No events were contrived to see what sort of EMI/RFI they might generate. No microwave EMI/RFI was observed.

In the control room, two sets of observations were taken. The first week's results are summarized in Table 1. During this period the receiver was set at medium sensitivity (noise floor of 0.4 V/m).

Table 1. Bull Run Control Room Observations (Electric Field)

Date: 6/11/94 through 6/17/94
Total Number of Readings: 16300
Receiver Noise Floor: 0.4 V/m

Occurrence of non-zero readings:

Band (MHz)	Lower Bin Limit (V/m)	Upper Bin Limit (V/m)	Number of Readings
5-26.5 or 50-76.5	2.2	6.5	1
301-326 or 350-376	1.1	1.6	10
301-326 or 350-376	1.6	2.5	2
326-350 or 376-401	1.1	1.7	2
401-426 or 450-476	0.4	0.8	4
401-426 or 450-476	1.2	1.8	13
401-426 or 450-476	1.8	2.8	15
401-426 or 450-476	2.8	4.5	10
401-426 or 450-476	4.5	7.0	3
426-450 or 476-501	0.4	0.6	7
426-450 or 476-501	1.0	1.4	5

Since few non-zero readings were observed during the first week, the receiver sensitivity was increased by removing 10 dB of the attenuation that had been placed between the antenna and the receiver input terminal. Then, a month of observations were made as summarized in Table 2. Both sets of observations (Table 1 and Table 2) were made with the receiver in the same location.

A reading is made by one sweep of the receiver through all of its 21 frequency bins, which requires 35 seconds. Therefore, a week of continuous observation generates about 16300 readings, most of which are below the receiver noise floor. The 20 non-microwave frequency bins each consist of the band of 12.5 MHz to 37.5 MHz above and below the local oscillator frequency. The microwave bin is the entire 1-8 GHz band. Due to variation as a function of frequency in antenna factor and mixer conversion loss, the field strength bin limits are different for each local oscillator frequency. Receiver noise floor is controlled by varying the amount of lumped attenuation between the antenna and the receiver.

For both sets of observations, non-zero events were rare, about one non-zero event per 200 readings (on average, one non-zero event every 90 minutes). For June 11-17, 1994, a total of 16300 readings were taken. Out of these, there were 72 non-zero readings (readings above the receiver noise floor). For June 17-July 14, 1994, a total of 63300 readings were taken. Out of these, there were 286 non-zero readings. The rarity of non-zero events shows the need for continuous long term observation. Catching a significant EMI/RFI event during a spot check is a matter of blind luck.

A similar set of observations was made in the "L&N" room at Bull Run, so called because it houses switchgear manufactured by Leeds and Northrup. This is intended to be an electrically quiet (low EMI) location. The results are summarized in Tables 3 and 4. Generally the "L&N" room was found, as expected, to be much quieter than the control room.

The predominant EMI/RFI activity at Bull Run is attributable to hand held transceivers. These transceivers are widely used at the site. Bull Run security personnel say that the transceivers operate near 419 MHz. At a local oscillator frequency of 438 MHz, the electric monitor responds to any signal in the bands of 401-426 MHz or 450-476 MHz. Consequently, this is the band in which hand held transceiver activity would be detected.

Before deployment at a nuclear site, four days of observations were made with the magnetic spectral receiver in the control room at TVA's Bull Run Fossil Plant. As with the electric receiver field test, the primary objective of these observations was to assess the performance of the receiver under conditions similar to those that might be encountered in a nuclear plant. One set of observations was taken. The results are summarized in Table 5. Assessing the state of EMI/RFI ambient conditions in the Bull Run control room was of secondary interest.

ORNL employees were present only for setup and removal of the receiver. Otherwise, it operated completely unattended. The captured data are the result of normal operations at Bull Run. It is noteworthy that one day before the receiver was removed, Bull Run began a scheduled 8-week maintenance outage. No events were contrived to see what sort of EMI/RFI they might generate.

Table 2. Bull Run Control Room Observations (Electric Field)

Date: 6/17/94 through 7/14/94
Total Number of Readings: 63300
Receiver Noise Floor: 0.06 V/m

Occurrence of non-zero readings:

Band (MHz)	Lower Bin Limit (V/m)	Upper Bin Limit (V/m)	Number of Readings
5-26.5 or 50-76.5	0.31	0.92	9
5-26.5 or 50-76.5	0.92	1.75	4
5-26.5 or 50-76.5	1.75	2.92	4
26-50 or 76-101	0.37	0.62	3
26-50 or 76-101	0.62	0.93	5
26-50 or 76-101	0.93	1.64	6
26-50 or 76-101	1.64	2.91	2
26-50 or 76-101	4.03	>4.03	1
101-126 or 150-176	0.17	0.25	2
101-126 or 150-176	0.25	0.4	8
101-126 or 150-176	0.4	0.62	3
126-150 or 176-201	0.17	0.28	1
126-150 or 176-201	0.28	0.4	2
301-326 or 350-376	0.16	0.23	3
301-326 or 350-376	0.23	0.35	12
301-326 or 350-376	0.35	0.57	6
326-350 or 376-401	0.16	0.24	5
326-350 or 376-401	0.24	0.35	2
326-350 or 376-401	0.35	0.57	3
326-350 or 376-401	0.57	0.89	1
401-426 or 450-476	0.11	0.17	42
401-426 or 450-476	0.17	0.25	20
401-426 or 450-476	0.25	0.4	4
401-426 or 450-476	0.4	0.64	11
401-426 or 450-476	0.64	0.99	5
401-426 or 450-476	1.05	>1.05	23
426-450 or 476-501	0.08	0.14	38
426-450 or 476-501	0.14	0.2	7
426-450 or 476-501	0.2	0.32	1
501-526 or 550-576	0.1	0.16	3
526-550 or 576-601	0.11	0.16	1
601-626 or 650-676	0.13	0.18	2
601-626 or 650-676	0.18	0.28	1
626-650 or 676-701	0.13	0.2	2
626-650 or 676-701	0.2	0.28	3
801-826 or 850-876	0.21	0.3	41

Table 3. Bull Run "L&N" Room Observations (Electric Field)

Date: 7/14/94 through 8/5/94
Total Number of Readings: 47000
Receiver Noise Floor: 0.06 V/m

Occurrence of non-zero readings:

Band (MHz)	Lower Bin Limit (V/m)	Upper Bin Limit (V/m)	Number of Readings
126-150 or 176-201	0.28	0.4	1
401-426 or 450-476	0.17	0.25	3
401-426 or 450-476	0.25	0.4	3

Table 4. Bull Run "L&N" Room Observations (Electric Field)

Date: 8/5/94 through 8/17/94
Total Number of Readings: 28000
Receiver Noise Floor: 0.06 V/m

Occurrence of non-zero readings:

Band (MHz)	Lower Bin Limit (V/m)	Upper Bin Limit (V/m)	Number of Readings
101-126 or 150-176	0.4	0.62	2
126-150 or 176-201	0.28	0.4	1
126-150 or 176-201	0.4	0.62	3
401-426 or 450-476	0.17	0.25	9
401-426 or 450-476	0.25	0.4	3

For several bands that include operating frequencies of video monitor deflection coils, several hundred thousand readings are seen just a little above the noise floor of the receiver. There are several monitors of assorted vintages in the Bull Run control room. This level of video monitor activity is not unexpected. Otherwise, as with electric fields, the magnetic fields are present only a small percentage of the time. Through 40 kHz, the Bull Run data are at least 29 dB below the EPRI recommended withstand. EPRI provides no recommendation above 40 kHz. [EPR 94]

Table 5. Bull Run Control Room Observations (Magnetic Field)

Date: 10/3/94 through 10/7/94
Total Number of Readings: 574000

Occurrence of non-zero readings:

Band (kHz)	Lower Bin Limit (mA/m)	Upper Bin Limit (mA/m)	Number of Readings
.61-1.22	24.5	49.0	6
1.22-2.44	12.7	25.4	3
2.44-4.88	7.1	14.2	3
2.44-4.88	14.2	28.4	1
4.88-9.77	3.36	6.72	293234
9.77-19.53	1.67	3.36	81537
9.77-19.53	3.36	6.72	151
19.53-39.06	.863	1.72	149441
19.53-39.06	1.72	3.46	155
19.53-39.06	3.46	6.91	15
39.06-78.125	.502	1.004	8743
39.06-78.125	1.004	2.008	4370
39.06-78.125	2.008	4.017	56
78.125-156.25	.335	.669	15117
78.125-156.25	.669	1.339	632
78.125-156.25	1.339	2.678	312
78.125-156.25	2.678	5.356	1
156.25-312.5	.289	.579	11676
156.25-312.5	.579	1.158	14
156.25-312.5	1.158	2.316	4
312.5-625	.264	.529	554
312.5-625	.529	1.058	12
312.5-625	1.058	2.116	3
312.5-625	2.116	4.232	2
312.5-625	4.232	8.464	5
312.5-625	8.464	16.928	1
625-1250	.267	.534	128
625-1250	1.07	2.14	3
625-1250	2.14	4.28	5
625-1250	4.28	8.56	3

7. CONCLUSIONS AND FURTHER RESEARCH

ORNL has assembled, tested, and deployed spectral receivers specifically intended for EMI/RFI monitoring in nuclear power plants. Both units are designed to operate unattended for weeks or months. Both are EMI/RFI hardened so as not to become a source or victim of EMI/RFI in the plant under observation. Both preserve frequency data and provide time stamping of data.

One receiver is designed to monitor magnetic fields. It covers 305 Hz through 5 MHz, and records peak magnetic field strength data in 14 one-octave-wide frequency bins. It can be used with a loop antenna to observe radiated fields, or with a current transformer to observe conducted fields. The unit was calibrated in the transverse electromagnetic (TEM) cell at Philips Consumer Electronics in Knoxville, Tennessee. It has been field tested at TVA's Bull Run Fossil Plant, and is currently deployed at Arkansas Nuclear One, in the Unit 2 control room.

The other receiver is designed to monitor electric fields. It covers 5 MHz to 8 GHz, and records peak electric field strength data in 21 frequency bins. The unit was calibrated in the anechoic chamber at the National Institute of Standards and Technology in Boulder, Colorado. It also has been field tested at TVA's Bull Run Fossil Plant, and is currently deployed at Arkansas Nuclear One, in the Unit 2 control room.

The following conclusions can be drawn from the field test data acquired at Bull Run:

- The receivers work in real world conditions, and do not disrupt power plant routine.
- Potentially disruptive EMI/RFI events were observed, but were rare.
- Extended continuous monitoring is required to assure that significant EMI/RFI events are observed.
- A week of continuous monitoring is not a sufficiently long observation period. A month may be.
- A susceptibility limit of 10 V/m (140 dBμV/m) is sufficient to withstand all ambient electric fields observed at Bull Run.
- A susceptibility limit corresponding to te sloping scale recommended by EPRI is sufficient to withstand all ambient magnetic fields observed at Bull Run.
- Video monitor activity is barely detectable above the magnetic receiver noise floor, but low level field strengths are usually present.

A major conclusion of the Bull Run observations is that handheld transceivers are the dominant source of undesired electric fields in and around its control room. The electric spectral receiver recorded fields in the 401-426 MHz band as high as 5-7 V/m. According to Bull Run security, their handheld transceivers operate at 419 MHz. Careful experiments with handheld transceivers show that they can produce an electric field as high as 95 V/m at

a distance of 12 cm from the antenna [Ada 93]. At a distance of 16 feet, a handheld transceiver typically produces a field of 2.5 V/m [Cir 86]. Thus, the electric spectral receiver readings are consistent with operation of a handheld transceiver near the monitor.

The other major conclusion of the Bull Run observations is that while magnetic fields are detectable at a wide range of frequencies, they are at such a low level as to not be a cause for concern.

Over the next year, ORNL plans to use the two monitors to observe long term EMI/RFI effects at several nuclear sites. Both monitors were recently deployed at Arkansas Nuclear One in Russellville. In mid-November they will be moved to Oconee in Clemson, South Carolina, to observe the EMI/RFI effects associated with a nuclear unit startup. Discussions are underway with various nuclear plant operators about possible deployment at other sites. The results of these long term nuclear plant EMI/RFI surveys, and their implications for achievement of electromagnetic compatibility, will be reported in a future paper.

8. REFERENCES

[Ada 93] "Electric Field Strengths Measured Near Personal Transceivers," Adams, J., *1993 IEEE International Symposium on Electromagnetic Compatibility*, presented at Dallas TX, August 9-13, 1993, Published by IEEE, 93CH3310-0, pp. 42-45.

[Asl 87] "A Combined Electric and Magnetic Field Monitor," Aslan, E., *Journal of Microwave Power*, 1987, pp. 79-83.

[Bab 86] Babij, T. M. and Bassen, H., *Broadband Isotropic Probe System for Simultaneous Measurement of Complex E- and H-Fields*, US Patent 4,588,993, May 13, 1986.

[Bei 83] "High Frequency Magnetic Measurements Using Small Inductive Probes," Biersdorfer and Clothiaux, *American Journal of Physics*, Vol. 51, 1983, pp. 1031-1036.

[Ber 89] "A Large Loop Antenna for Magnetic Field Measurements," Bergervoet and Veen, *The Eighth International Zurich Symposium and Technical Exhibition on Electromagnetic Compatibility*, presented at Zurich, March 7-9, 1989, pp. 29-34.

[Cir 86] "Electromagnetic Compatibility in Nuclear Power Plants," Cirillo and Prussel, *WATTec Conference*, presented at Knoxville TN, February 11-14, 1986.

[Eng 93] "Advanced Technologies for Ultrawideband System Design," Engler, H. F., *1993 IEEE International Symposium on Electromagnetic Compatibility*, presented at Dallas TX, August 9-13, 1993, Published by IEEE, 93CH3310-0, pp. 250-253.

[EPR 94] *Guidelines for Electromagnetic Interference Testing in Nuclear Plants*, Final Report, TR-102323, April 1994, produced by Electric Power Research Institute, 3412 Hillview Ave., Palo Alto CA 94304.

[Eum 93] "Aperiodic Active and Semi-Active High Sensitivity Broad Dynamic Range Electromagnetic Sensors," Eumurian and Pampalone, *1993 IEEE International Symposium on Electromagnetic Compatibility*, presented at Dallas TX, August 9-13, 1993, Published by IEEE, 93CH3310-0, pp. 315-317.

[Ewi 92] "Technical Basis for Acceptance Criteria on the Susceptibility of Digital Systems to Electromagnetic Interference," Ewing, Korsah, and Antonescu, *20th Water Reactor Safety Information Meeting*, presented at Rockville MD, October 21-23, 1992.

[Ewi 94] Ewing and Korsah, *Technical Basis for Evaluating Electromagnetic and Radio Frequency Interference in Safety Related I&C Systems*, NUREG/CR-5941, April 1994, available from National Technical Information Service, Springfield VA.

[Ful 85] "NBS Ambient Magnetic Field Meter for Measurement and Analysis of Low-Level Power Frequency Magnetic Fields in Air," Fulcomer, P.M., National Institute of Standards and Technology Report NBSIR 86-3330, prepared for the Department of Energy, 1985.

[Gas 93] "An Isotropic Broadband Electric and Magnetic Field Sensor for Radiation Hazard Measurements," Gassmann and Furrer, *1993 IEEE International Symposium on Electromagnetic Compatibility*, presented at Dallas TX, August 9-13, 1993, Published by IEEE, 93CH3310-0, pp. 105-108.

[Gra 94] "EMI Testing of a High Speed Rail Train Set," Gray and Ambrose, *1994 IEEE International Symposium on Electromagnetic Compatibility*, presented at Chicago IL, August 22-26, 1994, Published by IEEE, 94CH3347-2, pp. 242-247.

[Hew 93] "HP 8546A EMI Receiver Preliminary Technical Data," published by Hewlett Packard Company, May 1993, 5091-7218E.

[Jok 89] "Measurements of Electromagnetic Emissions from Video Display Terminals at the Frequency Range from 30 Hz to 1 MHz," Jokela, Aaltonen and Lukkarinen, *Health Physics*, Vol. 57, No.1, July 1989, pp. 79-88.

[Mas 89] "Photonic Probes for the Measurement of Electromagnetic Fields over Broad Bandwidths," Masterson et al., *Proceedings of IEEE National Symposium on Electromagnetic Compatibility*, Presented in Denver CO, May 23-25, 1989, Published by IEEE.

[MIL 93] *Electromagnetic Interference Characteristics Measurement*, MIL-STD-462-D, January 1993.

[Mis 93] "ELF Electric and Magnetic Field Measurement Methods," Misakian, M., *1993 IEEE International Symposium on Electromagnetic Compatibility*, presented at Dallas TX, August 9-13, 1993, Published by IEEE, 93CH3310-0, pp. 150-155.

[Nel 94] "Electric Field Strengths Created by Electrosurgical Units," Nelson and Ji, *1994 IEEE International Symposium on Electromagnetic Compatibility*, presented at Chicago IL, August 22-26, 1994, Published by IEEE, 94CH3347-2, pp. 366-370.

[Nic 93] Private communication between Paul Nichols, TVA communications engineer, and Steve Kercel, January 1993.

[Nov 93] "An Optically Linked Three Loop Antenna System for Determining the Radiation Characteristics of an Electrically Small Source," Novotny, Masterson, and Kanda, *1993 IEEE International Symposium on Electromagnetic Compatibility*, presented at Dallas TX, August 9-13, 1993, Published by IEEE, 93CH3310-0, pp. 105-108.

[NRC 91] "Review of Vendors' Test Programs to Support the Design Certification of Passive Light Water Reactors," NRC Policy Issue SECY-91-273.

[Ott 88] Ott, H., *Noise Reduction Techniques in Electronic Systems*, Second Edition, 1988, John Wiley and Sons, New York.

[Roc 90] "A Personal Radio Frequency Dosimeter with Cumulative Dose Recording Capabilities," Rochelle et al., *Proceedings of Sensors Expo 90*, Presented at Sensors Expo, Chicago IL, September 11-13, 1990, published by Helmers Publishing Co., Peterborough NH, Paper number 107B.

[Sik 94] "A New Generation of EMI Receiver System," Sikora, Platt and Iannotti, *1994 IEEE International Symposium on Electromagnetic Compatibility*, presented at Chicago IL, August 22-26, 1994, Published by IEEE, 94CH3347-2, pp. 132-137.

FIBER OPTIC PRESSURE SENSORS FOR NUCLEAR POWER PLANTS

H. M. Hashemian
C. L. Black

Analysis and Measurement Services Corporation
AMS 9111 Cross Park Drive
Knoxville, Tennessee 37923 USA

Phone: (615) 691-1756
Fax: (615) 691-9344

ABSTRACT

In the last few years, the nuclear industry has experienced some problems with the performance of pressure transmitters and has been interested in new sensors based on new technologies. Fiber optic pressure sensors offer the potential to improve on or overcome some of the limitations of existing pressure sensors.

Up to now, research has been motivated towards development and refinement of fiber optic sensing technology. In most applications, reliability studies and failure mode analyses remain to be exhaustively conducted. Fiber optic sensors have currently penetrated certain cutting edge markets where they possess necessary inherent advantages over other existing technologies. In these markets (e.g. biomedical, aerospace, automotive, and petrochemical), fiber optic sensors are able to perform measurements for which no alternate sensor previously existed.

Fiber optic sensing technology has not yet been fully adopted into the mainstream sensing market. This may be due to not only the current premium price of fiber optic sensors, but also the lack of characterization of their possible performance disadvantages. In other words, in conservative industries, the known disadvantages of conventional sensors are sometimes preferable to unknown or not fully characterized (but potentially fewer and less critical) disadvantages of fiber optic sensors.

A six-month feasibility study has been initiated under the auspices of the U.S. Nuclear Regulatory Commission (NRC) to assess the performance and reliability of existing fiber optic pressure sensors for use in nuclear power plants. This assessment will include establishment of the state of the art in fiber optic pressure sensing, characterization of the reliability of fiber optic pressure sensors, and determination of the strengths and limitations of these sensors for nuclear safety-related services.

1. BACKGROUND

Over 25 years have passed since fiber optic sensors were first conceived, designed, and developed. Since then, the components of such systems have become more easily available, less expensive, and more efficient.

Research into fiber optic pressure sensors has grown to a great extent. Some of the asserted and demonstrated performance advantages of fiber optic sensing include wide dynamic range[1,2], sensitivity[2,3], signal isolation[3,4,5], distributed measurement[1,6], reduced size and mass[7,8], and resistance to environmental extremes[8,9].

In certain fields, and in certain applications, fiber optic sensors now provide measurements that were not previously obtainable. In the bio-medical field, the extreme miniaturization possible with fiber optic sensors made possible the development of catheter tip probes. The automotive industry is also developing small sensors for combustion temperature and pressure measurements. In the aerospace field, sensors are being imbedded in composite material structures, as well as replacing much of the current instrumentation. Electrical isolation makes fiber optic sensors the candidates of choice in high EMI/RFI environments, and their inherent safety is a popular feature in potentially explosive environments.

However, in mainstream industries and applications, fiber optic sensors have not yet firmly established themselves in process sensing. This may be interpreted as a failure in demand. The lack of demand is due, in most cases, to the premium price for the increased resolution, performance, and other features of fiber optic sensors. For most applications, this price may be unjustifiable, as current conventional sensor characteristics may be seen as adequate.

In the case of fiber optic pressure sensors, many different transducers have been developed and built. Unfortunately, almost all of these transducers were developed on a custom/prototype basis as part of a research effort. Only a handful of these sensors have since been successfully commercialized. These few sensors are intended for highly specialized applications. The lack of a commercial market at the present time has impeded the development of a more general purpose fiber optic pressure sensor.

2. ASSESSMENT OF FIBER OPTIC PRESSURE SENSORS FOR USE IN THE NUCLEAR POWER INDUSTRY

The state of the art in fiber optic pressure sensing has been determined from finding, surveying, and visiting manufacturers and researchers of fiber optic pressure sensors. A comprehensive library of texts, papers, and articles on fiber optic pressure sensor

designs, applications, and theory has also been gathered. From this information, inferences have been drawn concerning the status of current research and development efforts. This study forms the basis for the technology review provided below.

The current availability of fiber optic pressure sensors has been characterized by the survey efforts. It has been found that fiber optic sensors are being employed mostly in niche applications, and are generally utilized to measure process parameters other than pressure.

Negotiations are currently underway to obtain fiber optic pressure sensors, in order to compare performance characteristics of fiber optic sensors with those of conventional sensors typically utilized in nuclear power plants. Calibration accuracy, repeatability, and stability with pressure and temperature cycling will be investigated. Other characteristics such as response time will be explored.

3. FIBER OPTIC PRESSURE SENSOR TECHNOLOGIES

Fiber optic sensor designs may be divided into two categories, intensity-modulated and phase-modulated. In intensity-modulated sensors, which are also known as intensity-type sensors, the measurand affects the intensity of light transmitted along a fiber optic cable. Phase-modulated or interferometric sensors encode the measurand in the phase difference between the light returning from a sensing optical path and a reference optical path.

3.1 Intensity-Modulated Sensors

In intensity-type sensors, the light emitted from an optical source is carried along a fiber. The light intensity is modified at the sensor element and is returned to a detector. Generally, the light is required to leave the fiber to interact with the sensing element. Intensity-modulated sensors enjoy the benefit of requiring relatively simple electronics to decode the measurand from the transmitted light. This results in a more simple and less expensive device to develop or manufacture. However, some intensity-type designs suffer from lead and source dependencies. If the light intensity is affected by changes other than in the area of measurement interest, then the output of the sensor will be biased by these changes.

Intensity-modulated sensors can be classified into three general mechanisms: transmission, reflection, and microbending.

The transmissive concept is normally associated with intensity-modulated sensors in which the light is interrupted while passing from one segment to another of a measurement loop. All of the transmission sensors described below directly measure displacement or deflection of a diaphragm. The diaphragm deflection is generated due to the pressure difference across the diaphragm.

The simplest of the transmissive concept fiber optic pressure sensor designs is shown in Figure 1. A movable shutter connected to a flexible diaphragm is allowed to interrupt the light path proportionally to the pressure applied to the diaphragm. Another transmissive sensor design involves displacement (either axially or radially) of one of the fiber optic segments to modulate intensity, as displayed in Figure 2.

Frustrated total internal reflection (FTIR) is a modification of the transmissive concept. The FTIR sensor concept is illustrated in Figure 3. In this sensor, the ends of each segment are polished parallel to one another at an angle to the fiber axis. When the fiber segment ends are at a distance from one another, total internal reflection of all propagating modes occurs. However, as the fiber ends are brought closer to one another as a diaphragm is deflected, energy is coupled, and light may pass. This sensor is the most sensitive of the sensors employing transmission intensity modulation.

The reflective concept generally refers to a sensor consisting of a pair of fiber bundles and a reflective target. One bundle serves to transmit the light to the target, and the other receives the reflected light from the target. As the target is displaced, the reflected light received is modulated. In a reflective concept fiber optic pressure sensor, as shown in Figure 4, the target is the diaphragm. This design enjoys several advantages, including noncontact measurement, simplicity and low cost.

Another reflective concept sensor is the near total internal reflection (NTIR) sensor. This sensor, as shown in Figure 5, requires only a single measurement fiber, the end of which has been polished slightly just below the critical angle. The tip of the fiber is the sensor element, and is subjected to the process pressure. Light travels along the fiber, strikes the polished end, reflects to the mirrored surface, reflects back to the polished end, and is reflected back along the fiber. The returned light intensity is modulated with small shifts in the critical angle as pressure variations induce unequal variations in the refractive indices of the fiber and the surrounding medium.

Figure 6 shows a diaphragm pressure transducer containing a fiber optic microbend sensor. The microbend sensor consists of a multimode step-index optical fiber with a metal cladding which is squeezed between grooved surfaces. One of the surfaces is attached to the diaphragm, and as the diaphragm is displaced, the fiber is squeezed and bent. As the fiber is bent, small amounts of light, proportional to the pressure applied to the diaphragm, are lost due to microbending losses through the walls of the fiber. In general, as the number of bending points on the corrugated surfaces are increased, and

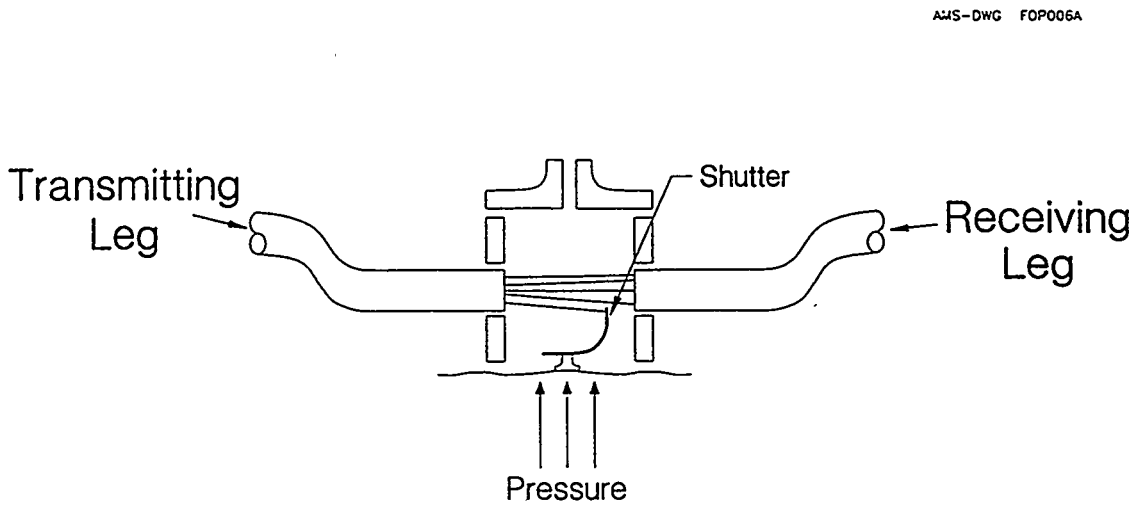


Figure 1. Fiber Optic Pressure Sensor with Movable Shutter Modulating Transmitted Light Intensity

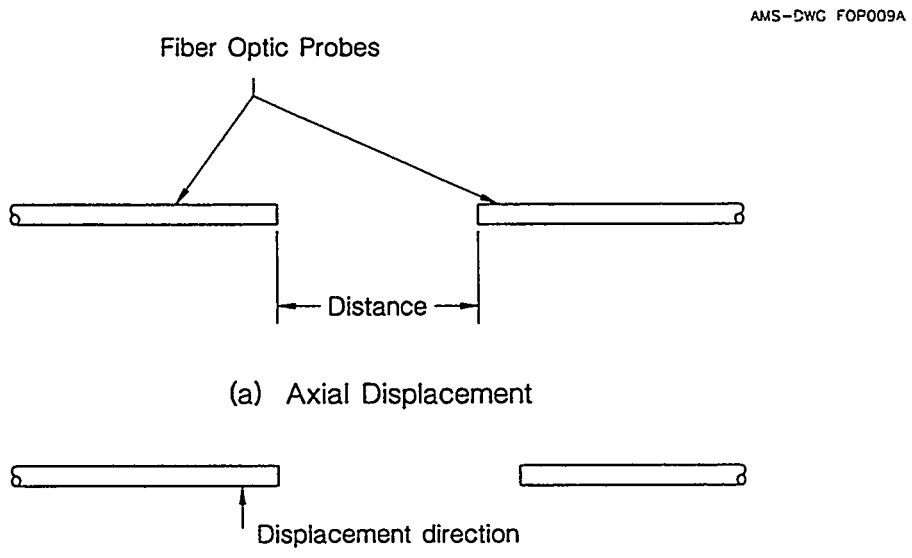


Figure 2. Transmissive Fiber Optic Pressure Sensor with Movable Fibers Modulating Light Intensity

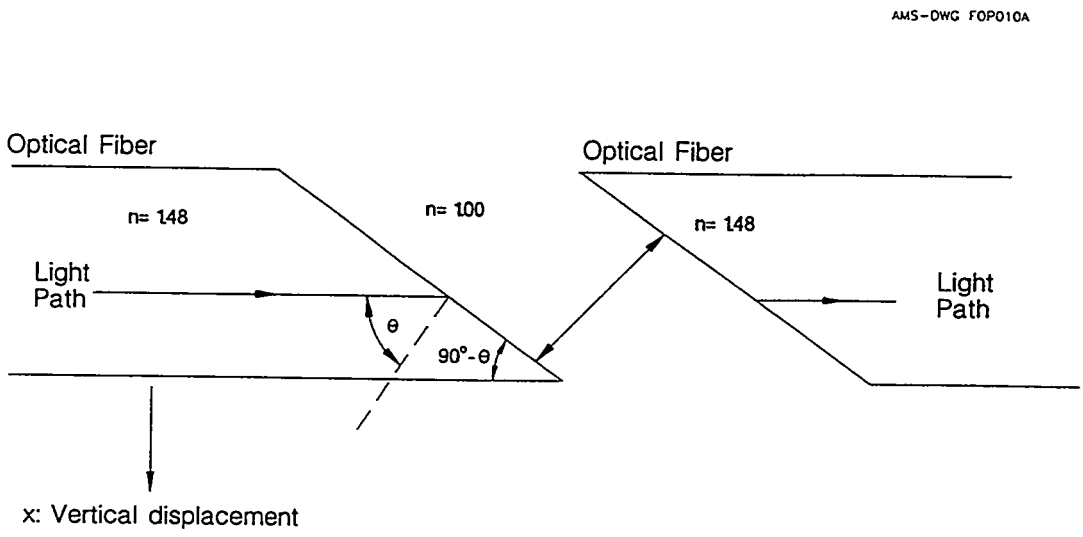


Figure 3. Frustrated Total Internal Reflection (FTIR) Sensor

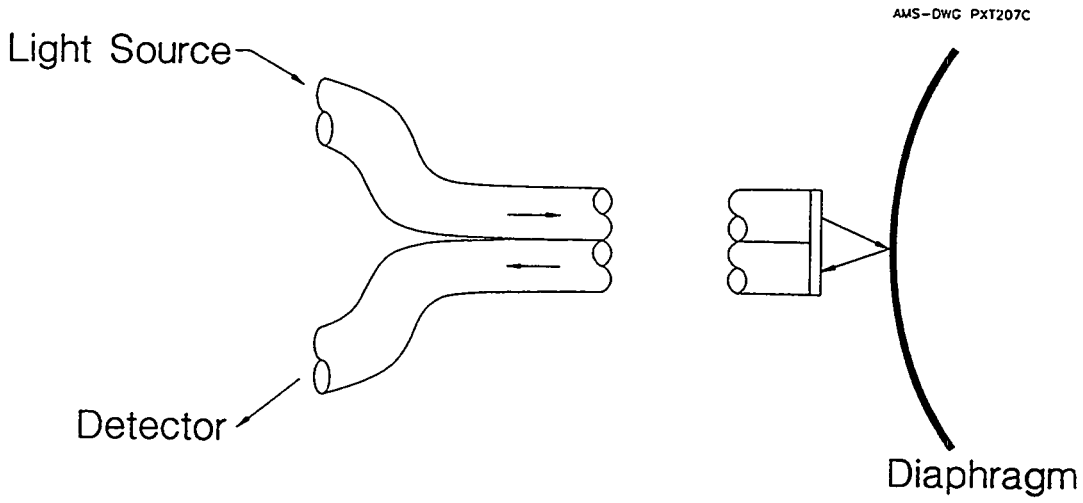


Figure 4. Reflective Fiber Optic Pressure Sensor

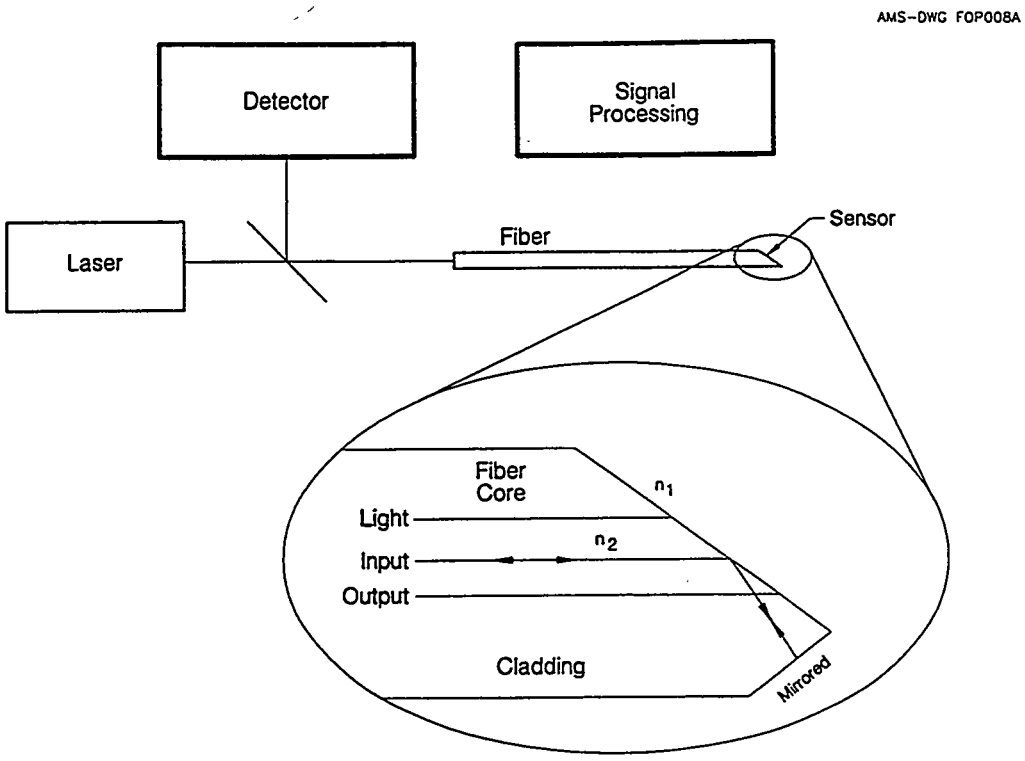


Figure 5. Near Total Internal Reflection (NTIR) Sensor

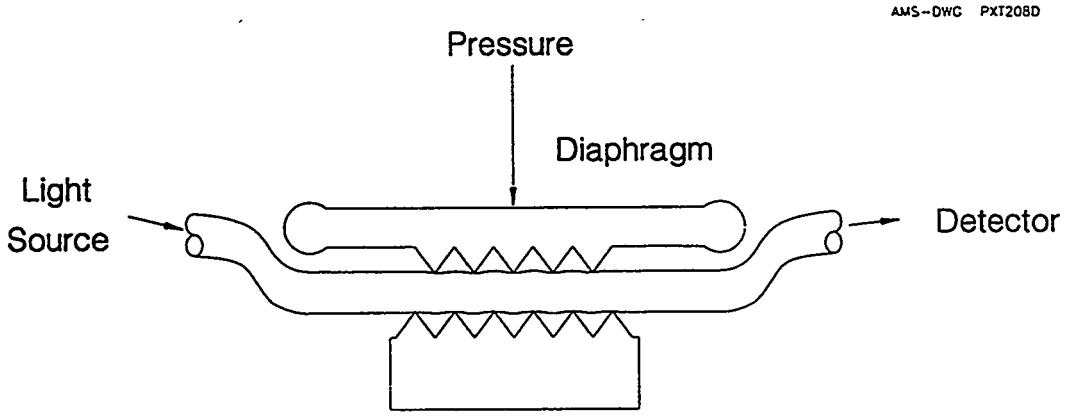


Figure 6. Microbend Pressure Sensor

as the spacing between the corrugations are decreased, the sensitivity of the sensor is increased.

3.2 Phase-Modulated Sensors

Interferometric sensors, by virtue of the use of a reference leg, are generally less affected by irrelevant variations in non-measurement regions of the fiber optic leads. Phase-modulated sensors are generally much more sensitive than intensity-modulated sensors due to the extreme accuracy which may be obtained in measuring phase differences. However, phase-modulated sensors are also generally more expensive due to the increased complexity of decoding the measurand from the frequency domain. There are four interferometric configurations. They include the Mach-Zehnder, the Michelson, the Fabry-Perot, and the Sagnac. The Mach-Zehnder, the Michelson, and the Fabry-Perot configurations may be utilized for pressure measurement. The Sagnac configuration is chiefly utilized for gyroscopic applications. Of three possible pressure measurement configurations, the Mach-Zehnder is most frequently applied to pressure measurements.

The configuration of a Mach-Zehnder interferometric sensor is shown in Figure 7. The light beam is split into a reference leg and a measurement leg. The measurement leg experiences both a length change and change in refractive index due to the pressure applied directly to the fiber. The two beams are recombined, and the phase modulation is detected. The response and sensitivity of a Mach-Zehnder fiber optic pressure sensor are dependent on the fiber optic coating on the cable. Metallic coatings reduce the sensitivity, while plastic coatings increase sensitivity. The lead and reference fibers may be coated with metal to reduce their sensitivity.

Fabry-Perot interferometric pressure sensors incorporate a sensing resonance cavity consisting of two reflectors on either side of an optically transparent medium. One of the reflectors or mirrors is attached to a diaphragm, and the cavity length is allowed to vary with the pressure applied at the diaphragm. A schematic of the Fabry-Perot configuration is shown in Figure 8. Due to the high (but not perfect) reflectivity of the mirrors, the light is bounced back and forth many times inside the sensing cavity. Phase delay is experienced multiple times in the cavity, until light escapes to the detector. This compounding of phase delay increases the sensitivity of the Fabry-Perot sensor with respect to the other interferometric configurations. Other advantages of the Fabry-Perot configuration include: it only requires one fiber, and it is insensitive to intensity variations in the lead fiber.

The Michelson interferometer configuration is illustrated in Figure 9. The Michelson interferometer is very similar to the Mach-Zehnder configuration, except the sensing and reference legs are terminated with a reflector. This results in the elimination of a coupler,

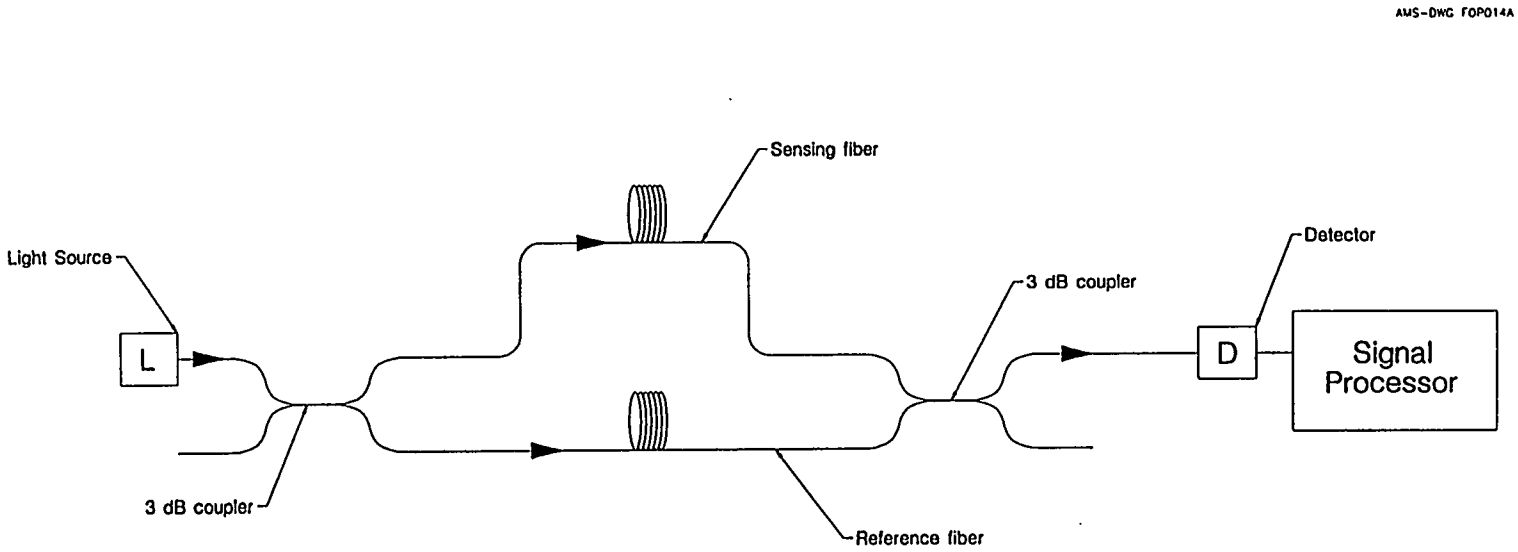


Figure 7. Mach-Zehnder Interferometric Fiber Optic Pressure Sensor

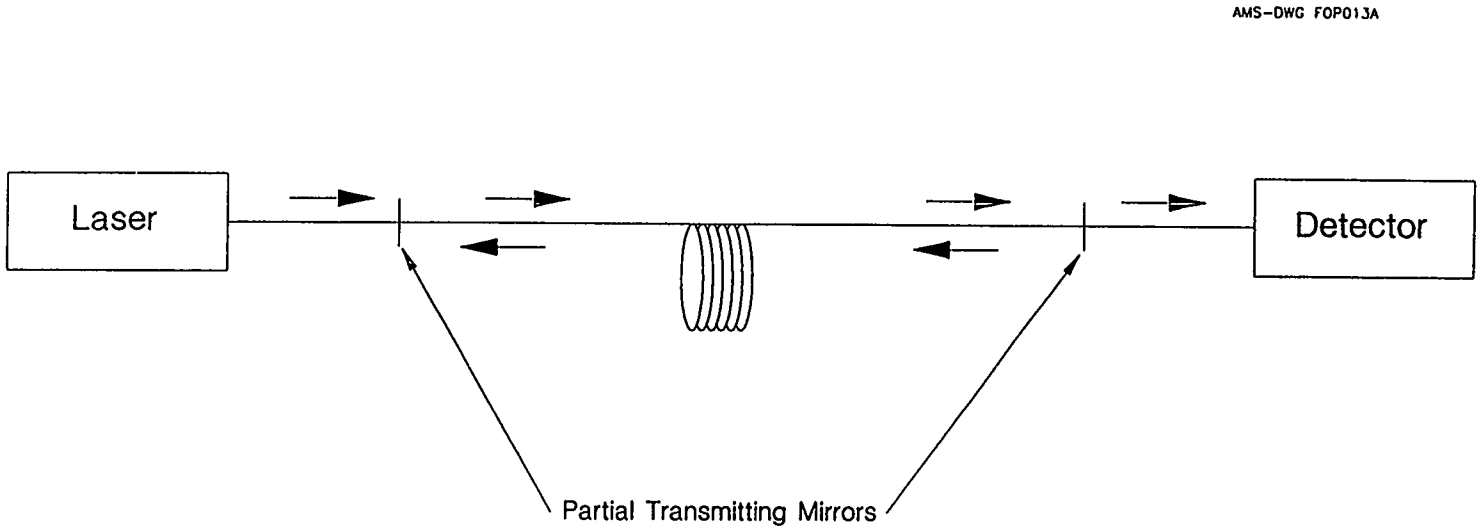


Figure 8. Fabry-Perot Interferometric Fiber Optic Pressure Sensor

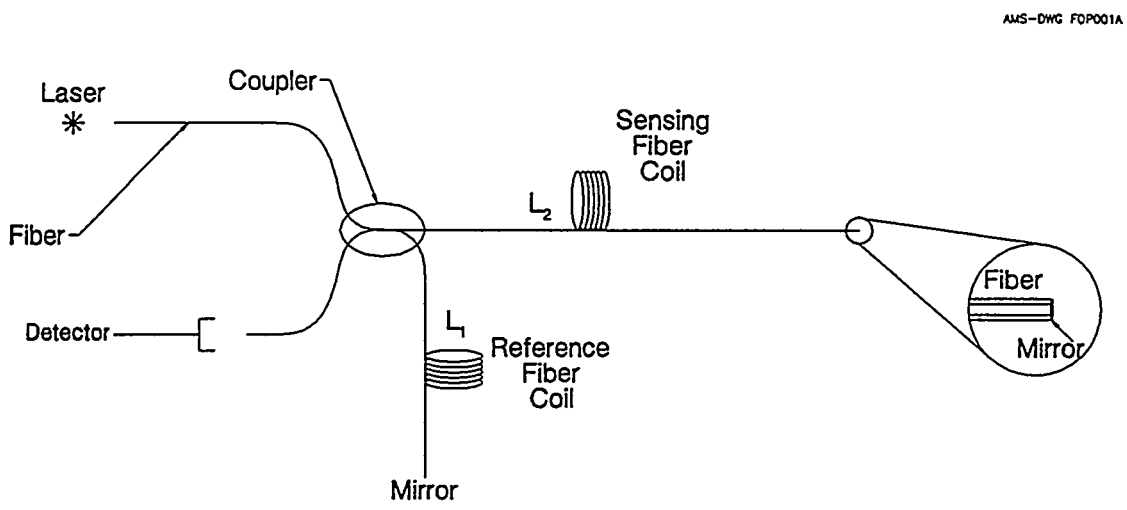


Figure 9. Michelson Interferometric Fiber Optic Pressure Sensor

but also introduces a significant disadvantage. In the Michelson interferometer configuration, the coupler feeds light back both into the detector and the laser. Feedback into the laser creates a source of noise.

4. CONCLUSIONS

Despite their numerous demonstrated advantages, fiber optic pressure sensors have not yet penetrated many industries because their long term performance characteristics are not known and they are more expensive than other existing pressure sensors. Fiber optic pressure sensors are currently used chiefly in very specialized applications where conventional sensors do not meet the required specifications.

Only a handful of fiber optic pressure sensor manufacturers are currently marketing fiber optic pressure sensors. These manufacturers all target special markets and applications for their sensors (e.g. ultra-high precision, high temperature, explosive environments, high RFI/EMI environments, and small sensor applications). The lack of a profitable market for fiber optic pressure sensors has slowed their development and availability.

REFERENCES

1. Abushagur, M.A.G., et al., "O-Ring Fiber Optic Pressure Sensor," *Opt. Engrg.*, vol. 33, p. 1074, April 1994.

2. Cho, Y.C. and Soderman, P.T., "Fiber-Optic Interferometric Sensors for Measurements of Pressure Fluctuations: Experimental Evaluation," *NASA Technical Memorandum 104002*, p. 1, January 1993.

3. Jackson, D.A. and Rao, Y.J., "Prototype Fiber-Optic-Based Ultrahigh Pressure Remote Sensor with Built-In Temperature Compensation," *Rev. Sci. Instrum.*, vol. 65, p. 1695, May 1994.

4. Henderson, P.J., Jones, G.R., and Spencer, J., "Pressure Sensing Using a Chromatically Addressed Diaphragm," *Meas. Sci. Technol.*, vol. 4, p. 88, 1993.

5. Jian, P., Libo, Y. and Shunling, R., "Automatic Compensation Fiber-Optic Differential Pressure Sensor," *Sensors and Actuators A*, vol. 36, p. 183, 1993.

6. Barel, A.R.F., Desforges, F.X., and Voet, M.R.H., "An Optical Fiber Network for Analog Temperature and Pressure Sensing Purposes," in *Proceedings of the 8th Optical Fiber Sensors Conference*, pp. 205-208, January 1992.

7. Barwicz, A. and Bock, W.J., "An Electronic High-Pressure Measuring System Using a Polarimetric Fiber-Optic Sensor," *IEEE Trans. Instrum. and Meas.*, vol. 39, p. 976, December 1990.

8. Jackson, D.A. and Rao, Y.J., "Prototype Fiber-Optic-Based Fizeau Medical Pressure Sensor that Uses Coherence Reading," *Opt. Lett.*, vol. 18, p. 2153, December 1993.

9. Berthold, J.W., Ghering, W.L., and Varshneya, D., "Design and Characterization of a High-Temperature, Fiber-Optic Pressure Transducer," *J. Lightwave Technology*, vol. LT-5, July 1987.

ENVIRONMENTAL TESTING OF A PROTOTYPIC DIGITAL SAFETY CHANNEL, PHASE I: SYSTEM DESIGN AND TEST METHODOLOGY*

K. Korsah, G. W. Turner, and J. A. Mullens
Oak Ridge National Laboratory (ORNL), Oak Ridge, TN, 37831-6010

ABSTRACT

A microprocessor-based reactor trip channel has been assembled for environmental testing under an Instrumentation and Control (I&C) Qualification Program sponsored by the U.S. Nuclear Regulatory Commission. The goal of this program is to establish the technical basis and acceptance criteria for the qualification of advanced I&C systems. The trip channel implemented for this study employs technologies and digital subsystems representative of those proposed for use in some advanced light-water reactors (ALWRs) such as the Simplified Boiling Water Reactor (SBWR). It is expected that these tests will reveal any potential system vulnerabilities for technologies representative of those proposed for use in ALWRs. The experimental channel will be purposely stressed considerably beyond what it is likely to experience in a normal nuclear power plant environment, so that the tests can uncover the worst-case failure modes (i.e., failures that are likely to prevent an entire trip system from performing its safety function when required to do so). Based on information obtained from this study, it may be possible to recommend tests that are likely to indicate the presence of such failure mechanisms. Such recommendations would be helpful in augmenting current qualification guidelines.

1. INTRODUCTION

Rising maintenance costs and a lack of spare parts are forcing an increasing number of nuclear utilities to consider upgrading analog safety systems with newer, more readily available technologies such as fiber optic transmission systems and microprocessors. In addition, advanced light-water reactor (ALWR) manufacturers intend to make even more extensive use of such technologies in the design of both control and safety (Class 1E) systems. However, many of the qualification standards used for nuclear plant instrumentation were developed for analog equipment and so they do not account for performance and functionality issues that are unique to digital equipment. In addition, the consequences of environmental stressor effects have not been clearly determined, in part due to the inability to completely map all possible relationships between inputs to a microprocessor and its outputs. As a result, investigative work is needed to characterize the failure modes and degradation mechanisms of technologies proposed for use in ALWR safety systems and/or future retrofits for existing LWRs. This information supports the determination of the likelihood of environmental stress for digital components and the expected effect. The result would be a more clear definition of what stressors (and to what level) digital equipment should be qualified to withstand and what symptoms should be indicative of an unacceptable response in type testing.

---

*Research sponsored by the Office of Nuclear Regulatory Research, U. S. Nuclear Regulatory Commission, under Interagency Agreement DOE 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.

The vulnerabilities of "advanced" technologies such as fiber optic transmission systems, multiplexers, and microprocessor-based systems to environmental stressors is currently being investigated by ORNL as part of an NRC-sponsored I&C qualification research program[1-3]. The goal of this program is to establish the technical basis and acceptance criteria for the qualification of advanced I&C systems. Initial studies in this regard have been documented in NUREG/CR-5904, *Functional Issues and Environmental Qualification of Digital Protection Systems of Advanced Light-Water Nuclear Reactors*, where the likely impact of environmental stressors on safety systems and the failure mechanisms of fiber-optic transmission system components are examined. A methodology for identifying the need for accelerated aging in a qualification program for new I&C systems placed in benign environments was also suggested in the cited document. As a follow-on to that work, the safety channel and test methodology described in this present paper will be used to investigate *experimentally* the functional behavior and failure modes of a microprocessor-based trip system resulting from the application of environmental stressors such as temperature, humidity, and the presence of smoke.

2. DIGITAL SAFETY CHANNEL DESIGN

2.1. Rationale for Design Choices

The reactor trip system designs for the *AP600* (Westinghouse), the *ABWR* (General Electric), and the *System 80+* (Combustion Engineering) were reviewed to identify technologies that are different from present-day safety system implementations. Descriptions of the three designs can be found in NUREG/CR-5904. ORNL's design employs technologies that are representative of these three designs.

ALWR trip systems are typically implemented as four separate divisions. In ORNL's system, however, only one division is implemented; the trip information to/from the other three divisions is simulated by a *Host Processor*. This approach does not compromise the objectives of the task, since any vulnerabilities identified in the channel implemented in the ORNL system could be expected to be present in similar (redundant) channels.

2.2. System Level Design Description

Fig. 1.1 shows a block diagram of the prototypic reactor trip channel (PRTC). It consists of one division of the reactor trip subsystems and an engineered safety feature (ESF) multiplexer subsystem. The inputs and outputs of these subsystems are established and monitored, respectively, by the Host Processor. The following is a description of the various subsystems and their functions:

Reactor Trip/Remote Multiplexing Unit

The function of the reactor trip/remote multiplexing unit (TRP/RMU) is to acquire analog process signals, convert them to digital form, and format them into frames suitable for transmission over a *Fiber Distributed Data Interchange* (FDDI) ring network. All process variables used for reactor trip (e.g., hot leg temperature, coolant flow rate, etc.) are simulated by a digital-to-analog multiplexer card contained in the Host Processor.

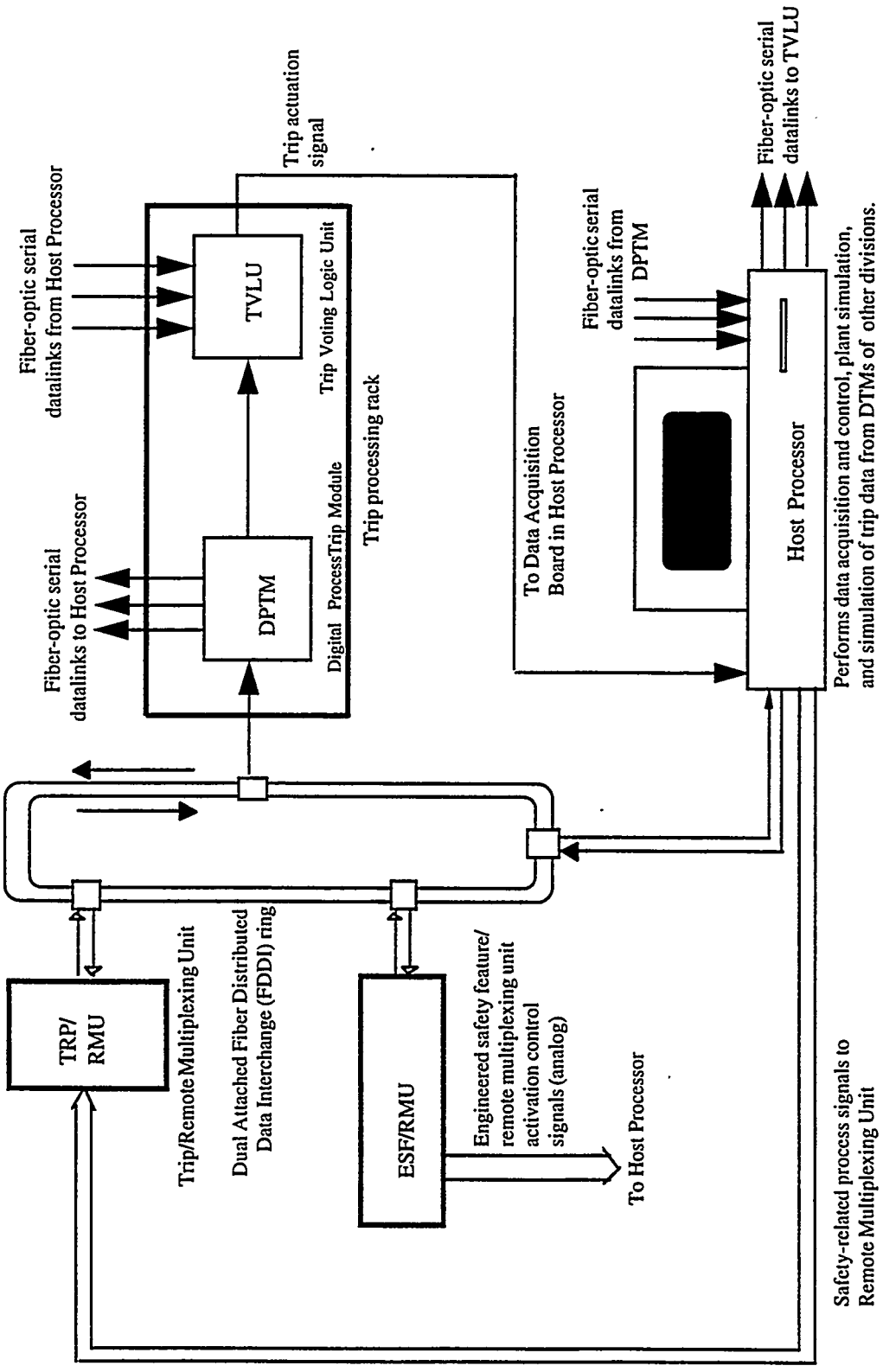


Fig. 1. Diagram of the prototypic reactor trip channel.

Digital Process Trip Module and Trip Voting Logic Unit

The digital process trip module (DPTM) acquires the digital values of the process signals off the FDDI network. The DPTM compares individual process values with trip setpoint values and *for each variable* sends a separate trip/no trip indication to the trip voting logic unit (TVLU). At the same time, it sends identical information to the Host Processor via optical fiber serial datalinks. Note that in a typical ALWR trip system the trip/no trip information from the DPTM would be sent to the three other divisions' TVLUs via optical fiber datalinks, whereas in this implementation, the Host Processor will simulate the functions of the DPTMs and TVLUs of the three other divisions.

The Host Processor

The Host Processor (HOSTP) monitors all information going to and from the reactor trip subsystems, performs diagnostic checks when requested, and stores general information on system performance. In particular, the HOSTP performs the following activities:

- Simulates process signal variables typical of either normal or accident conditions, and sends the variables to the TRP/RMU;

- Acquires the data sent over the network by the TRM/RMU. (Note that the data from the TRP/RMU is also acquired by the division's DPTM processor.) In this way the HOSTP verifies that the process signals it sent to the TRP/RMU have not been corrupted as a result of passing through the network;

- Simulates *process trip* conditions assumed to come from the DPTM of the three other divisions. This "Process Trip" information is sent over three separate optical serial datalinks to the TVLU of the division under test;

- At the same time, the HOSTP receives process trip information from the DPTM of the division under test. It then performs a 2-out-of-4 (software) voting based on the process trip information from this division, as well as the process trip information assumed to have come from the "other three divisions" (but actually simulated by the HOSTP);

- Monitors the voting result from the TVLU of the division under test. Prior to this time, the TVLU of the division under consideration would have received both the process trip information from the "DPTM of the other three divisions" (actually simulated by the HOSTP and sent via three independent fiber optic datalinks as shown in the figure), *and* the process trip information generated by the DPTM in its own division. The TVLU would have performed its own 2-out-of-4 voting, and sent *divisional trip* information to the HOSTP;

- Provides specified pump, valve, and other ESF actuation signals to the ESF/RMU under simulated accident conditions (e.g., a loss of coolant accident (LOCA) or Steam Line Break).

- Monitors the ESF/RMU outputs to verify that:

    a. A condition requiring a trip actuation was successfully analyzed by the subsystems in the division;

b. Any ESF actuation signals generated by the HOSTP were successfully sent across the FDDI ring network, as well as correctly interpreted by the ESF/RMU.

3. TEST METHODOLOGY

As indicated earlier, a major objective of this study is to investigate the failure modes, under various environmental stresses, of representative digital technologies that are likely to be employed in future nuclear power plants or in retrofits. The study is expected to result in a more clear definition of what stressors (and to what level) digital equipment should be qualified to withstand and what symptoms should be indicative of an unacceptable response in type testing.

A previous study of proposed ALWR protection systems conducted by ORNL staff determined that multiplexing equipment used in the safety system will most likely be located outside reactor containment in "divisional clean areas[1]." In addition, this equipment will be placed at locations that are geographically separate from the protection system cabinets installed in "mild" (i.e., control room) environments. Thus, it appears reasonable to divide the equipment to be tested into two major subsystems, so that tests can be conducted on each major subsystem separately. The major subsystems are defined as:

- The multiplexing equipment used for acquiring process information (TRP/RMU in Fig. 1). This is designated *subsystem 1.*
- The trip modules and ESF actuation multiplexing equipment. This is designated *subsystem 2.*

Subsystem 1 will first be subjected to all the tests; the tests will then be repeated on subsystem 2. All tests will be performed under software control from the Host Processor. A brief outline of the general test procedure is as follows:

- *Configure the PRTC;*
- *Place the subsystem to be tested in the test chamber;*
- *Apply a chosen stressor for a specified period of time;*
  - *generate test signals typical of both normal and various accident conditions;*
  - *for each set of test signals, verify system response and log any errors;*
  - *increase the severity of the stressor;*
  - *repeat the tests.*

The stressors to be applied are temperature, humidity, EMI/RFI, and smoke. Since the objective is not to qualify the system hardware, the subsystems will be stressed considerably beyond what they are likely to experience in a normal nuclear power plant environment. The procedure followed in applying the stressors is briefly described as follows:

Steady State Humidity Tests:

- Initial conditioning [122°F (50°C) at 30% RH] for 24 hours.
- Continued testing until system is brought down to ambient.
- Steady state tests [106°F (41°C) at 93% RH] for 24 hours.

Accelerated Humidity Tests:

- Initial conditioning [122°F (50°C) at 93% RH] for 24 hours.
- Continued testing while system is brought down to ambient.
- 10 cycles of the following: temperature ramping from 75°F to 150°F in 2-1/2 hrs at 94% RH.

Smoke Tests:

- Initial conditioning at 73°F and 50% RH for 24 hours.
- Increment of RH to 60%
- Burning of fiber optic cable specimen while equipment under test (EUT) is in test chamber.
- Placement of EUT in test chamber and continued testing for additional 8 hours.
- Physical examination and analysis of EUT for damages.
- Repetition of tests at increments of 10% RH up to and including 90% RH, or until permanent failure, whichever comes first.

EMI/RFI Tests:

These tests will be performed to MIL-STD 462D specifications:

- CS01 - Conducted susceptibility; low frequency;
- CS02 - Conducted susceptibility, high frequency;
- CS06 - Conducted susceptibility, spikes;
- RS01 - Radiated susceptibility, magnetic fields;
- RS02 - Radiated susceptibility, spikes;
- RS03 - Radiated susceptibility, electric fields.

The following industry standards were used as guidelines to develop the temperature/humidity/smoke test procedures:

- ANSI/TIA/EIA-526-1992, "Standard Test Procedures for Fiber Optic Systems."
- ANSI/EIA/TIA-455-5A-1990, "Humidity Test Procedure for Fiber Optic Connecting Devices."
- ANSI/EIA/TIA-455-3A-1989, "Procedure to Measure Temperature Cycling Effects on Optical Fibers, Optical Cable, and Other Passive Fiber Optic Components."
- CNS C6046, "Environmental Testing Methods and Endurance Test Methods for Discrete Semiconductor Devices (Cycle Test for Temperature and Humidity)."
- ASTM/D 5485-94, "Standard Test Method for Determining the Corrosive Effect of Combustion Products Using the Cone Corrosimeter."

Electromagnetic Interference/Radio-Frequency Interference (EMI/RFI) tests will be performed on the PRTC according to applicable test criteria and methods stipulated in MIL-STD-461 and MIL-STD-462,

respectively. MIL-STD-461 establishes the military's emission and susceptibility requirements for electronic, electrical, and electromechanical equipment and subsystems. It also provides a basis for evaluating the electromagnetic characteristics of equipment and subsystems by setting operational acceptance criteria. The test methods corresponding to the MIL-STD-461C requirements are described in MIL-STD-462.

The objective of the EMI/RFI tests under this task is to identify how EMI/RFI-induced upsets in the EUT can affect the reactor trip systems's ability to fail safe. The tests are *not* intended to ascertain whether the subsystems meet emissions and susceptibility criteria called out by MIL-STD-461. Thus, only applicable *susceptibility* criteria and test methods will be used in conducting the tests.

The smoke tests will be performed in collaboration with Sandia National Laboratories (SNL). There is currently no standard for smoke tests of electronic equipment; existing "smoke standards" or draft standards have a focus that is different from the objectives of this task. For example, Underwriters' Laboratory (UL) Std 1685, "Vertical Tray Fire Propagation and Smoke Release Test for Electrical and Optical Fiber Cables," is designed to determine values of cable damage height and smoke release from electrical and optical-fiber cables when the cables are subjected to a flaming ignition source. The standard does not investigate the toxicity of the products of combustion or decomposition, nor does it address how an equipment's susceptibility to smoke should be measured.

IEEE draft Std 1202.1, "Standard for Measuring the Release Rates of Smoke and Heat of Wire & Cable for Use in Industrial and Commercial Occupancies," is expected to be similar in content and focus to UL Std 1685.

In the design of a test chamber for ORNL's smoke tests, SNL is following an ASTM draft standard,"Standard Test Method for Measuring the Corrosivity of Smoke from the Burning or Thermal Decomposition of Materials and Products." However, this standard focuses on a test method for determining the corrosive effects of smoke on metals under specified conditions, rather than on the potential for degradation or failure of electronic equipment. ORNL and SNL have used this draft standard, UL 1685, and ASTM/D 5485-94 as guidelines in developing the smoke test chamber and test procedures that will be used in this work.

4. CONCLUDING REMARKS

This paper has discussed the design of a digital safety channel employing technologies similar to those likely to be used in the next generation of nuclear power plants. We have also summarized the test methodology to be used to investigate the vulnerabilities of these technologies to various environmental stressors. Based on information obtained from this study, it will be possible to determine the expected effect of a stressor on digital subsystems likely to be used in nuclear power plants. This information, combined with a knowledge of the likelihood of the stressor in the environment, can provide a more clear definition of what stressors (and to what level) digital equipment should be qualified to withstand, and will provide the technical basis that will be helpful in augmenting current qualification guidelines.

At the time of this writing, the hardware design is complete, the assembly of the hardware is nearly finished, and the software test algorithms are nearing completion. Actual system tests in stressing environments are expected to commence in December 1994.

REFERENCES

1. Korsah, Kofi, Robert L. Clark, and Richard T. Wood, *Functional Issues and Environmental Qualification of Digital Protection Systems of Advanced Light-Water Nuclear Reactors*, NUREG/CR-5904, April 1994, U.S. Nuclear Regulatory Commission.

2. Ewing, P. D., and K. Korsah, *Technical Basis for Regulatory Guidance on the Susceptibility of Digital Systems to Electromagnetic and Radio-Frequency Interference*, NUREG/CR-5941, ORNL/TM-12221, May 1993, Oak Ridge National Laboratory.

3. Korsah, K., R. L. Clark, and D. E. Holcomb, "A Methodology for Evaluating 'New' Technologies in Nuclear Power Plants," *Instrumentation, Controls, and Automation in the Power Industry, Vol. 37, p. 131-148*, Proceedings of the 4th Annual ISA/EPRI Joint Controls and Automation Conference, Orlando, FL, June 1994.

ON-LINE CALIBRATION OF PROCESS INSTRUMENTATION CHANNELS IN NUCLEAR POWER PLANTS

H. M. Hashemian
J. P. Farmer

Analysis and Measurement Services Corporation
AMS 9111 Cross Park Drive
Knoxville, Tennessee 37923 USA

Phone: (615) 691-1756
Fax: (615) 691-9344

ABSTRACT

An on-line instrumentation monitoring system was developed and validated for use in nuclear power plants. This system continuously monitors the calibration status of instrument channels and determines whether or not they require manual calibrations. This is accomplished by comparing the output of each instrument channel to an estimate of the process it is monitoring. If the deviation of the instrument channel from the process estimate is greater than an allowable limit, then the instrument is said to be "out of calibration" and manual adjustments are made to correct the calibration.

The success of the on-line monitoring system depends on the accuracy of the process estimation. The system described in this paper incorporates both simple intercomparison techniques as well as analytical approaches in the form of data-driven empirical modeling to estimate the process.

On-line testing of the calibration of process instrumentation channels will reduce the number of manual calibrations currently performed, thereby reducing both costs to utilities and radiation exposure to plant personnel.

1. INTRODUCTION

Conventional calibration of nuclear power plant instrumentation involves applying a series of known inputs to the instruments and measuring the resulting outputs. If the outputs do not fall between the predefined limits assigned to that particular instrument, then the instrument is said to be out of calibration. Therefore, manual adjustments are made to offset the calibration deviation and bring the instrument back into calibration. However, if the original measurements, known as the "as-found" data, show that the instrument is not out of calibration, then no adjustments are necessary.

For instrumentation located in the field, such as process sensors, the calibration effort is not only time consuming and costly, but also involves radiation exposure to the test personnel. Furthermore, the historical calibration data from nuclear power plants have shown that a majority of sensors drift very little and do not often require calibration. A reduction in the unnecessary manual calibrations would reduce costs and personnel radiation exposure and eliminate the risk of maintenance-induced damage to the plant equipment.

To improve the efficiency of instrument calibrations in nuclear power plants, an on-line instrumentation monitoring system was developed and validated under a contract with the U.S. Nuclear Regulatory Commission (NRC). This system periodically scans the outputs of the instrument channels and determines if any instrumentation is out of calibration. The system is intended to replace the first part of the conventional calibration procedure where the as-found data is evaluated to determine if manual adjustments are necessary. A main advantage of the on-line monitoring system is that the calibration checks can be performed remotely and automatically on each instrument channel as a whole rather than the current practice of calibrating a single component or group of components at a time. Since conventional calibrations on process sensors are typically only performed once every eighteen months, the on-line system provides proactive maintenance capabilities since it monitors the condition of the instrumentation continuously during the fuel cycle.

2. DESCRIPTION OF THE ON-LINE MONITORING SYSTEM

The on-line instrumentation monitoring system consists of a data acquisition system with the necessary data storage capabilities and a data analysis software package (Figure 1). The data acquisition system is a fixed hardware device connected to the plant instrumentation, typically at the plant computer inputs. It consists of a set of multiplexers and a signal isolation amplifier, along with a precision digital voltmeter for measuring the steady-state values of the instrumentation. The computer provided with the data acquisition system periodically samples the outputs of the plant instrument channels and stores the data for later analysis. The sampling rate of the system, which is variable, is limited only by the time required to finish a sampling run and the amount of data storage available.

The data analysis software package can be installed as a part of the data acquisition system, allowing continuous evaluation of the calibration status of the plant instruments. The system will "flag" any channels whose calibrations deviate from the allowable limits. This information can then be used to calibrate the instruments that are out of tolerance or schedule them for manual calibrations during the plant outage.

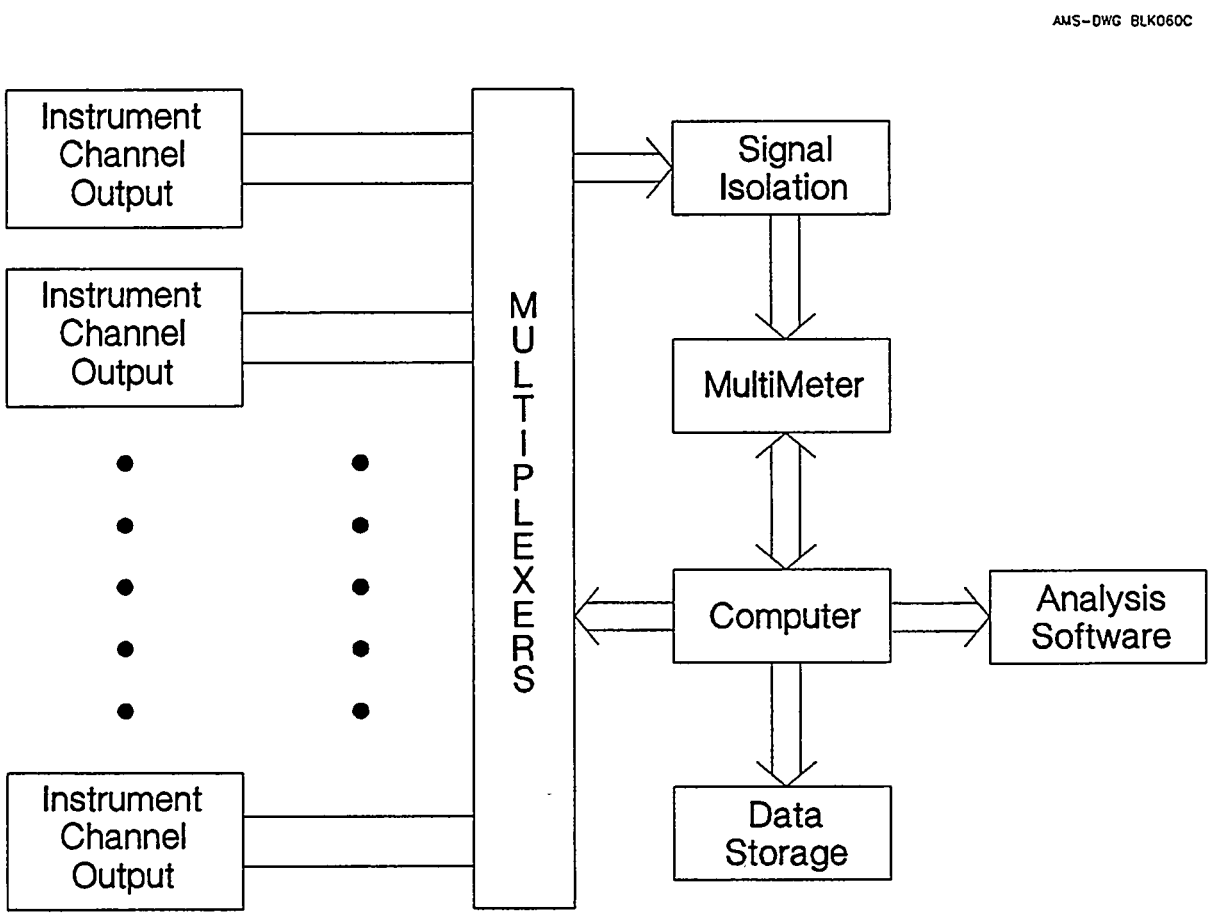


Figure 1. Illustration of On-Line Calibration Monitoring System

3. DATA PROCESSING

On-line monitoring data usually contains normal process fluctuations, noise and signal anomalies. These effects must be eliminated prior to data analysis. Higher frequency process fluctuations and noise can be removed by a tunable digital low-pass filter. Although this is an effective means of removing the process fluctuations, care must be taken so as to avoid over-filtering which may distort critical regions of the data. The spikes that are encountered when plant technicians calibrate the rack can be eliminated by employing a tunable median filter algorithm. Figure 2 shows on-line monitoring data before and after low-pass filtering and spike removal. Sections of data that are still undesirable after filtering can be removed manually by placing exclusion bands around the undesirable portions of the data in question.

4. DATA ANALYSIS

After the data is processed, the deviation of each instrument channel output from the process estimation is calculated. This result can then be compared to the allowable deviation limit for that particular channel to determine if it is or is not out of calibration. Although this is a simple procedure, accurate determination of a process estimate is essential to its success.

Several process estimation methods, often referred to as signal validation methods, have been incorporated into the on-line instrumentation monitoring system. Some involve simple intercomparison techniques which rely on channel redundancy in most safety systems of nuclear power plants. These methods are known as like-signal comparison and involve both simple and weighted averaging algorithms. Analytical redundancy, in the form of physical and empirical modeling, is used to add to the reliability of a process estimate, avoid common-mode effects and compensate for any lack of redundancy. These analytical techniques, which use data from related instrument channels, provide an independent estimate of the process. Due to its independence from the other channels in the process group, the analytically redundant process estimate is free from the potential of common-mode errors which rnay affect the like-signal comparison estimate. Figure 3 shows graphically how the estimate of the process is calculated by the on-line monitoring system.

Although it has been shown through validation work that the analytical methods for determining a process estimate are usually accurate and reliable, an estimate based on actual calibration data may be included to be conservative. This is accomplished by manually calibrating at least one of the instrument channels in a redundant group and using this calibration information to validate the process estimate.

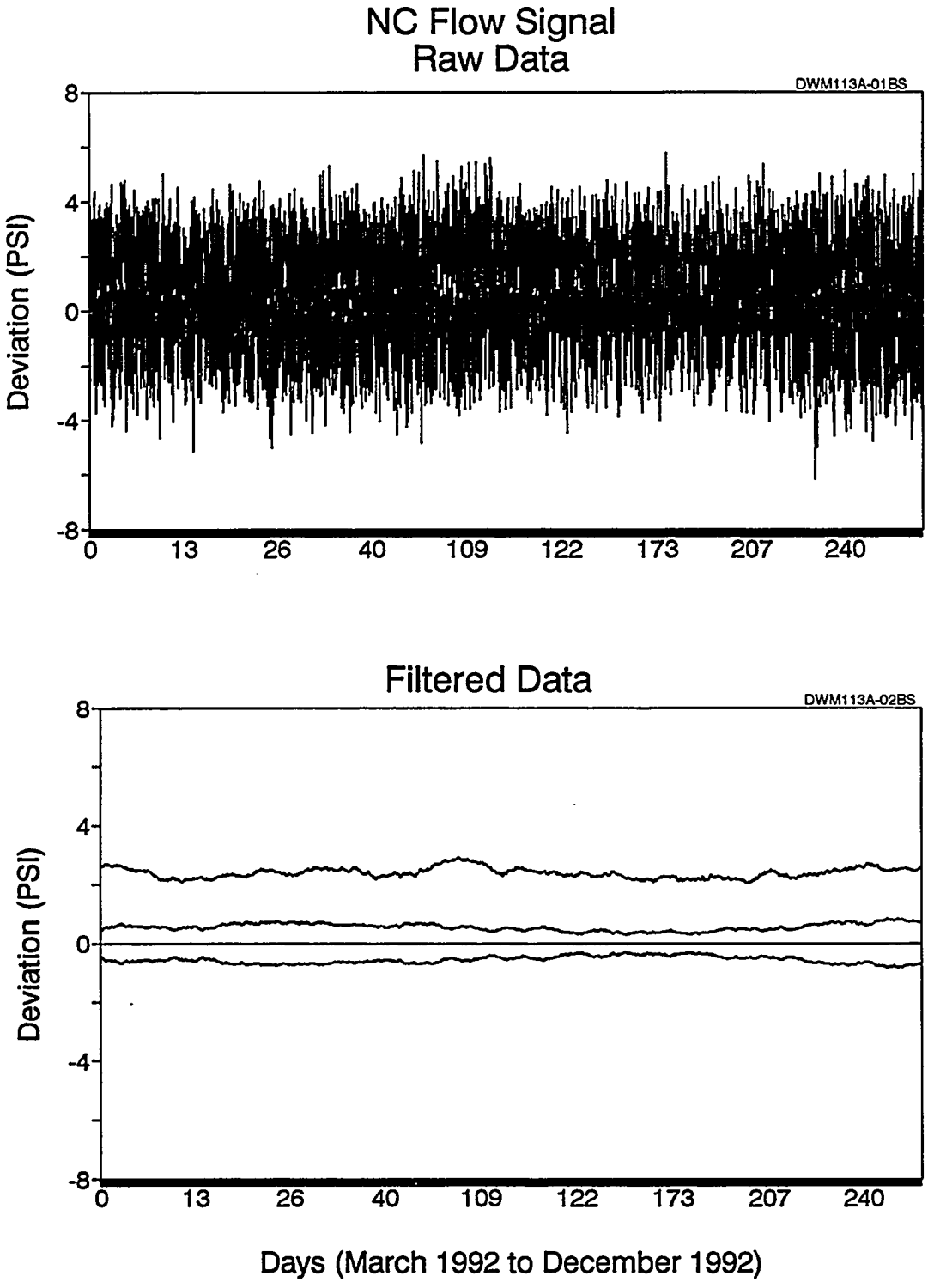


Figure 2. On-Line Monitoring Data Before and After Filtering

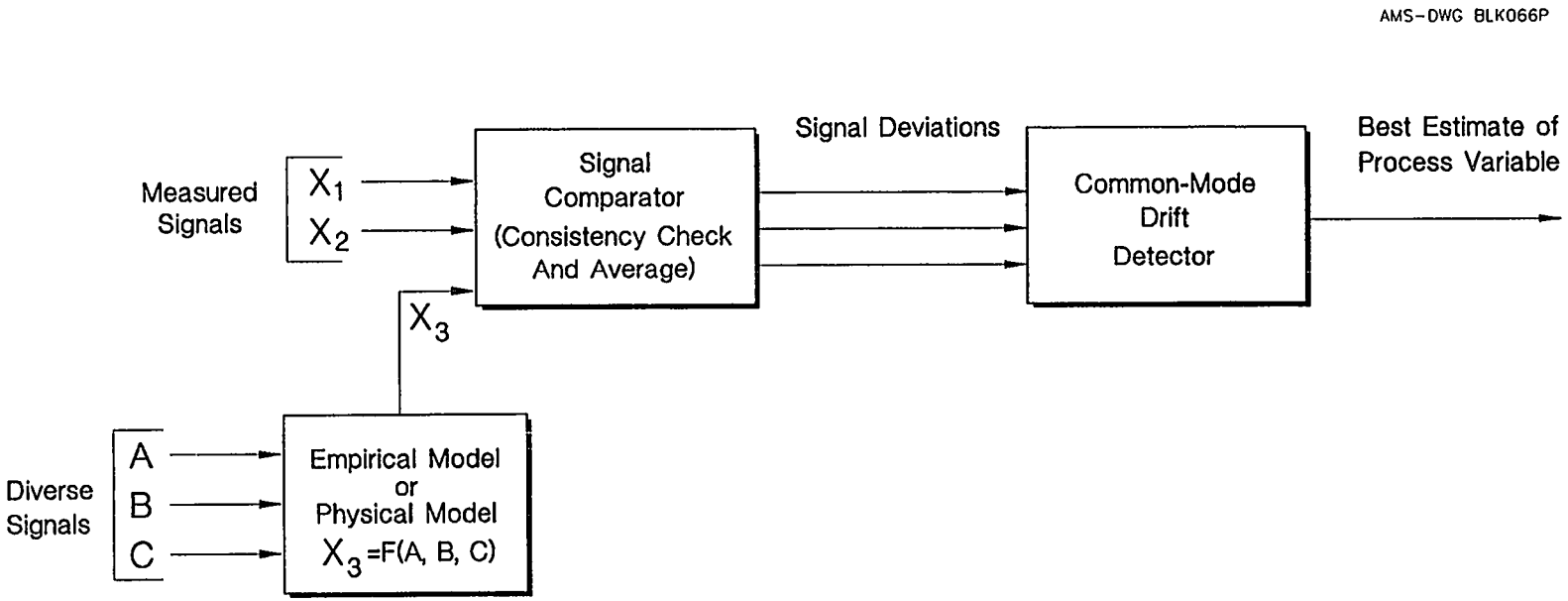


Figure 3. Illustration of Principle of Process Estimation

5. DETERMINATION OF ALLOWABLE DEVIATION LIMITS

As mentioned above, the calibration status of an instrument channel is determined by comparing its deviation from the process estimate to predetermined deviation limits. If the channel deviation lies between the upper and lower limits then the channel calibration is acceptable (Figure 4). If not, the channel is deemed to be out of calibration. These limits are determined based on the channel statistical allowance (CSA) information which is the basis for the instrument setpoint calculations for the plant.

The deviation limits are comprised of the uncertainties attributed to each of the components in the instrument channel. This includes sensor and rack accuracies, temperature effects, manual calibration accuracies, etc.. A statistical combination of these items gives the total measurement uncertainty attributed to the entire instrument channel. Of course, the channel uncertainties differ from channel to channel and from plant to plant. In order to be conservative, the deviation limits for the on-line monitoring system are typically lower than the total channel uncertainty.

The resulting deviation limits for the instrument channels are large relative to the typical manual calibration criteria for individual components in the channel. This is due to the fact that the on-line monitoring system monitors the calibration status of all the instruments simultaneously rather than one instrument at a time. The implementation of this system can potentially reduce the uncertainties in the instrument channels by eliminating the inaccuracies attributed to the manual calibration activities. These inaccuracies are a result of temperature effects, static pressure shifts and other environmental effects.

6. SYSTEM VALIDATION

A research and development (R&D) project, sponsored by the NRC, was undertaken to develop and validate the on-line instrumentation monitoring system. This R&D effort was conducted in cooperation with the Duke Power Company which allowed the system to be installed at the McGuire Nuclear Power Station Unit 2 for field validation purposes. A feasibility study was completed in January 1993, and is documented in NUREG/CR-5903. The results of the second phase of the validation work performed over a two year period are being prepared at the time of this writing for presentation to the NRC. This will also be documented in the form of a NUREG/CR report to be issued in early 1995. Research into similar on-line monitoring systems is being conducted at several nuclear power plants including Millstone, San Onofre, V.C. Summer, and the South Texas Project.

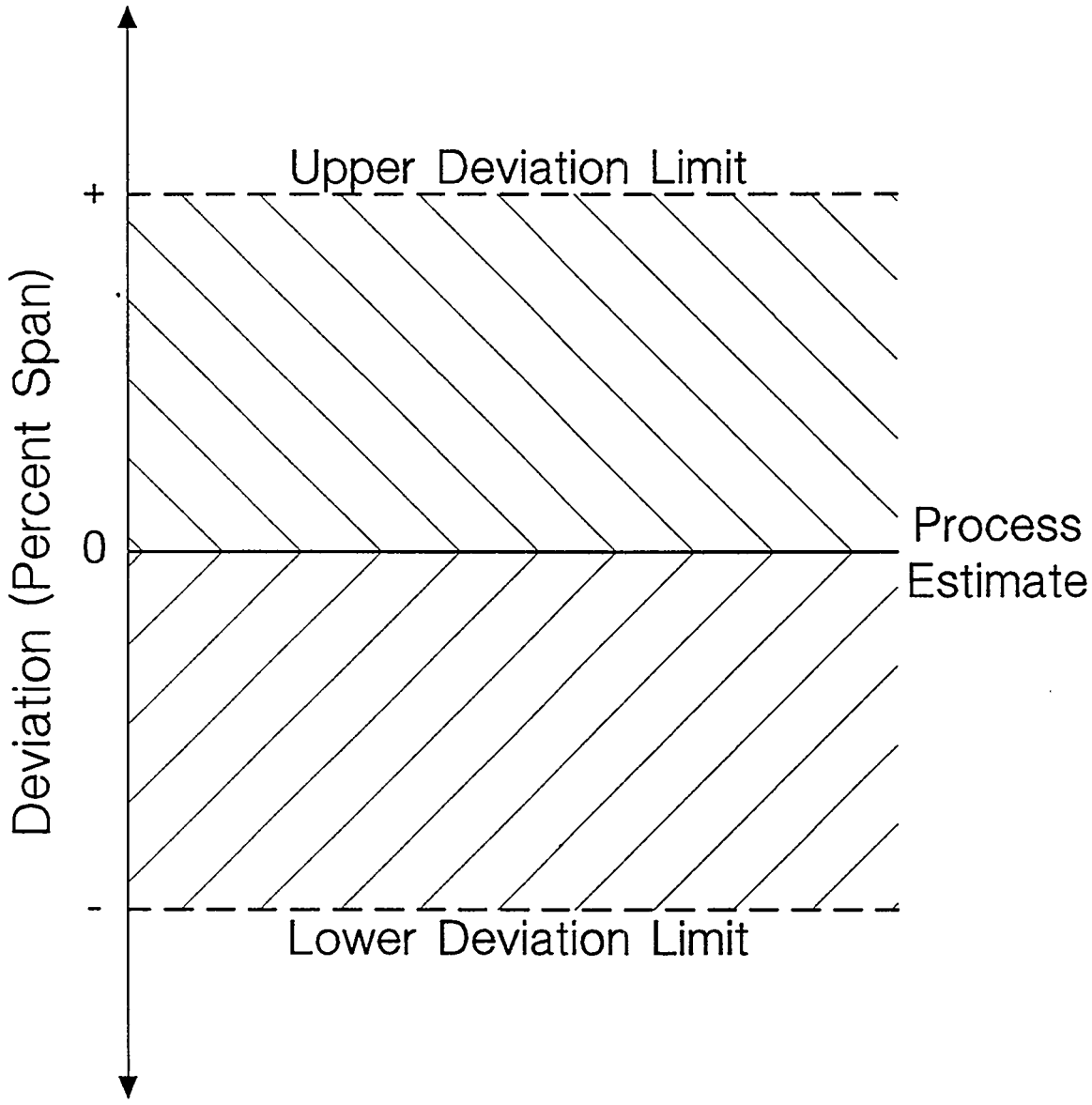


Figure 4. Illustration of Channel Deviation Limits

6.1 Laboratory Validation

The validation of the on-line monitoring system was accomplished through both laboratory and in-plant testing. A laboratory test loop was constructed and instrumented with a variety of nuclear grade sensors which were connected to a Westinghouse Model 7300 instrumentation system of the type used in many nuclear power plants. The on-line monitoring system was used to acquire data from the instrument channels while the loop processes were cycled through a variety of states such as increasing and decreasing ramps and steady-state operation as would be seen in typical nuclear plant operations.

While monitoring the data, the calibrations of one or more of a group of redundant instrument channels were manually altered in order to simulate calibration shifts. A series of small calibration shifts was periodically introduced into the channels to simulate the effects of calibration drift over a period of time. The actual amount of calibration change was determined by the manual calibrations performed on the instrument channels before and after each test run. This result was then compared to the results of the on-line calibration analysis as a means of determining the accuracy of the on-line monitoring system. Figure 5 shows typical results for one pressure transmitter during a series of test runs.

6.2 In-Plant Validation

An on-line instrumentation monitoring system was installed at the McGuire Unit 2 Nuclear Power Plant in February 1992. The system monitors the outputs of 170 instrument channels at the plant. The signals monitored include the primary coolant temperature, core exit temperature, neutron flux, reactor vessel level indication system (RVLIS), and various pressures, levels, and flows. The steady-state outputs of the instrument channels are sampled once every hour, although the sampling rate has been varied throughout the project in order to establish the optimum parameters for the system. The system continues to operate successfully at the McGuire plant.

For validation purposes, the deviations from the process estimate for each channel, as calculated by the on-line monitoring system, were compared to the manual calibration results performed on the channel instrumentation at the end of the most recent fuel cycle. Due to inaccuracies involved in the manual calibrations, as well as the errors due to the difference in the calibration environment and the actual operating environment, exact correlations between the two results were not expected. However, as seen in Figure 6, the results of these comparisons show that the differences between the results from the on-line monitoring system and the manual calibrations are usually smaller than the channel uncertainties in most cases.

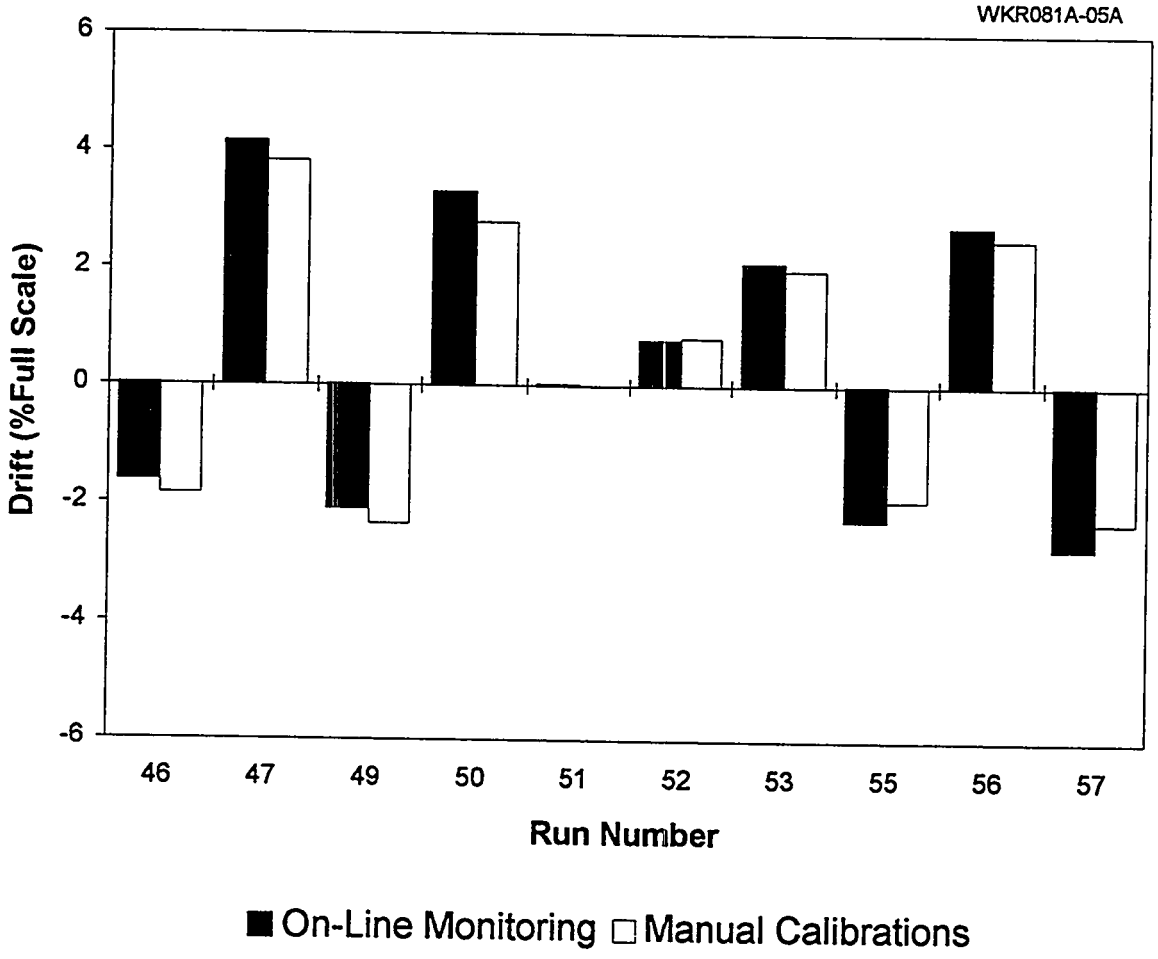


Figure 5. Example of Laboratory Validation Results

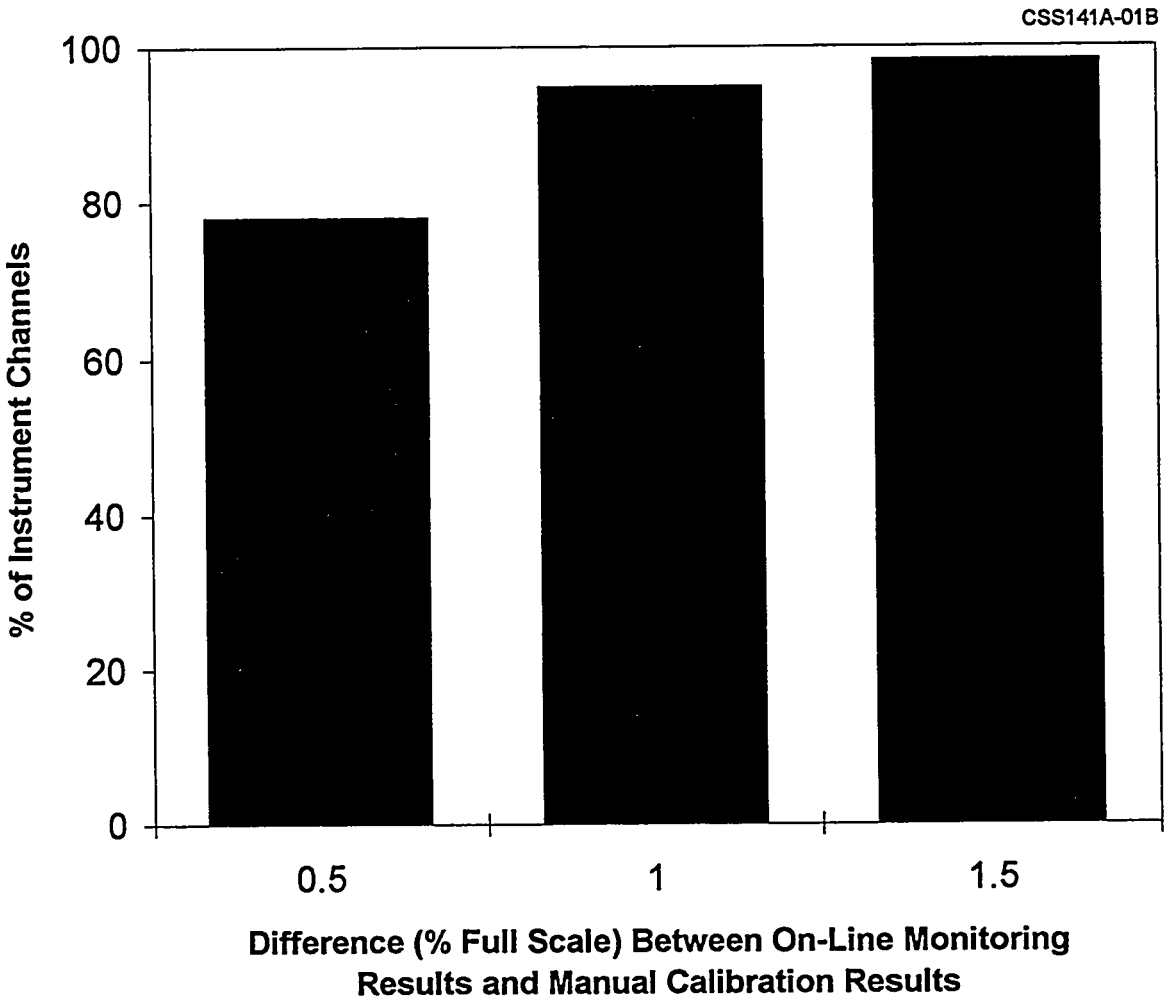


Figure 6. In-Plant Validation Results for the On-Line Monitoring System

7. CONCLUSIONS

An on-line monitoring system for testing the calibration of process instrumentation channels in nuclear power plants has been developed and validated. This system periodically scans the outputs of the instrument channels and compares them to estimates of the processes they are monitoring. If the deviation of the channel output from the estimate exceeds a predetermined limit, the channel is defined as out of calibration. The instruments in the channel would then require manual adjustments to bring the channel back into calibration.

The use of an on-line calibration monitoring system offers many advantages over the typical practice of periodic manual calibrations on nuclear plant instrumentation. The major advantage is the remote identification of suspect instrument channels which can reduce the number of manual calibrations required. This can produce significant cost savings to utilities and a reduction in radiation exposure to plant personnel. Also, the potential for human error and damage to plant equipment is reduced by employing this technology.

ENGINEERING DEVELOPMENT OF A DIGITAL REPLACEMENT REACTOR PROTECTION SYSTEM AT AN OPERATING US PWR NUCLEAR POWER PLANT

INSTALLATION AND OPERATIONAL EXPERIENCES

M. H. Miller, Senior Engineer
Duke Power Company
Oconee Nuclear Station
P O Box 1439 M/C ONO1ES
Seneca, SC, USA 29691

AEA Technology
Technical Products Division
Winfrith, Dorchester, Dorset
United Kingdom DT2 8DH

INTRODUCTION

The existing Reactor Protection Systems (RPSs) at most US PWRs are systems which reflect 25 to 30 year-old designs, components and manufacturing techniques. Technological improvements, especially in relation to modern digital systems, offer improvements in functionality, performance, and reliability, as well as reductions in maintenance and operational burden. The Nuclear power industry and the US nuclear regulators are poised to move forward with the issues that have slowed the transition to modern digital replacements for nuclear power plant safety systems. The electric utility industry is now more than ever being driven by cost versus benefit decisions. Properly designed, engineered, and installed digital systems can provide adequate cost-benefit and allow continued nuclear generated electricity.

This paper describes various issues and areas related to an on-going RPS replacement demonstration project which are pertinant for a typical US nuclear plant to consider cost-effective replacement of an aging analog RPS with a modern digital RPS.

The following subject areas relative to the Oconee Nuclear Station ISAT™ Demonstrator project are discussed:

- Operator Interface Development
- Equipment Qualification
- Validation and Verification of Software
- Factory Testing
- Field Changes and Verification Testing
- Utility Operational, Engineering and Maintenance Experiences with Demonstration System
- Ability to operate in parallel with the existing Analog RPS

Replacement Digital RPS Demonstration Project

AEA Technology and Duke Power Company are collaborating on an Inherently Safe Automatic Trip System (ISAT™) Demonstration Project at Duke's Oconee Nuclear Power Station in Seneca, South Carolina. Oconee and Duke's other nuclear facilities desire to maintain a current working knowledge of RPS replacement strategies and vendor products. While no commitment is made on the part of Duke or Oconee to replace the current RPS, this demonstration project allows Duke/Oconee to evaluate a potential replacement strategy that is available to the worlds nuclear electric generating community.

Duke and AEA in June, 1994 completed installation of an ISAT™ dynamic safety system demonstrator in the control interface portion of the Oconee RPS. AEA provided the ISAT™ hardware and assisted in hardware and software checkout and testing. Duke provided engineering and technical support as well as installation resources for the ISAT™ hardware.

The original RPS was supplied by B&W and originally manufactured by Bailey Meter Company. The RPS consists of Bailey 880 and 885 analog electronic modules with some use of Science Applications International Corporation (SAIC) signal converters. The SAIC signal converters are used to convert 4-20 milliAmp (mA) transmitter inputs into 0-10 Volt DC (VDC) system level signals.

ISAT™ receives 6 analog and 8 discrete signal inputs. ISAT™ connects to isolation amplifiers for the analog signals. These isolation amplifiers are also used to provide signals to the plant computer. ISAT™ connects to relay contacts for the discrete signals. Coil to contact clearance is provided as the isolation methodology for the discrete inputs.

ISAT™ replicates the trip functions of a complete Oconee RPS channel. ISAT™ has operated flawlessly in parallel with Oconee's RPS Channel A for nearly 6 months.

The ISAT™ Demonstrator consists of three 5.25" (3U) high, 19" digital equipment racks, a signal interface terminal strip and a Nixdorf-386 Personal Computer (PC) which acts as the ISAT™ monitor. An additional PC was also supplied with the ISAT™ demonstrator for plant input signal simulation and system response testing. This PC is not connected to the system except for hardware or software checkout after maintenance or for testing and verifying software changes. The three 19" racks (signal conditioner, data collector & trip processor) and interface terminal strip are mounted in Oconee's RPS Channel E

(Control Interface) cabinet while the PC is located at the rear of the control room on a table convenient for engineering and operator interface. Temporary cabling was installed to connect Oconee's RPS Channel A inputs to the AEA ISAT™ input signal conditioning equipment. Fiber optic cabling connects the ISAT™ electronic racks and the ISAT™ monitor PC. All cabling was routed in the control room suspended ceiling. 120 volt AC (VAC) power for the electronic racks is supplied from RPS Channel E cabinet power source through a isolation breaker and internal ISAT™ fusing. ISAT™ PC monitor power is from a convenience receptacle in the control room.

An integral part of the ISAT™ Demonstration project is the development of a generic ISAT™ Topical Report for submission to the USNRC.

Engineering Development Activities

Operator and Engineering Interface Development:

During the development of the ISAT™ equipment for installation at Oconee, the operator and engineering interfaces were reviewed for future RPS upgrade strategies both at Oconee and at the other Duke nuclear facilities. The existing ISAT™ display equipment and methodology for the Dungeness 'B' nuclear power plant in the UK were reviewed against the Oconee control room display arrangements. Oconee and many other nuclear power plants are leaning towards replacement operator interface strategies which use 19" and larger CRTs as the display hardware and "Windows" type platforms for display methodology. The ISAT™ monitor specification and display screens were provided to Oconee Operating and Engineering personnel for human factors and functional reviews prior to final development by AEA. The Oconee ISAT™ monitor uses OS/2 and "Windows" type displays for operator and engineering interfaces.

Equipment Qualification:

Hardware

Equipment qualification issues are an integral part of the engineering development of the ISAT™ Demonstrator development at Oconee and for application at other PWR and BWR plants. ISAT™ must be qualified to Environmental Qualification (EQ) standards required by the US nuclear power industry. Presently, the US nuclear industry and the rest of the world's nuclear industry do not operate from a common base of equipment

qualification standards. Each vendor must qualify equipment in a manner which is transferable (documentation-wise and test specifics-wise) across different nationalities or risk repeating tests to meet nation-specific requirements. Because of location based seismic and environmental differences across the US using the same standards does not guarantee a straight forward equipment qualification specification process. Interactions with Duke Power's EQ and seismic qualification groups have provided guidance on qualification parameters which would allow single seismic and environmental testing to cover a majority of the US plants.

The ISAT™ hardware is scheduled to undergo seismic and environmental qualification testing in 1995. It is the goal of AEA Technology, with Duke's engineering assistance, to qualify ISAT™ hardware to generic environmental and seismic qualification profiles.

An additional area for testing and equipment qualification of digital replacement protection systems is Electromagnetic and Radio Frequency Interference (EMI & RFI). The ISAT™ hardware has passed UK EMI & RFI testing to IEC standards as part of the Dungeness 'B' equipment specification. ISAT™,however, has not yet been tested for EMI & RFI using guidance from any US standards or other relevant EMI & RFI documents. EMI & RFI testing is planned in 1995 to support the topical report process.

The ISAT™ will also undergo power source harmonics testing and system heat output measurement as part of equipment qualification and system development.

Validation and Verification of Software:

Software Verification and Validation (V&V) enables confidence and trust in safety-related software systems and components, as well as being a comprehensive part of the regulatory approval process. Many standards are available to use as reference for software V&V. US Standard ANSI/IEEE-ANS-7-4.3.2 and International Standards IEC-880 and 987 are some of the widely quoted software V&V standards. Many others also exist which address various aspects of the Software V&V issue.

IEEE Standard 610.12-1990 defines software V&V as, *"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."*

ISAT™ software has undergone extensive testing, validation and verification in the UK during development for application at Dungeness 'B'. ISAT™ software programs are described in proprietary AEA Technology Software Design Specification Documents.

The software used in the Oconee ISAT™ Demonstrator has undergone partial V&V processes and complete functional testing. While this would not be the case for an actual RPS replacement, it is justified remembering that this demonstrator has no actual trip functions, to limit AEA's overall project expenditures. The ISAT™ Demonstrator software underwent some "White-Box" testing as part of the software developmental process and conventional "Black-Box" testing as part of the factory checkout testing via the factory test schedules described below. Although a complete software life-cycle verification and validation process was not used, the processes used produced a high quality product for use in the Oconee ISAT™ Demonstrator project.

Upgraded software under development for the ISAT™ Demonstrator at Oconee will undergo formal V&V testing prior to installation utilizing AEA Technology procedures and guidance found in various IEC Standards and other UK Standards. An assessment of the equivalency of the ISAT™ software V&V process to US standards will be included in the Topical Report submittal to the USNRC.

Factory Testing:

In April, 1994, factory testing was initiated on the ISAT™ Demonstration unit intended for installation at Oconee. A Duke/Oconee representative witnessed the factory acceptance testing at AEA Technology's Winfrith assembly location in the UK.

Test schedules had been developed and approved by both parties for the ISAT™ Demonstrator. These test schedules rigorously tested the functionality of the ISAT™ hardware and the displays created for operator and engineering interface. The test schedules were intended to test overall system functionality and not equipment qualification. These test schedules in essence perform "Black-Box" testing on the system. As mentioned above, equipment qualification and software V&V are still ongoing.

AEA Technology and Duke/Oconee personnel both actively participated in the test schedule routines. During the functional checkout, some minor discrepancies between the test schedules and the actual hardware were noted. These proved to be entirely documentational in nature, yet validated the objectives the test

schedules were meant to achieve. Factory Testing also included a final review of the PC display screens. Some changes were identified and were to be implemented after the hardware was shipped and installed due to shipping constraints between the UK and the US.

Field Changes and Verification Testing:

The software delivered with the ISAT™ had been produced in accordance with the Trip Algorithm Specification agreed upon by Duke Power. It was subsequently discovered by Duke that the specification quoted Technical Specification safety limits as trip settings rather than the actual RPS system set points actually used in the RPS channels. This set point arrangement employeed at Oconee involves setting the RPS to trip inside the boundary of the Technical Specifications. This configuration provides a margin of conservatism for RPS actions in order to prevent exceeding Technical Specification limits.

AEA Technology and Duke personnel then connected the AEA plant simulator PC to the ISAT™ Demonstrator equipment mounted in RPS Channel E. The following work was then performed.

1. By injecting input signals from the simulator, the factory test schedule was run to confirm the ISAT™ Demonstrator system was correctly functioning while installed in RPS Channel E with the original trip settings corresponding to the Technical Specification safety limits.

2. PROMs and monitoring software were then changed to install the trip settings corresponding to the actual RPS Channel A set points. This involved changing a set of two PROMs in both the Trip Processor and the Data Collector. The PROMs reflected changes to the set points and test data. Correspondingly, new monitor program software was also installed from a diskett.

3. The new software at both the ISAT™ Demonstrator and the ISAT™ Monitor was then functionally checked by using the plant simulator PC to inject simulated input signals into the Signal Conditioner rack. A revised factory test schedule (Reviewed and Approved by both AEA and Duke) was used to validate the correct installation of the new RPS based set points on an individual trip string basis.

The actual field wiring was then also checked to provide additional assurance that proper connections had been made during execution of the ISAT™ Demonstrator installation procedure.

(Note: The Oconee Temporary Modification installation procedure called for double verification of the field connections. This activity actually made use of the installed RPS test capabilities to triple verify that the proper RPS signal was connected to the correct ISAT™ Demonstrator input.)

RPS Channel A RC Pressure and Temperature variables were driven into a tripped state. In both instances, the ISAT™ Demonstrator replicated the RPS channel trips.

Changes to the monitor software included an additional margin to trip calculation and minor wording corrections as requested by Duke Power/Oconee during factory testing in the UK.

Utility Operational, Engineering and Maintenance Experiences:

Since installation of the ISAT™ RPS Demonstrator in June, 1994 almost 4 months of operation have been accumulated. During this time, the ISAT™ Demonstrator has functioned flawlessly. Weekly surveys of system status are made by Oconee personnel to observe plant process signal readings.

Operational Experiences

The ISAT™ Demonstrator hardware is installed in the control room inside the RPS Channel 'E' cabinet. The ISAT™ Demonstrator PC monitor is located at the rear of the combined Oconee Unit 1 & 2 control room. Oconee engineering personnel have demonstrated the ISAT™ Demonstrator operator interfaces and displayed the system hardware for numerous operating shift members. Since this is a demonstration project and not intended as a functional replacement of any of Oconee's RPS functions, the direction of operator experiences has been to gather actual reactor operator comments on informational interfaces with the ISAT™ Demonstrator. Virtually all comments have been postive in nature with helpful commenting on the look and feel of the interfaces. Much discussion has ensued concerning overall I&C system upgrade integration and implementation strategies regarding systems such as the ISAT™ Demonstrator into the existing Oconee control room arrangement.

Engineering Experiences

Shortly after Oconee Unit 1's return to near full power and during one of the weekly ISAT™ Demonstrator surveys, it was noticed that the ISAT™ Demonstrator was in the tripped condition. This tripped condition did not match the present plant condition. The root cause of the ISAT™ Demonstrator trip was

identified as an incorrect Reactor Coolant Flow gain. The ISAT™ Signal Conditioner had been configured with an incorrect gain for the two RC Loop Flow signals. Oconee engineering personnel did not provide the correct gain value for RC Loops A&B Flow to AEA Technology.

When the signal connections were determined, Oconee engineering personnel did not recognize the relationship of the output signal from the Bailey RPS to the internal use of the signal. The engineering personnel failed to correlate the difference in signal levels used and hence, the gain value was missed. The lesson learned from this instance is that in-depth and detailed system functional requirements are necessary to assure correct implementation of a replacement system. A complete understanding of the translation of existing system functions to the new system requirements is absolutely necessary. These responsibilities fall in the area of plant system engineers.

This RC Loop Flow gain condition has caused the flow related trip function to be disabled. The trip function is known as the Flux/Flow/Imbalance Trip. The disabling of the trip function was carried out by putting the ISAT™ Demonstrator RC Loop A Flow Bypass Switch in the Bypass position.

AEA Technology and Oconee personnel identified the corrective actions necessary to return the ISAT™ Demonstrator to full functional capability. AEA Technology will revise the Signal Conditioner software to provide the correct gain factor for the RC Loop Flows. AEA Technology personnel will then implement the software changes (through PROM replacement) and AEA Technology & Oconee and AEA personnel will conduct functional verification and validation testing on the installed equipment using the previously identified Test Schedules.

Maintenance Experiences

The Oconee ISAT™ Demonstrator has not required any maintenance in the time it has been installed.

Original installation was extremely straight forward. AEA Technology and Oconee personnel met twice prior to installation to review and plan the installation process and mounting of the hardware. AEA fabricated mounting brackets for the hardware which required a minimum of drilling to the RPS cabinets. The ISAT™ Demonstrator racks are mounted on tray-like brackets which are bolted to the structural frame work of the RPS cabinets. The racks are then secured on the front face to standoff brackts bolted to the same mounting frames. This makes for a very rigid

mounting which would make an appropriate starting point for mounting strategies for other RPS cabinet types or installations.

Note that at Oconee, the ISAT™ Demonstrator is mounted in the control interface portion of the RPS. This is a non-safety interface portion of the RPS and did not require seismic mounting of the ISAT™ Demonstrator hardware. The seismic integrity of the cabinet mount was reviewed and determined satisfactory for the temporary installation of the demonstrator.

Parallel Operation with Existing RPS:

As can be surmised from the above descriptions, the ISAT™ Demonstrator operates in parallel with the installed Oconee RPS.

While this is only a demonstration activity and has no real control rod trip outputs, an actual replacement installation could be configured which would place a complete ISAT™ RPS replacement in parallel with the existing analog RPS. ISAT™ could be connected through qualified isolators to the field sensors and a trip output confirmation indication provided in lieu of the actual ISAT™ connection to the control rod drive trip system. The ISAT™ system could then operate completely in parallel with the existing system, and at a later time (typically after one fuel cycle) the ISAT™ system could be connected directly to the field sensors and the reactor trip components.

This method of installation and system replacement would allow plant operations, engineering and maintenance personnel to become completely familar and comfortable with the operation of the new ISAT™ based RPS replacement.

Summary

General Conclusions:

The ISAT™ Demonstrator project at Oconee is in the 4th month of a scheduled 18 month project duration. Duke expects the project benefits to be worth much more than the financial and resource investment. The benefits that Oconee expects are:

- Working knowledge of the benefits and liabilities of a specific RPS replacement strategy. These include expected hardware costs, installation impact, regulatory impact maintenance cost savings, potential trip string margin improvements, as well as, overall control room layout and operator burden impact.

- Comparability knowledge between various available RPS replacement strategies. Presently, there are considered to be three actively marketed digital based strategies for RPS replacement at Oconee. Each offer different benefits and liabilities. Oconee has actively installed and is testing and evaluating two of them. Experience will prove the best guidance for Oconee's future plans.

- Competitive marketplace advantages by having detailed experiences and knowledge gained at low cost regarding potential expenses to support continued operation of Oconee if a RPS replacement is warranted.

Vendor Interactivity:

AEA Technology has been a very open and responsive partner. From the beginning, the partnership has been productive and beneficial. AEA's experience in the development of products for the nuclear power industry has been borne out in the compact yet functional design of the ISAT™ Demonstrator. Installation was very straight forward and adequate documentation provided. Due to the time zone differences between the UK and the US, vendor/utility communication patterns developed (Morning US time/Afternoon UK time). Monthly progress/project meeting were held during 1993 and up through project installation in June, 1994.

Duke/Oconee is acting as sponsor for the topical report review with the USNRC. While topical report submittals will be made directly to the USNRC from AEA, with copies going to Duke/Oconee, billing for the review process will be handled by Oconee with reimbursement from AEA.

The AEA Technology and Duke/Oconee partnering is an earnest commitment by both parties.

Regulatory Interactivity:

Regulatory interactions by AEA and Duke/Oconee have been very postive. The perception is that the USNRC is supportive of new technologies and products from outside the US becoming available to the domestic nuclear industry. The USNRC and AEA have had numerous technical interchange meetings at which various aspects of system design, system functionality and regulatory processes have been discussed.

Representatives from the USNRC have visited AEA Technology in the UK. The regulatory process has been reviewed with AEA since they are new players in the domestic market. Regulatory hurdles still exist, but the process began early and communication lines are continuously open and frequently accessed.

While domestic upgrades of RPS's in the US stopped because of cost concerns and licensing uncertainties, the industry and the regulators have been progressively been resolving those licensing uncertainties. Various industry groups with timely regulatory interaction have been pro-actively resolving these critical issues. 1995 is poised as the year where the uncertainties surrounding licensability of replacement safety-related digital are resolved and the utiltiy industry has a clearer, more prescriptive process for digitial safety system replacement.

While the licensing arena may become clearer and potentially more stable, the competition envisioned by most electric utility management in an open electrical generating market may add other unknown dimensions to major plant I&C system replacement considerations and cost-benefit analyses.

EUROPEAN STANDARDS AND APPROACHES TO EMC IN NUCLEAR POWER PLANTS

Dr D J Bardsley, Mr S R Dillingham & Mr K McMinn
AEA Technology, Winfrith, Dorset, UK

ABSTRACT

Electromagnetic Interference (EMI) arising from a wide range of sources can threaten nuclear power plant operation. The need for measures to mitigate its effects have long been recognised although there are difference in approaches worldwide. The US industry approaches the problem by comprehensive site surveys defining an envelope of emissions for the environment whilst the UK nuclear industry defined many years ago generic levels which cover power station environments. Moves to standardisation within the European community have led to slight changes in UK approach, in particular how large systems can be tested. The tests undertaken on UK nuclear plant include tests for immunity to conducted as well as radiated interference. Similar tests are also performed elsewhere in Europe but are not, to the authors' knowledge, commonly undertaken in the USA. Currently work is proceeding on draft international standards under the auspices of the IEC.

INTRODUCTION

AEA Technology is a science and engineering business which sells technical safety and environmental services and products to industries and governments around the world. AEA Technology has evolved from the United Kingdom Atomic Energy Authority and has an annual turnover of £250M.

Winfrith Safety Systems Department is part of AEA Technology which has been involved with reactor instrumentation for over 30 years. In particular it has had a significant role in assessing the need for EMI considerations in reactor instruments and in designing appropriate practical tests. The department is actively involved with EMI testing on UK nuclear plant and has recently completed a programme of EMI consultancy, factory and site tests on the UK's first PWR at Sizewell B.

ELECTROMAGNETIC INTERFERENCE (EMI)

The sources of EMI are wide and various ranging from power controllers (2 to 15kHz) and digital switching (up to 100MHz) to radio transmissions (1GHz) and may be broad or narrow band, continuous or discontinuous in nature. The interference generated by these sources may couple to the reactor protection system by either radiated (via the atmosphere) or conducted (via metallic structures) methods causing spurious instrument readings. One of the most sensitive areas is the neutron flux instrumentation where signal levels are very low and these systems need special attention. However similar problems can also occur on signal leads from a wide variety of plant sensors as well as in signal conditioners, bistables and even in logic circuits. Therefore the potential for spurious plant trip caused by EMI exists.

Since the neutron flux instrumentation system is probably the most sensitive area, most attention has been given to that area. In a nuclear reactor unexpected excursions in the neutron flux level are considered unsafe and they are usually made to trip (shutdown) the reactor. A more serious problem arises however when interference prevents an instrument from tripping causing a fail danger situation which must obviously be guarded against. The neutron flux control **system** must therefore be electromagnetically compatible within its environment to avoid 'fail danger' situations and unnecessary reactor trips. To ensure this is the case there exist standards and procedures to guard against the effects of EMI. In the UK two installed system EMI immunity tests have been developed for the nuclear industry: they are the CEGB specification DN5 (which predates but corresponds to IEC 801-3) used to cover radiated interference sources and the AEA Technology specification AEEW R919 for conducted and mains borne interference.

DEALING WITH THE PROBLEM OF EMI: US AND UK APPROACHES

The US presently has no one specification which the nuclear industry follows for testing equipment for EMI immunity. The general approach is to carry out a comprehensive site

survey at the power station (each survey apparently different) to obtain levels of background interference. Various data are now available on the level of radiated emissions at several sites and it is proposed that in the near future a series of equivalent surveys for conducted emissions will be performed. These results can then be used to specify the immunity requirement for instrumentation purchased in the future. There is a recommended practice for a comprehensive site survey [1] which has been followed at a number of power stations in the US and the results published [2]. In conjunction with this site approach it is of course true that equipment can be formally tested at a "Test House".

Until the introduction of the EEC directive on electromagnetic emissions [3] the UK nuclear industry had been less concerned with emissions and actively followed the line of improving instrument interference immunity, as it is our experience that not much is emitted from a well screened (ie. immune) circuit. In practice the levels of EMI disturbance vary over a wide range of amplitudes and choosing an "immunity level" is statistically based. The choice is based on a perceived acceptably low rate of high amplitude events. The UK levels were determined after surveys, admittedly less comprehensive than those currently proposed in the US, on UK reactors and practical experience shows that when a system is installed to the appropriate guidelines and specifications it operates essentially free from EMI problems. The US site surveys [2] appear to reinforce the justification for the immunity levels set for the UK in DN5 and AEEW R919 specifications.

In the UK the philosophy regarding EMI is changing slightly as a result of the EEC Directive on EMC. At the present time an informal arrangement exists where subsystems are tested independently (increasingly to the requirements of the Directive) and the whole system is then tested on site to satisfy UK licensing requirements set by the Nuclear Installations Inspectorate (NII). The site tests acceptable to the NII are DN5 and R919. In the future (January 1996) it will be a legal requirement that equipment satisfies the formal standards specified by the EEC Directive. In practice this will mean that subsystem tests are unchanged. Any installed protection system (such as a neutron flux measurement channel) however, is likely to be accepted as "too large" for the standard tests and a formal assessment route to qualification is proposed. This is known as the Technical Construction File Route. It will entail carrying out the long accepted DN5 and R919 tests on the installed equipment, correlating these with the subsystem tests and submitting a formal report to a "competent body" appointed by the UK DTI. The competent body assesses the report and will pass or fail the installation on the basis of the construction file. The equipment will not legally be allowed to operate without the approval of the competent body.

STANDARDS AND TEST METHODS OF IMMUNITY TESTS

Radio Frequency Interference (RFI)

In Europe the specification which covers the immunity testing of electronic instrumentation to radiated electromagnetic interference is IEC 801-3. IEC 801-3 requires that the instrument

under test be irradiated by an electric field of 10V/m over the frequency range of 27MHz to 500MHz. Other field strength levels exist within IEC801-3 for other types of equipment. The specification DN5 used in the UK modifies IEC 801-3 for use specifically on nuclear power stations. The main differences are the frequency range, which has been extended upward to cover mobile communication transceivers in the 900MHz band, and coverage of instrument testing in sites other than 'open field'. Military standards MIL-STD-461D and MIL-STD-462D cover the immunity testing of equipment to RFI in the US.

Within specifications, such as the US military standards, which cover such a variety of instrumentation, the levels of equipment immunity are not defined. It is therefore up to the power station or the NRC to decide what 'acceptable' instrument deviation is in the presence of RFI. The DN5 specification, being applied only to reactor instrumentation, has inherently defined pass/fail levels.

AEA Technology have in recent years developed an automated test system to cover the requirements of both IEC 801-3 and DN5 specifications using a lap-top computer and IEEE interface bus. This produces discrete frequencies rather than a continuous sweep but in the limit the discrete frequencies are separated by the resolution of the equipment used. This method is therefore more reproducible, less prone to errors and is quicker than any manual frequency sweeping method.

Conducted Interference

Analogous to the radiated interference immunity test in the US the conducted tests are also covered in the military standards MIL-STD-461D and MIL-STD-462D. They are, as for radiated tests general specifications for military use and not for nuclear power installations. Hence, no relevant immunity levels are stated. The method employed is that of bulk current injection. A ferrite clamp is placed around the cable under test and a current is induced in the cable screen by transformer action. This method has the advantage of ease of use but care must be taken to ensure that a current path exists all along the cable under test and that the attenuation of the induced current in the cable is acceptably low.

In Europe the specification for testing electronic equipment for conducted interference is IEC 801-6 which is at present only in draft form. This, as IEC 801-3, is a general specification and not specific to nuclear plant instrumentation. A conducted interference immunity test method developed by AEA Technology is detailed in the specification AEEW R919 [4]. This involves running a wire parallel to the system under test, terminating it at the far end in the characteristic impedance of the line and injecting a current down the wire. The current is then varied over the frequency range of 10kHz to 100MHz at a rate determined by the response time of the instrument. The injected current couples to the system under test inducing current flow in that systems screen. This simulates the effect of inherent earth currents flowing through the buildings metal structures such as cable conduit, water pipes and supports. The equipment developed for this test at AEA Technology is extremely useful in

diagnostic work and can, because of timing features, indicate where in the system the screening weakness lies. The injection test, as with the bulk current method, can provide early warning of system screening degradation if carried out on a regular basis. In the UK the test is repeated at regular interval as part of a life management programme and degeneration trends can be noted.

Mains Borne Interference

This involves superimposing large transient spikes onto the to the mains sine wave to simulate large switching power surges. These can occur in either series (live to neutral) or common mode (live, neutral to earth). Voltage transients on the power lines can be several kV in amplitude but, from surveys performed in the UK the most significant can be as high as 8Amps peak amplitude with rise times of a few nanoseconds. A 5kW pulse generator has been developed to simulate this kind of interference and the test procedure is detailed in AEEW R919.

The relevant IEC specification is IEC 801-4 which has quite different characteristic for the superimposed pulse. This has far less low frequency energy and greater high frequency energy. The low frequency energy is less as the pulse is applied to the mains lead via a 100nF capacitor.

The US military standard MIL-STD-462, now at issue D, covers this topic using two tests: impulse excitation and damped sine wave. The current is superimposed on the mains leads via transformer action using a current injection probe.

Detailed analysis of the US test has not been made so no comment can be made on its ability to represent the "real world". The pulse shape and energy levels in AEEW R919 and IEC 801-3 differ but at present it is contentious which is a more realistic test.

STANDARDS AND TEST METHODS OF EMISSION TESTS

UK

Emissions testing is not routinely performed on installed systems in UK reactors but, as discussed in relation to the EEC Directive, individual subsystems must meet various standards. For example, individual items of reactor instrumentation installed in the UK have to pass EN55022 Part B [5] which covers light industrial equipment for both radiated and conducted emissions. The testing is performed as a standard part of the type approval testing of new instrumentation. It is carried out as in the UK, as in the US, in a screened room at an accredited test house. AEA operates such a facility at one of its sites in the UK.

USA

There is no standard specific to nuclear plant but two existing standards, IEE 473-1985 [6] and MIL-STD-462/461 cover radiated emissions and, as mentioned previously site surveys are now being performed at US reactors to determine immunity levels for new instrumentation. This a long exercise since on-site surveys require months of monitoring to ensure the worst case emissions levels are measured. On an instrument level the are two standards, firstly the military standards mentioned earlier and the IEEE standard C63.4-1992 [7].

CONCLUSIONS

The minimising of emissions from electrical and electronic equipment is advantageous and is done for subsystems but for an installed system there will always be high levels of electromagnetic fields due to hand-held transceiver, communications and broadcast equipment. Therefore, emphasis should be put on testing equipment for interference immunity. The levels adopted in the UK through DN5 and Europe through IEC 801-3, have over many years practical use, been shown to be acceptable and the justifications for using the same test levels in the US are clearly supported by the EPRI report.

Conducted emission levels will be set for equipment within the UK by standards, under the EEC Directive. Though these currents may be low for electronic instrumentation such as reactor protection systems it will not be practicable to control to such low levels emissions from large generators and pumps. These are remote from the nucleonic instrumentation but induce earth currents to flow in the sensitive instruments screen via metalwork throughout the building. Therefore, conducted interference is potentially a serious problem. Tests such as AEEW R919 should be performed on system installation and on a regular basis to bring to light degradation of the systems screening performance.

The EEC Directive will bring a conformity to EMI testing of equipment throughout Europe. It will specify the standards to which the equipment must adhere to gain certification. As mentioned earlier there are two ways to certification: formal testing to the required standard or by means of a Technical Construction File. Extended systems such as neutron flux measurement systems will almost definitely need to follow the latter route.

The UK over many years has developed the immunity specifications DN5 and R919 for the nuclear industry. Although, developed for nucleonics they have found applications outside the nuclear industry. At present the US has little in the way of specifications solely aimed at the testing of nucleonic reactor control systems for EMI immunity.

REFERENCES

1 P D Ewing & K Korsah, "Technical Basis for Evaluating Electromagnetic and Radio-Frequency Interference in Safety Related Systems",ORNL/TM-12221, April 1994.

2 Electric Power Research Institute, "Guidelines for Electromagnetic Interference Testing in Power Plants", June 1994.

3 Official Journal No. L 139, Directive 89/336/EEC.

4 Fowler, E P "Interference immunity tests for nucleonic instrumentation", AEEW-R919, April 1974.3. E P Fowler

5 EN55022, "Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment, CISPR 22(1985) ed 1, 1986.

6 IEEE Standard 473-1985, "IEEE Recommended Practice for an Electromagnetic Site Survey (10 kHz to 10 GHz), June 1985.

7 ANSI C63.4-1992, "Radio-Noise Emissions from Low-Voltage, Electrical and Electronic Equipment in the Range of 10 kHz to 1 GHz, American National Standard Methods of", 1992.

CONTRIBUTION TO THE SAFETY ASSESSMENT OF INSTRUMENTATION AND CONTROL SOFTWARE FOR NUCLEAR POWER PLANTS

APPLICATION TO SPIN N4

Mme	B. SOUBIES
Messrs.	J.-Y. HENRY
	M. LE MEUR
	O. ELSENSOHN
	J. BOULC'H

INSTITUTE OF PROTECTION AND NUCLEAR SAFETY

SAFETY ASSESSMENT DEPARTMENT (DES)

STRUCTURE AND EQUIPMENT ANALYSIS OFFICE (SAMS)

CEA - FONTENAY-AUX-ROSES NUCLEAR RESEARCH CENTRE

1. INTRODUCTION

1300 MWe pressurised water reactors (PWRs), like the 1400 MWe reactors, operate with microprocessor-based safety systems. This is particularly the case for the Digital Integrated Protection System (SPIN), which trips the reactor in an emergency and sets in action the safeguard functions. The softwares used in these systems must therefore be highly dependable in the execution of their functions. In the case of SPIN, three players are working at different levels to achieve this goal:

- the protection system manufacturer, Merlin Gérin,
- the designer of the nuclear steam supply system, Framatome,
- the operator of the nuclear power plants, Electricité de France (EDF), which is also responsible for the safety of its installations.

Regulatory licences are issued by the French safety authority, the Nuclear Installations Safety Directorate (French abbreviation DSIN), subsequent to a successful examination of the technical provisions adopted by the operator. This examination is carried out by the IPSN and the standing group on nuclear reactors.

This communication sets out:

- the methods used by the manufacturer to develop SPIN software for the 1400 MWe PWRs (N4 series),
- the approach adopted by the IPSN to evaluate the safety softwares of the protection system for the N4 series of reactors.

2. METHODS USED BY THE MANUFACTURER TO DEVELOP THE SPIN SOFTWARES

2.1. Description of the SPIN

The protection system for 1400 MWe PWRs, like that for the 1300 MWe PWRs, consists of the Digital Integrated Protection System (SPIN), which is made up of:

- four redundant and independent Protection Acquisition and Processing Units,
- two redundant and independent Safeguard Logic Units.

These units trip scram circuit breakers and control the safeguard actuators when two of the four redundant measurements of a given physical parameter exceed a predetermined value.

In the case of the N4 series of reactors, each unit of the SPIN consists of a Motorola 68000 microprocessor. The software, the binary code of which is stored in REPROM, is written in C and in 68000 assembler code. Information is exchanged between the SPIN units via local area networks:

- eight redundant protection local area networks, of the NERVIA type, exchange information between the Protection Acquisition and Processing Units and the Safeguard Logic Units,
- two redundant signalling local area networks, of the NERVIA type,
- actuator networks internal to the Safeguard Logic Units which transport protection orders between the processors and the actuator cards.

Special units are incorporated in SPIN for periodic testing.

2.2. Development of SPIN softwares

The general approach behind this development work is set out in the Software Quality Plan of the manufacturer Merlin Gerin. The softwares were mainly developed on a computer assisted specification and code generation sets of tools (SAGA), by means of programming rules, and by separating the design and verification teams.

The process of developing a software in this context consists of seven stages, each of which gives rise to one or more documents. These stages and the associated documents are as follows:

- writing the software specifications, with the associated Software Specifications,
- the preliminary design stage, with the associated Software Preliminary Design dossier,
- the detailed design stage, with the associated Software Detailed Design dossier,
- coding stage, with the associated programming dossiers for the lists of instructions for the various components of the software,
- component integration testing stage, associated with the Software Integration Test dossiers.
- the software validation testing stage, with the associated Software Validation Test dossiers

Four of these documents (Software Specifications, Software Preliminary Design, Software Detailed Design and Software Validation Test) give rise to a review by the persons in charge of the design and verification teams and the quality assurance manager. These reviews come under the umbrella of "quality" actions during the development process.

Furthermore, the Software Specifications are submitted for approval to the designer of the nuclear steam supply system.

The process of development enters into its next stage after each satisfactory review.

The SAGA atelier takes part directly in several stages of the development cycle. It makes use of five tools:

- the specification tool,
- the code generation tool,
- the programming tool,
- the documentation tool,
- the administration tool.

The specification tool is used during the preliminary and detailed design stages. Its interactive graphical interface can be used to produce a top-down description of the software to be developed in terms of its components, which are in turn broken down into easy-to-program components.

The code generation tool is used to obtain the C code for the softwares mentioned above.

The programming tool is an aid to the programmer when designing and developing the component source program, which cannot be generated automatically using the previous tool.

it does this by suggesting a standard template and by checking compliance with certain writing rules. The interface for this component is generated automatically at the design stage.

The documentation tool is used as the preliminary and detailed design stages progress, and formats the written documentation associated with the components described using the specification tool.

The administration tool is used to manage access to atelier resources by the different users.

The programming rules must, in particular, ensure compliance with the provisions of standard IEC 880 "Computer software in nuclear power plant safety systems", and ensure that the programming remains uniform, thereby simplifying the task of testing and maintaining softwares.

Separate design and verification teams were used, as in the software quality plan for 1300 MWe PWRs, in order to increase the number of independent checks.

3. EVALUATION OF SPIN SOFTWARE BY THE NUCLEAR OPERATOR

The safety approach adopted by the operator consists in demonstrating compliance with the safety functions by studying those accident scenarios requiring the use of safety class systems or equipment which must satisfy design, manufacture and installation requirements.

In the case of the reactor protection system, the operator performs an independent validation of the SPIN safety software in addition to the provisions adopted in the manufacturer's quality assurance plan. He approves the specifications contained therein and performs audits, especially during the tests carried out during the software validation stage in the manufacturer's premises.

Furthermore, the tests carried out on each item of equipment in the SPIN with validated programs (Protection Acquisition and Processing Units and Safeguard Logic Units), and then on the SPIN and its interfaces with other systems, give rise to joint reviews between the manufacturer, NSSS designer and the operator.

4. METHODOLOGY USED BY THE IPSN FOR EVALUATING THE SAFETY SOFTWARES

The technical support body (IPSN-DES-SAMS) of the safety authority (DSIN) is responsible for carrying out any investigations they deem necessary in order to ensure that the methods and technicques used by the manufacturer and operator guarantee that the SPIN software reaches the expected level of safety and exhibits an adequate degree of testability and maintainability. In order to do this, the support body pay particular attention to the following issues:

- rational and thorough methods of developing softwares by following a specific quality assurance plan (documentation and code);
- strict programming rules for producing a testable and maintainable program (code);
- tests carried out to ensure sufficient coverage both in the manufacturer's premises and on site (simulation).

The assessment carried out by the IPSN does not cover all the equipment which makes up the SPIN, in view of their relative complexity. It was decided to limit the analysis to:

- all documentation associated with the SPIN technical specifications,
- a representative set of protection system functions.

The representative set of functions chosen for the safety assessment consists of two channels, one relating to a trip request and the other to a safety injection request. They each involve the functional units needed to perform a safety task:

- two process data acquisition units,
- a processing unit for this data allowing a partial trip to be executed corresponding to a trip request or a safeguard action request,
- a unit in charge of the majority vote controlling the scram circuit breakers and safeguard actions.

The softwares associated with this representative set of functions process one or more items of data from the process, from acquisition to the input terminals of the actuators. The methodology adopted to analyse the SPIN N4 softwares proceeds in successive steps to evaluate the various technical solutions put forward by the operator. Currently, there are six different steps involved in the evaluation of safety software:

- step 1, critical examination of the documents (see §4.1),
- step 2, evaluation of the quality of the code (see §4.2),
- step 3, determination of the critical software components (see §4.3),
- step 4, development of test cases (see §4.4),
- step 6, consistency study (see §4.5),
- step 6, robustness study (see §4.6).

Some of these steps are carried out in parallel, as is the case with steps 2, 3 and 5. Steps 1 and 2 are more specifically focused on a so-called static analysis, because they do not require running the program. Steps 4, 5 and 6 are focused on a so-called dynamic analysis. Step 3 is the transition between the static analysis steps and the dynamic analysis steps. In order to ensure an acceptable approach for the tasks to be performed and to provide the analyst with technical elements, special tools have been developed:

- a tool for modelling text in natural language to evaluate the completeness and consistency of specification and design documents,
- a static analysis tool which is used to evaluate the quality of programming and which, with its semantic analyser, is an aid for generating test cases,
- a tool which is used to determine the critical components in terms of the safety objectives which the software must meet,
- a simulation atelier which consists of the following tools:
  - a simulation and testing tool for carrying out dynamic analyses,
  - a tool for describing environment programs for the simulation,
  - a tool for processing the results which gives a graphical readout of the results of dynamic analyses.

The analyses set out in the sections which follow will enable the IPSN to meet the objectives stated above.

4.1. Critical examination of documents

An evaluation of the safety of the programmed systems is leading the IPSN to pass judgement on the relevance of information contained in the software specification and design documents, in respect of technical knowledge of the project and the standards relevant to the facility using these systems.

The examination of the protection system carried out as part of this evaluation takes account of the safety requirements of the installation, the system architecture and its specifications. The examination therefore consists in verifying the presence of all the functions needed to ensure that the installation is safe and to comply with the functional diversity which will make it possible to protect against common mode failures.

These functions make use of protection signals, for instance water-level in the steam generators, and result in protection actions being taken (scram or safeguard). Several protection signals appearing during a single accident sequence must be processed in different functional units of the SPIN (principle of functional diversity). This was the case, for instance, with the signals indicating very low pressure in the pressuriser and very high pressure in the containment, which arise during a loss of coolant accident (large break LOCA) and which are processed in two different functional units of the SPIN.

The development of softwares corresponding to the functions of the protection system is organised in a Software Quality Assurance Plan which gives rise to a very much documentation, throughout the development cycle.

This documentation consists of documents written in natural language (specifications, design, tests) and the source program itself.

The documentation is produced over a long time-scale, owing to the extent of this type of softwares.

Each document is analysed, not just to understand the functions performed, but mainly to check that there is no superfluous information (causes for complexity), or information which is incoherent or missing from the software documentation.

The AVIS method and its AVISO computer tool are an aid to examination involving the application of a systematic and thorough approach.

The method uses linguistic analysis to compile graphs showing the information set out in the document.

This operation relates each text element with its corresponding point on the graph.

This sort of modelling is more useful than a discursive or mathematical language, because it shows the relationships existing between the information contained in the text. The resulting overview can be used to focus attention both on the meaning and on the details of each piece of information.

This representation simplifies the task of examining the completeness and consistency of this information.

Besides, the references drawn up between the text and the graphic allow any anomalies picked out during the modelling process to be linked to the original text.

So, analysis of documentation produced over a long period of time and modified with each version of the softwares is more powerful by the ability of this tool to store information contained in the different texts together with observations and comments raised by the analysis.

4.2. Evaluation of the quality of the code

The sourcce program of the representative set of functions are analysed to:

- search for any constructions dangerous for the type of language used:
  - data flow anomalies (definitions and uses of variable values, types of variables etc.),
  - arithmetic expressions (parentheses, division by zero),
- search for an incorrect or over complex structure in the programs:
  - multiple input or output loops,
  - variable index loops,
  - inaccessible code,
  - unnecessary code,
- verifying compliance with those provisions of IEC 880 deemed important by the IPSN.

The components from which the programming anomalies were detected become so-called sensitive components. The testability and maintainability of these components are in turn evaluated. Some of these components, mainly those containing variable index loops, could be tested during the robustness study of the program, thereby allowing the verification of their behaviour under these conditions.

A first campaign of analyses was carried out using a static analysis tool (structural analysers of the MALPAS tool) on the program of one of the SPIN functional units. These results showed some feautures of the code which could affect the testability and maintainability of this program.

4.3. Determining the critical software components

The software of the chosen unit processes several channels. Those parts relating to the two channels selected (the essential components) must be distinguished from the representative set of functions.

Amongst these components, the so-called critical functions, whose failure is likely to cause a severe system malfunction must be identified.

This is carried out using the Failure Modes, Effects and Criticality Analysis (FMECA) adapted for software analysis. This is the first stage in the AFFUT approach, which is intended to determine the most important unit functions for the IPSN to test.

This approach consists in evaluating the effects of postulated failures on each function of the softwares in turn.

An index of relative importance can then be calculated for each function, by taking into account the number and severity of failures, and hence categorise them.

The second step in the AFFUT approach consists in studying the critical functions in detail by analysing all the tests performed by the manufacturer.

If these tests are not sufficient for ensuring that the postulated failures cannot occur, these critical functions performed by the components which are called up in turn will be the subject of additional tests as part of the consistency and robustness studies.

4.4. Developing test cases

This is a two-part stage. The first part is based on an examination of the manufacturer's tests with a view to the consistency study, the second is currently based on results from the semantic analyser of the MALPAS tool and is focused on the robustness study.

In the first part, the analyst selects from the series of manufacturer's tests those which correspond to specific system operating conditions in order to verify system behaviour.

In the second part, the study of the critical and sensitive components that the analyst adopted continue with the PEGASE tool. This is used to give all the functional paths which lead to the values which can be assumed by each output variable of the component in question. It can be used to find the ranges of values for input data by means of the conditional relationships which describe the functional paths.

Values are selected for the input data in order to activate the critical components during the tests.

This analysis can also be used to verify the ranges within which the data vary from their specification values.

Besides, this type of analysis shows the dependencies which exist between the input and output data, and makes it possible to verify that the program code and specification conform, if the software contains such information.

4.5. Consistency study

An evaluation of the programs of the representative set of functions gives rise to a dynamic analysis which can determine, in a first stage, how consistently these programs perform with regard to their specifications.

The consistency study can be used to verify, for the representative example cited earlier, the values assumed by outputs from these channels (for instance controlling a scram) when the inputs assume values selected by the analyst from the nominal operating range of the protection system. This study verifies the most significant aspects of the behaviour of the binary program which is actually used at the site.

The IPSN has developed for the purposes of this type of examination a set of tools which can simulate operation by execution of a binary program without recourse to equipment (CPU card, peripheral cards etc.) used on site. These tools, which are supported on a computer, make it possible to:

- compile an environment which reproduces the exchanges between each microprocessor and the circuits (clocks, communication circuits, memory etc.) which are associated with it in each unit of the protection system installed on site,

- run the binary programs of the units of the protection system by means of a microprocessor simulator, generating special files which track all interactions between the microprocessors and their environments, with a statement of the run time,
- present, in mimic form (time diagrams, curves etc.), the values assumed by the different variables monitored, in order to analyse simulation results.

The environment of the binary program and the microprocessor which runs it is simulated by developing special programs which replace the equipment called up by these programs. This development was carried out mainly by using a graphical description based on the SADT method.

Programs are run to take account of the values of the input variables given by the series of tests designed for this consistency study.

The implementation of such a simulated system is currently in hand. In a first stage, the normal operating conditions of the protection system will be selected to ensure that the model obtained using the environment developed for the purposes of this study is adequate. In a second stage, the program will be run to check the behaviour of the system in specific operating situations (degradation of the two-out-of-four voting logic, for instance) provided for in the specifications.

The simulated system and the associated tests series will be reused to verify that each version of the softwares works as well as before.

4.6. Robustness study

The main purpose of this study is to judge the behaviour of the programs of the representative set subjected to series of tests, defines in advance, which represent abnormal situations for the protection system or of the systems which provide it with information. The series of tests are focused on the critical or sensitive components detected during the previous steps. It sets in place an analysis which covers one area not touched on in the manufacturer tests.

This study makes use of the simulation tools set out for the consistency study, in order to create a more complete environment, making it possible in particular to arrive at certain internal program variables which are representative of the abnormal situation selected.

The results of the simulations obtained using the different series of robustness tests must be analysed to identify the state of each output variable of the system representative set of functions. This implies ascertaining the values which should be obtained for each test case. Special semantic analyses are carried out to calculate the expected values (Oracle).

An analysis of the simulation results is carried out to identify, for system outputs, the consequences of malfunctions introduced and to draw conclusions on the adequacy of system behaviour with respect of the missions it must perform.

5. CONCLUSION

The tools mentioned earlier are in operation or in the experimental stage and are based on technologies currently available. Improvements are being made continually in this area and could lead to the resources used to carry out one or more of these analyses being changed. The IPSN is devoting a considerable share of its efforts to develop research programs into these issues.

However, the evaluation methodology set out in the above sections can be considered to be a satisfactory basis for examining the various aspects of safety software. This is an evolutionary approach, and other possibilities have still to be explored. These cover, *inter alia*, the self tests included in the protection system equipment softwares, the exhaustive nature of which affects the dependability of this system. Similarly, the problem raised by the software common modes and the extension of this evaluation method to other types of "real time" system will be dealt with in greater detail in the near term.

BIBLIOGRAPHY

Bussac, J.P.[1], Jover, P.[2], Conflant, M.[2]
"The Introduction of Computer Systems into Nuclear Power Plant Instrumentation and Control: the French Safety Approach"
International Symposium on Nuclear Power Plant Instrumentation and Control
Tokyo, Japan. May 1992.

Soucies, B., Le Meur, M., Henry, J.-Y., Boulc'h. J.[1]
"Evaluation Methods for the Instrumentation and Control Safety Softwares of Nuclear Power Plants"
IAEA Specialists' Meeting on Software Engineering in Nuclear Power Plants: Experience, Issues, Directions
Chalk River, Ontario, Canada. September 1992.

Notes:

[1]Institute for Nuclear Safety and Protection CEA CENFAR
[2]Nuclear Installations Safety Directorate (DSIN) CENFAR

Use of Circadian Lighting System to Improve Night Shift Alertness and Performance of NRC Headquarters Operations Officers

T.L. Baker, D. Morisseau, N.M. Murphy, K.P. Buckley, J.J. Persensky

ShiftWork Systems, Cambridge, MA
Nuclear Regulatory Commission, Division of Systems Research, Human Factors Branch

We wish to thank the DSR and AEOD for initiating the NRC project, and maintaining a strong interest in the results. We would specifically like to thank Tim McGinty, Joe Giitter, and Ken Brockman for their immense amount of site support and assistance. Most importantly, we would like to thank all of the Headquarters Operations Officers who participated in this project.

Abstract

The Nuclear Regulatory Commission's (NRC) Headquarters Operations Officers (HOOs) receive and respond to events reported in the nuclear industry on a 24-hour basis. The HOOs have reported reduced alertness on the night shift, leading to a potential deterioration in their on-shift cognitive performance during the early morning hours. For some HOOs, maladaptation to the night shift was also reported to be the principal cause of: (a) reduced alertness during the commute to and from work, (b) poor sleep quality, and (c) personal lifestyle problems. ShiftWork Systems, Inc. (SWS) designed and installed a *Circadian Lighting System* (CLS) at both the Bethesda and Rockville HOO stations with the goal of facilitating the HOOs physiological adjustment to their night shift schedules. The data indicate the following findings:

- Less subjective fatigue on night shifts
- Improved night shift alertness and mental performance
- Higher HOO confidence in their ability to assess event reports
- Longer, deeper and more restorative day sleep after night duty shifts
- Swifter adaptation to night work
- A safer commute, particularly for those with extensive drives

Introduction

Shiftworkers invariably have difficulty staying awake while working the night shift, even after many years on the job. They also are unable to obtain satisfactory sleep during the day. This is primarily due to the fact that their internal biological clocks remain set to a daytime schedule. The mismatch between work and sleep schedules of the shiftworker and the biological timing system is the cause of a wide range of problems:

- **Productivity** is impaired. The performance of routine tasks becomes more difficult. Reaction times slow significantly. Judgment is diminished.
- **Safety** is compromised. Both the risk of employee accidents and the potential for industrial accidents increase.
- **Personnel costs** are higher. Shiftworkers are substantially more likely to suffer cardiovascular and digestive disorders. Shiftworkers also experience more frequent headaches, fatigue, stress, muscle pain, respiratory infections and general malaise.
- **Employee quality-of-life** suffers. Higher rates of divorce and suicide, as well as increased use of alcohol and drugs, have been documented. Frustration, low morale, and diminished job satisfaction are also common among shift workers.

In a series of studies beginning in the late 1970's, Dr. Charles Czeisler and his colleagues at Harvard Medical School reported that the human circadian timing system was very sensitive to variations in exposure to light and darkness during the 24-hour day (Czeisler 1978; Czeisler et al 1980, 1981, 1986, 1987, 1988, 1989, 1990; Kronauer 1987, 1990; Kronauer et al 1991, 1993, 1994). These findings challenged the conventional wisdom of the previous two decades, which stated that light was not a critical factor in the internal timekeeping mechanism of the human, also called the circadian pacemaker. Although these research findings were controversial when they were first published, the scientific community has now reached a consensus that the 24-hour pattern of exposure to light and darkness is by far the most important factor determining the phase position of the circadian timekeeping system in humans. Studies in many research laboratories have now convincingly confirmed the original findings of Czeisler and colleagues, and research in the circadian effects of light has become the focus of intense interest for both research and practical applications.

In 1990, Czeisler and co-workers first reported that maladaptation to night work, with its associated decline in alertness and performance, can be treated effectively with exposure to bright light during the conventional night shift working hours. (Czeisler et al 1990) These early studies used light of 7,000 to 12,000 lux intensity. A complete adaptation to night work was found when subjects were studied after four days of light therapy, as measured by both physiological parameters (core body temperature, cortisol and melatonin secretion) and behavioral parameters (subjective alertness, performance on computer test batteries).

One of the research results which has received relatively little attention, as compared to the shift in circadian phase of physiological and behavioral parameters, is that the duration of daytime sleep in these subjects increased by an average of two hours per day. Shiftworkers performing in normal room light did not show circadian rhythm shifts, or improvements in cognitive performance or sleep. Subjects in the bright light treatment group showed a consistent large (approximately 12 hours) shift in the rhythms of all physiological and behavioral parameters studied.

Since this study was reported, several investigators have independently confirmed that bright light exposure during simulated night shift work will increase performance, decrease sleepiness at work, and improve sleep patterns away from work (Eastman 1992; Dawson & Campbell 1991; Thessing et al 1994; Boyce et al, 1993). These studies have used Czeisler's strategy of exposure to bright light during the night shift, often coupled with avoidance of competing bright light during the desired sleep time away from work. Various researchers have reported increased cognitive performance, decreased physiological sleepiness (as measured by the Multiple Sleep Latency Test and subjective ratings), and increased sleep time during the daytime.

There are indications of immediate direct effects of bright light on alertness and performance, even on the first night of shift. The mechanism is still speculative, but probably involves suppression of melatonin and/or elevation of core body temperature (Campbell & Dawson 1990, Dawson & Campbell 1991, Strassman et al 1991; Lewy et al 1991; Myers & Badia 1993). These postulated direct effects of light are in addition to the circadian resetting which inevitably take place if a human is exposed to light at even 2-3 times the intensity of exposure, and may in fact be part of the same physiological process. It is highly unlikely that suppression of melatonin is important for the circadian shifting mechanism, since light exposure that lies outside of the window of melatonin secretion also causes circadian phase shifting.

ShiftWork Systems has licensed from Brigham and Women's Hospital the patented technology developed by Drs. Czeisler, Kronauer, and Allen of Harvard Medical School and Harvard University. Shiftwork Systems has developed a *Circadian Lighting System,* which uses precisely-timed bright lighting in the workplace to predictably reset the employees' biological clocks. The lights are installed only after an in-depth study of the workplace and of the individual employees' needs and requirements.

A *Circadian Lighting System* comprises three main components: a computer with specially designed software called the *Lighting Schedule Supervisor* (*LSS*), a computerized lighting controller, and high-intensity lighting luminaires.

- ***The computer software (LSS)*** calculates the lighting schedule (required timing, duration, and intensity) and transmits it to the controller. Lighting schedules are calculated using a set of mathematical equations derived from Dr. Czeisler's research. The *LSS* is customized to the work schedule and employees at each installation, and takes individual requirements into account. The *LSS* has a simple graphical interface which allows users to make roster and schedule changes easily.
- ***A computerized lighting controller*** stores the lighting schedules calculated by the *LSS*. The controller adjusts the intensity of light in the work area during the shift, according to the lighting schedule.
- ***Specially designed high-intensity luminaires,*** installed in the work area ceiling, provide the light necessary for shifting workers' biological clocks.

The intensity of light is adjusted throughout the work shifts. The lowest light level is about equal to normal baseline room lighting. The highest level is about the level of light outside on a cloudy day.

History of the Project

The project was divided into five tasks:

Task 1. Develop an experimental design, consisting of measures to validate the technology, and a plan for collecting the evaluation data. Based on discussions with the staff of the NRC Operations Center and the NRC's Division of Systems Research (DSR), SWS developed an experimental design that specifically addressed the needs of the NRC Operations Center. The design included:

- definition of baseline performance measures
- description of specific data to be gathered
- designation of responsibilities between SWS and the NRC with respect to data gathering, analysis and monitoring of participants while the experiment was in progress

This experimental design was submitted to the NRC Project Officer, who in conjunction with the NRC Operations Center staff, reviewed, commented on, and approved the design. This information also provided an understanding of the work schedule rotation and operational requirements. Measurement techniques used to determine the level of success of the project included:

- confidential questionnaires to all HOOs
- sleep/wake activity log books
- subjective self-rating scales of mood and alertness
- computer-based performance tests
- structured officer interviews

All measures were implemented three months before the intervention and were continued four months after the intervention. Questionnaires were done at the beginning of the three month baseline period and at the end of the four month intervention evaluation period.

Task **2.** Provide and install the *CLS*. SWS engineers assessed the HOO Station layout, usage and work flow patterns in order to establish optimal locations for the lighting hardware. The main objective was to provide maximum illumination while simultaneously minimizing glare on the instruments and CRT screens. Detailed engineering drawings were made and the hardware was manufactured. The *LSS* software was customized for the NRC.

To reinforce the effect of the lights, curtains designed to block out external light in the home sleeping environment were offered to all participating HOO's.

The *CLS* was installed in the HOO Station and activated on January 20, 1994.

Task 3. Support and train the HOOs in the use of the *CLS*.

- Dr. Charles Czeisler, chief scientific advisor to SWS, gave an educational seminar on the circadian lighting intervention. He presented the principles and research behind the technology as well as the expected benefits for the HOOs involved in the project.
- SWS distributed handbooks to educate the HOOs in optimal shiftwork adjustment practices to help them obtain maximum benefit from the *CLS*.
- SWS maintained a presence on-site for the initial post-intervention employee shift turnovers. Throughout the four-month evaluation period, SWS provided on-site and telephone consultation to the HOOs.

Task 4. Implement the experimental design. Subsequent to approval of the experimental design by the NRC Project Officer and the NRC Operations Center staff, SWS began the data collection phase of the project.

Task 5. Summarize the significant findings of the performance measures, in a final report.

Demographics and Work Schedule

Population Profile: Ten Headquarters Operations Officers were qualified to work in the HOO Station. Two of the ten officers were out of the rotation on special assignment at the time of the project. One officer had recently undergone a radial keratotomy, which is a laser procedure to change the corneal shape. He was excluded from the program; when he was on duty, light levels were not increased. Another officer opted to not participate in the program. In total, six officers participated in the project.

All of the HOOs are men. The six participants' ages ranged from 31 to 51 years. The median age was 41 years and the mean age was 40 years. These officers had been involved in night work for an average of 8.9 years and had been working the current schedule for an average of 3.6 years. They spent 96% of their day shift work time, and 95% of their night shift work time, in the HOO Station. All of the participants currently live with a spouse or roommate, and four (67%) have children living at home. The average commuting time was 50 minutes, ranging from 12 minutes to 110 minutes.

Data Collection Participation: All six participating officers completed the baseline and final evaluation questionnaires. All six participated in the ongoing and final structured interviews. Six officers submitted sleep/wake activity log books, while four of those six submitted logs for both the baseline and intervention period. Six officers participated in the Stanford Sleepiness Scale and subjective rating scales. Six officers participated in the computer-based performance tests.

Work Schedules: The HOO Station is staffed around the clock, with officers working on twelve hour shifts. The day shift (D) runs from 12 noon to 12 midnight (12 - 24), and the night shift (N) runs from 12 midnight to 12 noon (00 - 12). One complete rotation through the schedule takes 6 weeks; four weeks of 12-hour shifts and two weeks of 8-hour back-up or office shifts during normal daytime work hours. The table below shows the typical HOO schedule:

1	2	3	4	5	6	7
D	D	D	X	X	X	X
8	X	N	N	N	X	X
8	8	8	8	X	N	N
N	N	X	X	X	X	X
X	X	X	D	D	D	D
X	8	8	8	8	X	X

In this 42 day rotation, they work a total of seven 12-hour day shifts, seven 12-hour night shifts, nine 8-hour 'back-up' or office day shifts, and 19 days off (X).

Six of the ten eligible HOOs are assigned to the rotation or rotor at any given time, and will work the 12-hour night and day shifts in the HOO Station. One HOO is on duty at any given time, with a back-up officer on-shift during daytime hours (6:00 a.m. - 2:45 p.m.). The other remaining assignments for HOOs include special assignments, training, and daytime office work. During the course of the project, eight of the ten HOOs worked in the HOO Station in the rotor.

Intervention Methods

***Circadian Lighting System* Work Area Illumination:** The *CLS* was installed in the Headquarters Operation Center. Background lighting fixtures (both task and ceiling mounted) were left intact to provide lighting in the HOO station when the lighting system required "no additional lighting."

The level of light in the HOO Station before the installation of the *CLS* was approximately 50 lux. During the intervention period, the light level varied across the work shift. The Level 1, (or default level) remained at approximately 50 lux. Depending on the night of shift and the officer's personal preference, the system increased in intensity in three pre-set steps. Level 2 was between 800 and 1200 lux, Level 3 was between 2000 and 3000 lux, and Level 4 was between 4000 and 5500 lux of light. The positioning and direction of gaze of the HOO determined how much light actually reached the eye. The majority of higher intensity light exposures were at the start of a block of shifts, tapering off toward the end of the block of shifts.

Educational Sessions: HOOs attended an informational session presented by SWS training staff and Dr. Charles Czeisler of the Harvard Medical School. The sessions focused on circadian physiology and practices on- and off-shift that could help optimize the effects of the *CLS* for the HOOs.

Consultation: In addition to the educational sessions, SWS maintained a regular on-site presence at the HOO Station after the system was activated. SWS project managers provided suggestions on adaptation strategies in response to HOO feedback on how the system was working for them. SWS project managers also collected data on a regular basis and conducted structured interviews as scheduled.

Room-Darkening Curtains: HOOs were offered finished opaque window curtains for use in their home bedrooms. The intention was to create a dark sleep environment, more conducive to daytime sleep.

HOO Station CRT Display Glare Control: SWS installed anti-glare screens and hoods to retrofit existing CRTs to optimize visibility under the increased lighting levels in the HOO Station.

Intervention Assessment Methods

Questionnaires: Two questionnaires were distributed among the HOOs over the course of the project. At the beginning of the project a baseline questionnaire was distributed to the ten HOOs. At the end of the lights-on assessment period a final questionnaire was distributed to all HOOs. Only questionnaires from participating HOOs have been used in this report. The questionnaires addressed the following specific issues: HOO demographics, on-shift alertness, on- and off-shift safety, on-shift performance, off-shift sleep quality and quantity, general HOO well-being and quality of life, as well as ease of transition to and from shiftwork.

Sleep - Wake Activity Log Books: The HOOs were asked to fill out daily sleep and wake activity logs in both the baseline and intervention periods. These logs detailed their wake and sleep patterns, exposure to outdoor sunlight, and other activities, in 30 minute segments for 30 days at a time. They were also asked to estimate their sleep latency and sleep quality for each sleep period, including naps. Other data tracked included number of awakenings from sleep periods, caffeine consumption, and use of sleep aids.

Structured Interviews: At the conclusion of the data collection portion of the project an SWS project manager debriefed the HOOs individually in a formal structured interview. The intention was to record the HOOs impressions of the overall effectiveness of the *CLS*.

Stanford Sleepiness Scale: The Stanford Sleepiness Scale (SSS) is a seven point scale used to rate on-shift sleepiness. It is a standard self-rating scale used in research and clinical settings to quantify changes in subjective sleepiness. The form was completed by the on-shift HOOs every 2 hours. A computerized version automatically prompted the HOO to respond with a value from 0-6 every 2 hours. The SSS data was given values between 0 (feeling active and vital; alert; wide awake) and 6 (almost in reverie; sleep onset soon; lost struggle to remain awake). The lower the value the higher the on-shift alertness rating.

Subjective Rating: These forms were completed by the HOOs immediately following the Stanford Sleepiness Scale (SSS). At that time, the computer presented the HOO with a set of analog rating scales (called the Global Vigor and Affect [GVA] Instrument). Officers were presented with a question that was followed by a 100 mm line scale labeled at either end with descriptions of opposite extremes of degrees of feeling (very little, very much). The officer's task was to place a vertical hatch mark on the line to represent how he felt at that moment. He did so by clicking on the line with the computer mouse. The questions concerned alertness, sadness, tenseness, lethargy, happiness, weariness, calmness and sleepiness. The items on the GVA are always presented in the same order, and are arranged to avoid problems of adjacent opposites (e.g. "alert" immediately followed by "sleepy"). The computer calculated a numeric score, based on the placement of the officer's hatch mark.

Computer Based Performance Tests: Each HOO kept individual data diskettes for the Performance Assessment Battery (PAB). The tests are based on the Walter Reed performance assessment battery and are used to objectively assess operations officers' mental capabilities on the job. This test battery was selected because it has been validated in several previous research studies and is suited to field use. SWS's *LSS* computer automatically prompted the HOOs to take the PAB tests every four hours while on shift.

The PAB program computes precise performance data, including response time and accuracy for every trial within each test. These data files were stored to diskette. The data was analyzed by SWS using the standard Walter Reed PAB software.

The test battery included Logical Reasoning, Wilkinson Four-Choice Serial Reaction Time, Serial Add/Subtract, and the Manikin. A brief description of each of the performance tests follows.

Logical Reasoning: This test is an exercise in transformational grammar. The officer was presented with a 2-letter string (either "AB" or "BA") along with a logical statement describing the order of the letters within the string, e.g., "B follows A" or "A is not preceded by B." The officer's task was to press the "S" key if the logical statement is true or the "D" key if it is false. (These keys were chosen over "T" and "F" keys because they are adjacent to one another on a conventional keyboard.)

Four-Choice Serial Reaction Time: The officer was presented with an array of four boxes arranged in a square on a black background. The officer is told that each box corresponds to one of four adjacent keys (4, 5, 1, and 2; also in a square pattern) on the numeric key pad. A red-lighted background appears in one box at a time and the subject presses the key on the key pad that corresponds to the position of the lighted box. The red background then moves to another box until a predetermined number of trials are completed.

Serial Add/Subtract: This is a machine-paced arithmetic test requiring sustained attention. The officer was instructed to place his fingers on the 4, 5, 6, and 0 keys of the numeric key pad. The officer was presented with a single digit, then another single digit, and then a plus or minus sign, all in the same screen location. The officer's task was to enter the least significant digit of the addition or subtraction result. For example, 8, 6, + equals 14, so the officer enters 4. If the result is a negative number, the task is to add 10 to it and enter the positive single digit remainder. For example, 3, 9, - equals -6, so the officer enters 4.

Manikin Spatial Orientation: This is a visual/spatial perceptual task in which the officer was required to determine from visual cues in which hand a stylized person is holding a target object (circle or square). The Manikin appears on the screen holding a solid red circle in one hand and a solid green square in the other. Around the Manikin is a line drawing (a red circle or a green square) which indicates the target to be identified. The officer's task was to recognize the target shape sought, find the target, decide whether the target is held in the left or right hand, and then press a key signifying left or right hand. The difficulty in the task comes from the variable position of the Manikin, which can be either upside down or right side up and facing front or back.

Results

Performance:

It is not possible to measure HOO performance in the way one might measure employee productivity at a manufacturing facility. However, it can be assumed that if the officer is alert, then he is better able to perform his job function efficiently and accurately. The final questionnaire, self-rating forms, and the structured interviews all suggested improved job performance.

When asked what the most positive outcome of the project was, one officer said, "Enhanced alertness, concentration, and energy level, resulting in higher productivity."

In the final questionnaire officers were asked to rate their on-shift performance over successive days of a normal shift. The officers rated their first night of shift as "good" or "satisfactory" during the baseline period and they rated the same shift as "satisfactory" during the intervention period. On subsequent nights during the baseline period, performance declined on a nightly basis to between "poor" and "barely satisfactory," whereas during the intervention period, performance ratings improved to between "good" and "excellent." (Note: While Figure 13 shows the first night shift to have poorer performance during the intervention period than during the baseline, many officers reported during interviews that the first night of shift while working under the lights was substantially better than during baseline.)

The subjective rating of how much effort it took to do anything leveled off across the 24-hour day during the intervention period when compared with the variations reported in the baseline period. The officers reported that they required more effort during the early morning hour to accomplish something in the baseline period (Figure 1).

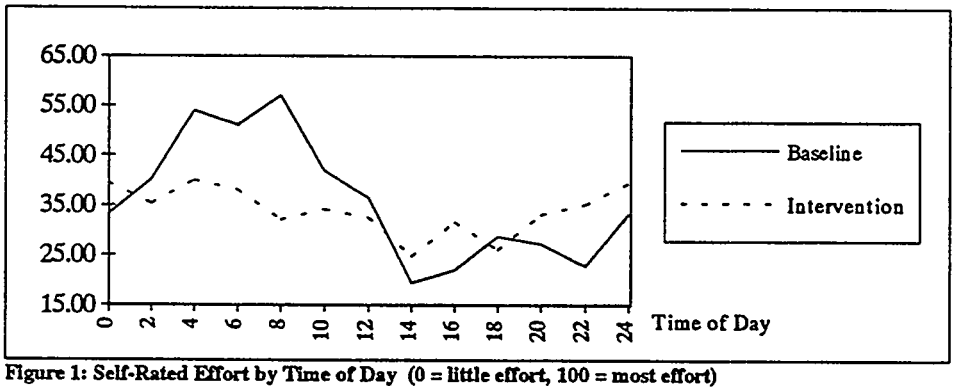


Figure 1: Self-Rated Effort by Time of Day (0 = little effort, 100 = most effort)

One HOO's illustration of the prevalence of low alertness and poor concentration on night shift in the baseline was the necessity of making numerous call backs to acquire additional information from a plant that was reporting an event. In the intervention period the HOOs reported that the lights had enhanced performance during the night shift to the point where it was comparable to day shift performance and that the overall level of efficiency and alertness had improved. Others reported feeling much more comfortable with their assessment capabilities since the system was installed. Some reported to be suprised by these improvements despite their initial skepticism.

Alertness:

Working under the *CLS* enhanced on-shift alertness, as indicated by data from the final questionnaire, Stanford Sleepiness Scale, self-rating forms, computer-based performance tests, and structured interviews. All of the officers who worked in the rotation reported being more alert during their night shift duty when using the CLS.

When asked if they have experienced an improvement in their on-shift alertness, HOOs reported, "At night, it is dramatic," and "I am much more alert, especially on night shift." During the baseline period, officers talked about their difficulty in reading or writing technical reports during the early morning hours (2 a.m. - 8 a.m.) since they were unable to concentrate or were struggling to stay awake. By contrast, in the intervention period, one officer reported, "I actually feel like doing technical work." Other comments were, "With better rest I am more active during the night shift," "I feel less drained on night shift after the lights," and "I have more energy in the off-hours."

The baseline measures of self-rated alertness, sadness, tenseness, effort, happiness, weariness, calmness, and sleepiness all illustrated a near replication of the 24-hour circadian cycle on the Self-Rating scale, which was completed every two hours on-shift. The officers reached their lowest points in all of the aforementioned categories during the early morning hours between 2 a.m. and 8 a.m., and rated themselves highest during the afternoon hours. In the intervention period, the ratings leveled off, demonstrating a consistency in ratings from day to night shift. Night shift ratings across all categories improved dramatically, while day shift ratings either remained the same or decreased (Figures 2 - 4).

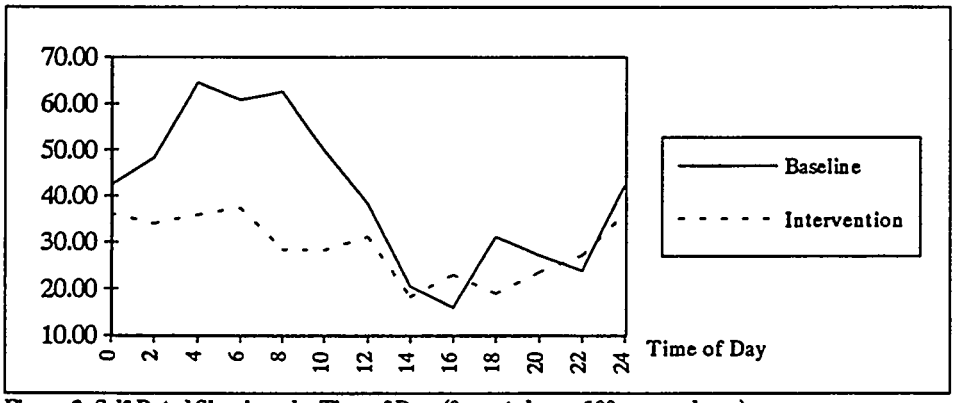


Figure 2: Self-Rated Sleepiness by Time of Day (0 = not sleepy, 100 = very sleepy)

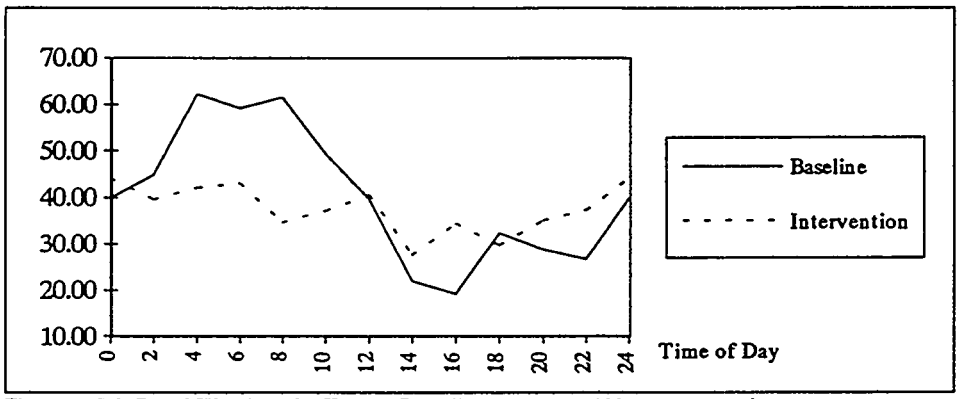


Figure 3: Self-Rated Weariness by Time of Day (0 = not weary, 100 = most weary)

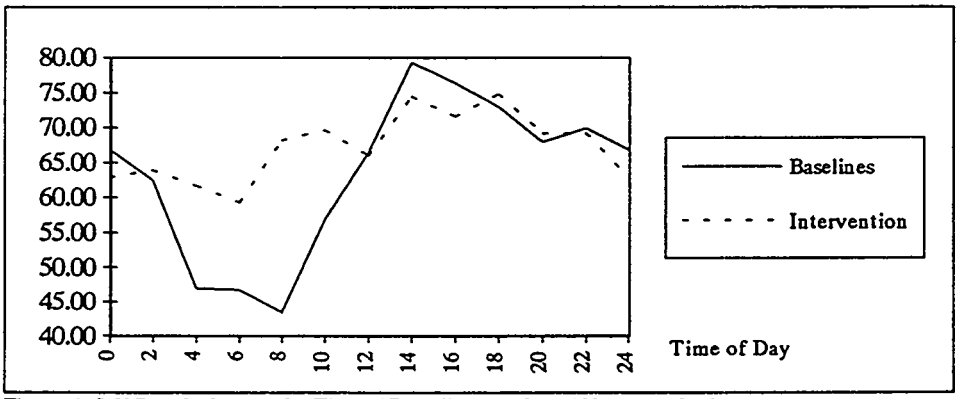


Figure 4: Self-Rated Alertness by Time of Day (0 = not alert, 100 = very alert)

The Stanford Sleepiness Scale results demonstrate a marked decrease in perceived sleepiness among the officers on both day and night shift. Officers rated themselves as less sleepy at all times of the day during the intervention period. (Figure 5).

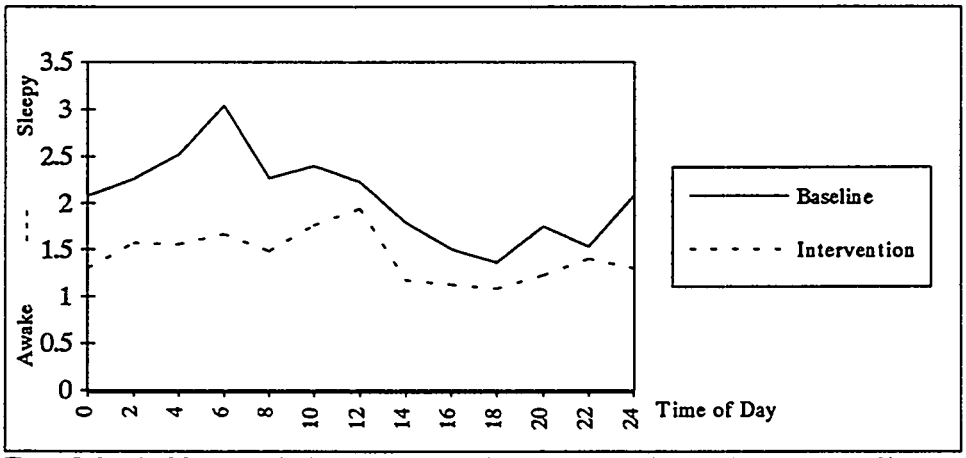


Figure 5: Stanford Sleepiness Scale by Time of Day (0 = wide awake, alert, 4 = foggy, not at peak)

In three of the four computer based performance tests, improvements were made in the mean reaction time without sacrificing accuracy. Performance ratings across time-of-day leveled off, to the point where night shift performance was equal to that of day shift (Figures 6 - 9).

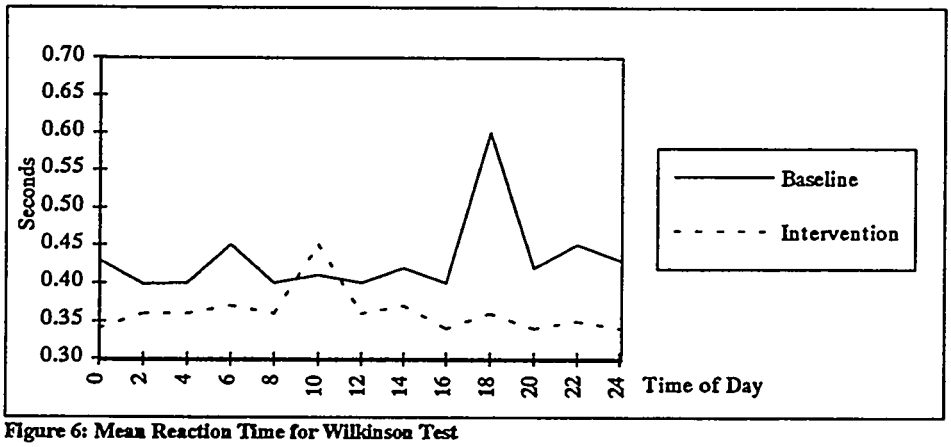


Figure 6: Mean Reaction Time for Wilkinson Test

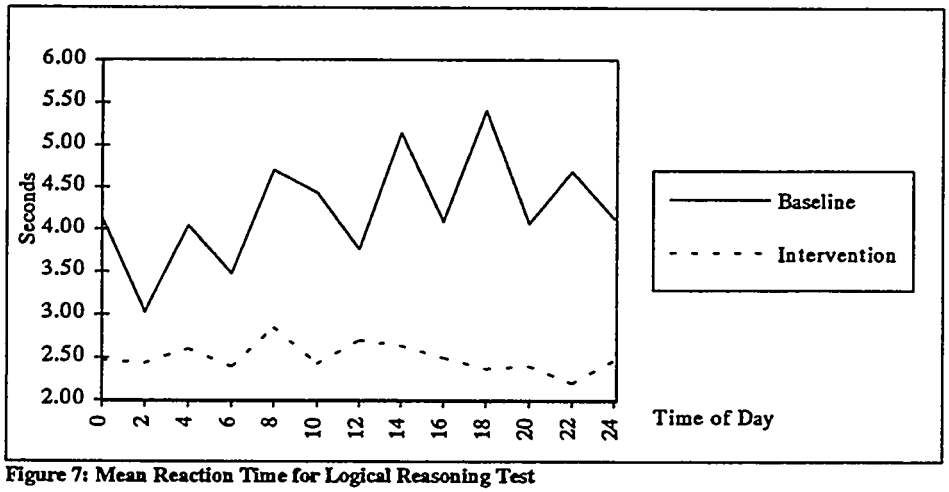


Figure 7: Mean Reaction Time for Logical Reasoning Test

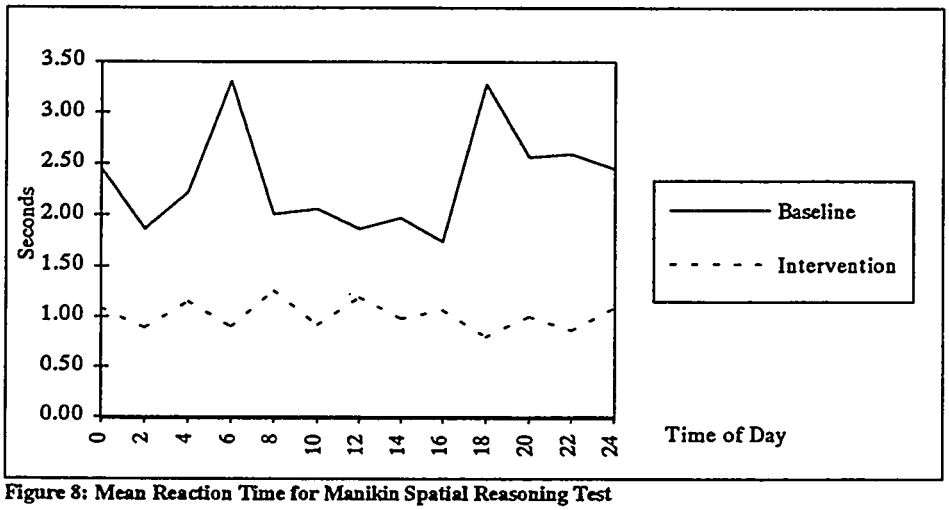


Figure 8: Mean Reaction Time for Manikin Spatial Reasoning Test

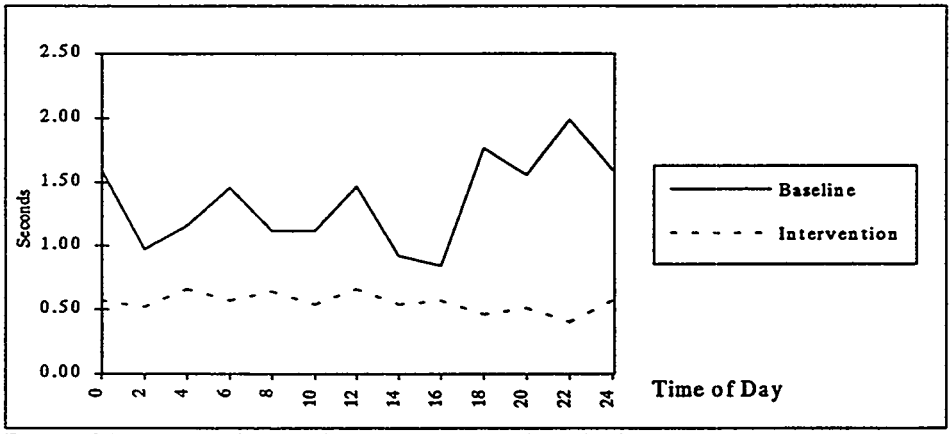


Figure 9: Mean Reaction Time for Serial Addition and Subtraction Test

Sleep:

The HOOs enjoyed longer and more refreshing sleep in the intervention period, according to their sleeplogs and questionnaires (Figure 10, 11, 12) and their structured interviews. Day sleep after the 00-12 shift improved by almost 3 hours over the course of three consecutive night shifts. Sleeplogs provided the most objective evidence of improved sleep length and quality, and these were supported by the HOOs subjective reports in their questionnaires and structured interviews . In addition, the HOOs reported that it took them less time to fall asleep and that there were fewer interruptions to their sleep. HOOs also reported longer and more refreshing night sleep after they worked 12 hour day shifts under the *CLS*.

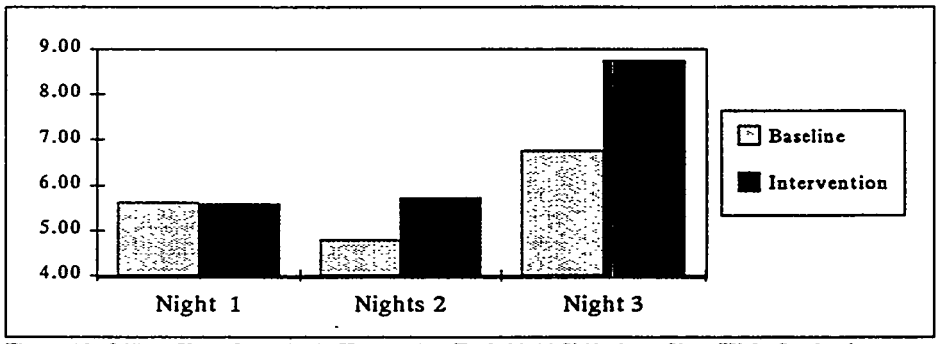


Figure 10: Officer Sleep Quantity in Hours After Each 00-12 Shift, from Sleep/Wake Logbooks

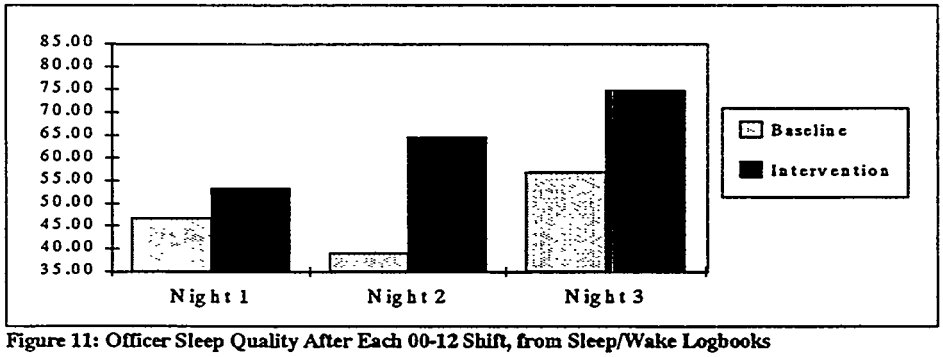


Figure 11: Officer Sleep Quality After Each 00-12 Shift, from Sleep/Wake Logbooks
(0 = wake groggy, 100 = wake refreshed)

HOOs also reported reductions in sleep latency during day sleeps, following the *CLS* intervention. In the baseline period:

- 49% of the HOOs reported falling asleep within 10 minutes of trying to fall asleep.
- 38% of the HOOs reported falling asleep within 10 and 30 minutes of trying.
- 13% reported taking 120 minutes to fall asleep.

By contrast, in the intervention period:

- 83% fell asleep within 10 minutes of trying.
- 17% fell asleep within 30 minutes of trying.

HOO comments and observations pertaining to sleep issues after working under the *CLS* were gathered from structured interviews and questionnaires. The estimates of improved sleep length varied from one hour extra of uninterrupted sleep to three hours of additional sleep. The HOOs reported being able to sleep longer and deeper during their day sleep period and were able to sleep when desired. The HOOs who had longer commutes did not have the time to sleep longer but they did report deeper, more restorative sleep. One HOO reported "actually oversleeping" and of having to purchase a clock-radio to wake from day sleep for the following night shift. (Previously some of the HOOs had reported experiencing fitful, light sleep and not needing an alarm to wake on time.) Other observations made by the HOOs were that they awoke feeling better and more refreshed, that they were more alert and productive on night shift, and that they experienced fewer of the physical problems associated with sleep debt. One HOO reported being more relaxed off-shift due to improved sleep. Finally HOOs reported fewer interruptions in their day sleep due to temperature and outside influences.

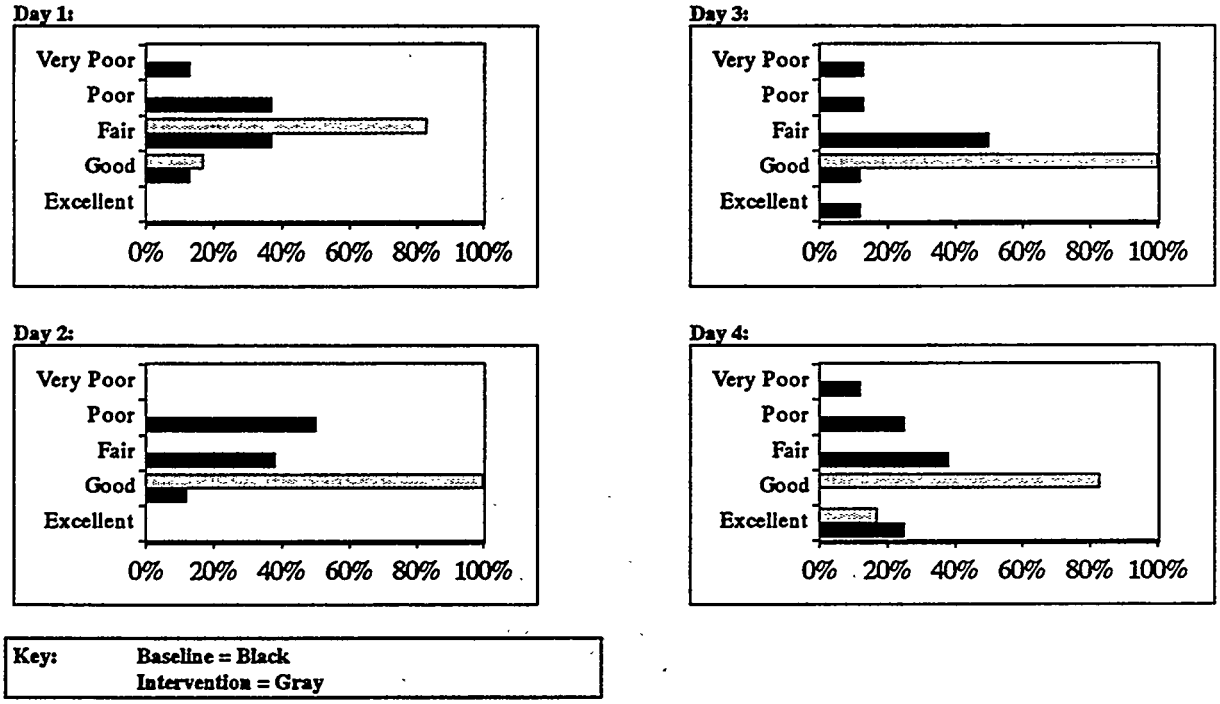


Figure 12 Day Sleep Quality following the 00-12 Shift, by Night of Shift

Shift Transitions:

The HOOs reported that the *CLS* helped them to adjust to night shift work and the HOOs also reported that training in individual adjustment strategies helped them to readjust to a night sleep schedule on days off (Figure 14).

When asked "How long does it take you to adjust to a shift change when coming back to work the 00-12 shift?," in the baseline period, 72% of the operators reported taking 2 - 3 nights. In contrast, during the intervention period, 67% of the HOOs reported being adjusted after the first 00-12 shift and every HOO reported being adjusted by their second 00-12 shift. When asked to rate their work performance over successive nights of a 3 or 4 night block of baseline 00-12 shifts, every HOO rated their performance as "satisfactory" or "barely satisfactory" over the block of shifts. During the intervention period they rated their performance as "barely satisfactory" on the first night of shift, but as "good" or "excellent" on the second, third and fourth day of shift. The fact that the HOOs reported significantly improved performance over the course of a single intervention block of shifts indicates a swift transition to their night shift schedules, with a corresponding decrease in fatigue.

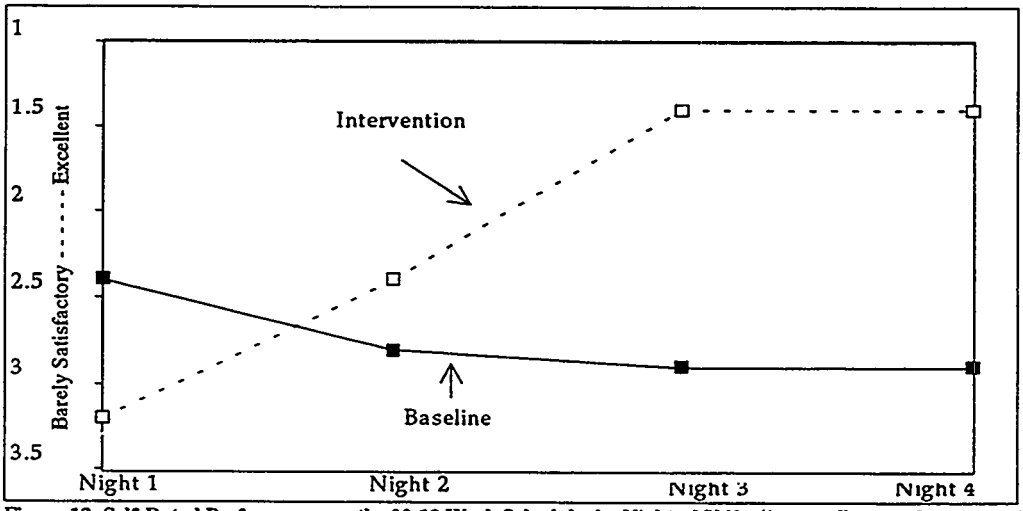


Figure 13: Self-Rated Performance on the 00-12 Work Schedule, by Night of Shift (1 = excellent performance, 4 = barely satisfactory)

In the intervention period structured interviews and questionnaires, most HOOs reported feeling better on the first night and being completely adjusted to night shift by the second night of shift. Some reported that they had never adjusted to night shift prior to the *CLS* installation but that they were adjusting in 2 - 3 nights in the intervention period. Enhanced alertness, better sleep, improved mood were the criterion used to define "adjustment to night shift". Most HOOs reported these conditions improving on each subsequent night, and some claimed to no longer experience the "second night shift dip."

When asked how the *CLS* had affected their ability to adjust back to a night sleeping schedule after working night shifts under the *CLS*, HOOs were divided with respect to whether it was easier or more difficult to readjust than it had been in the baseline condition. Some HOOs reported difficulty readjusting to a normal schedule while others reported the transition to be easier and more rapid than previously. One HOO reported being less irritable during the transition.

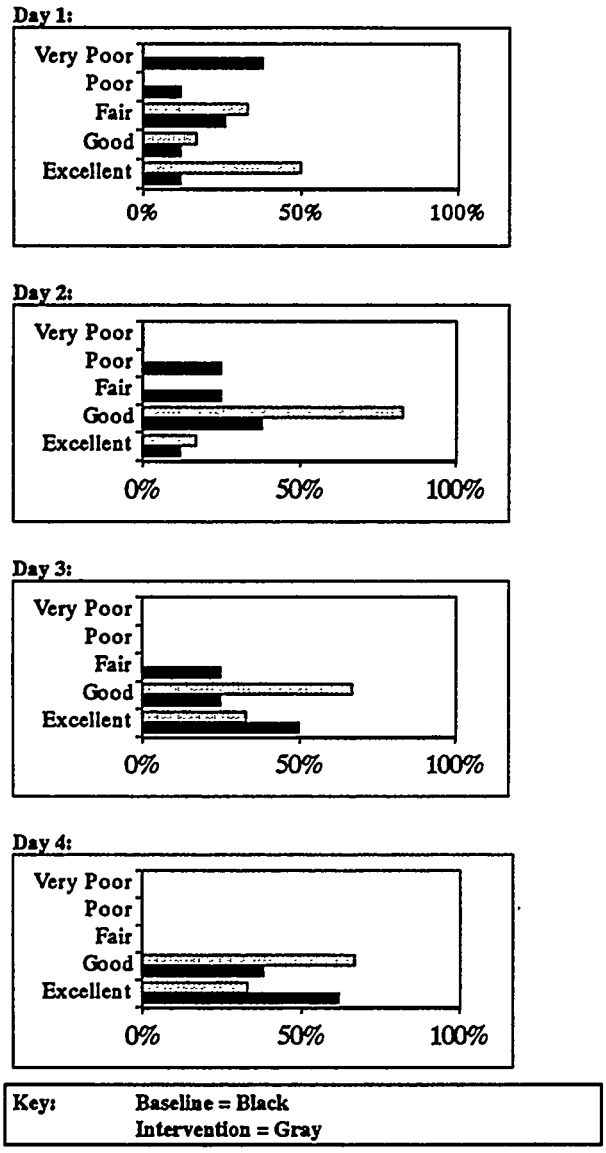


Figure 14: Night Sleep Quality on Days off Following a block of 00-12 Shifts

On-Shift Fatigue:

HOOs reported a reduction in on-shift fatigue and sleepiness, and an improvement in their ability to address incident reports in the intervention period. In addition they reported a swifter transition to peak performance on the 00-12 shift.

Before the installation of the *CLS,* HOOs reported struggling to stay awake on the 00-12 shift. During the baseline period, 75% reported having difficulty staying awake *more than once per block of shifts,* 66% of those reporting difficulty *once or more per shift.* In the intervention period, 34% reported struggling to stay awake on night shift *more than once per block of shifts,* while 66% reported struggling to stay awake only *once per block of shifts* or *once every 4 months.*

On-shift fatigue and sleepiness in the baseline period made it more difficult for the HOO to respond to incident reports. When asked how frequently sleepiness or fatigue made it more difficult to respond to incident reports on the 00-12 shift during the baseline period, 11% reported that it affected *them more than once per shift* and an additional 22% reported that it affected them *once per block of shifts.* In the intervention period nobody reported that fatigue/sleepiness made it more difficult to respond to incident reports *more than once per block of night shifts.* One officer reported difficulty *once per block of shifts,* with the remainder being reporting difficulty *once per 6 week rotor* or *never.*

During the questionnaires and structured interviews the HOOs were asked to comment on any improvements that they perceived to be a result of the *CLS* installation. Responses indicated that they felt more alert and more focused on night shift as a result of better day sleep. They also reported feeling more confident in their event assessment capabilities, giving higher quality responses and being better able to handle issues because they were more alert.

Commuting Safety

HOO commuting safety was improved by the *CLS* installation, particularly after their 00-12 shifts and even more so for those with long commutes.

According to HOOs' on-shift Stanford Sleepiness Scale (SSS) ratings, the HOOs were much more alert during the intervention period during the early hours of the morning, particularly between 2am and 8am (Figure 5). However, the alertness gap between the baseline and intervention period begins to close from 8am until noon, the point at which the HOOs begin their post-shift commute. Nevertheless, the gap never closes completely and there is no point at which HOOs reported being *less* alert in the intervention period than in the baseline period. Therefore, it was to be expected that the HOOs would feel much more alert during their 00-12 shift and more, or no less, alert during their commute than they did during the pre-lights period.

During the initial intervention period, one HOO reported lower alertness during his commute home. This decline in alertness was addressed by tailoring the software to provide the HOO with additional light at specific times in order to allow him improved commuting safety. In a follow-up telephone interview, this HOO reported the commuting problem was solved by the change in the lighting schedule.

HOOs comments on the changes in commuting safety were reported during structured interviews and in the baseline and intervention questionnaires. When asked about the problems of adjusting to his shift schedule in the baseline period, one HOO observed that he had trouble staying awake during the drive home, after 00-12 shift. Two of the HOOs had reported that it was necessary to stop on their long commute home in order to avoid falling asleep while driving. In contrast, during the intervention period both HOOs reported that stopping was no longer required and the commute was a lot safer. Other HOOs reported the commute to be safer since they were more alert and not as fatigued. The HOOs with the longest commutes (60-90 minutes) reported the greatest improvements in commuting safety. The HOOs who had a short drive did not report as great an improvement.

The Temporary Return to Baseline Conditions

During the entire course of the project, the HOO Station was in Bethesda, Maryland. The data collection portion of the project ended in May, 1994. The HOOs moved to their new facility in Rockville, Maryland shortly thereafter. Because of a delay in the installation of the *CLS*, many of the officers who had worked at night in the rotation under the *CLS* at the original location were forced to return to baseline conditions. Officers reported a degradation in their on-shift alertness, a return to "struggling through." They also reported a decline in the quality and quantity of their sleep.

Overview of Project Outcomes

ShiftWork Systems, Inc. designed and installed a computer controlled *Circadian Lighting System* (CLS) at both Bethesda and Rockville HOO stations with the goal of helping the HOOs to adjust physiologically to their night shift schedules. All participants reported benefits, including:

- Less subjective fatigue on night shifts
- Improved night shift alertness and mental performance
- Higher HOO confidence in their ability to assess event reports
- Longer, deeper and more restorative day sleep after night duty shifts
- Swifter adaptation to night work
- A safer commute, particularly for those with extensive drives

The following is representative of summary comments concerning the *CLS:*

- My reaction is positive, I was skeptical at the beginning. I have tried a lot of tactics over nine years (of shiftwork) and I wouldn't want to be without the (*CLS*) system now.
- Very positive. It has been a very enlightening experience, from a knowledge level, after years of shiftwork, to realize I didn't have to put up with 3 - 4 terrible nights.
- I'm less irritable at work and at home . . . I feel happier
- It used to be that I knew in my heart that I couldn't count on going to bed (during the day) and stay asleep for any length of time. Now I go to bed earlier, by choice, and stay asleep.
- Positive, I feel better. I get more sleep and it's heavier. I feel better coming in to work.
- It's positive, I'm a lot less grumpy now, not the normal bear.
- It's a positive feeling. I'm drinking decaffeinated coffee now. I was drinking up to 30 cups of caffeinated coffee per night shift previously.

Conclusion

The data and the Headquarters Operations Officers indicate that the *Circadian Lighting System* has been a success and that it has provided a physiological adaptation to shiftwork by improving alertness and performance during night work. The HOOs and the NRC have opted to install a second system in the new headquarters in Rockville.

The results of this project reflect those of the clinical research, i.e. an average increase in day sleep for night workers of approximately 2 hours, a decrease in reaction time tests without a compromise in accuracy, and subjective ratings of increased alertness. The results also reflect those from previous applications of the technology such as the application at San Diego Gas & Electric's South Bay Power Plant and with NASA's shuttle astronauts. The results and opinions of the HOOs indicate that it is possible for the results of circadian lighting laboratory research to be used successfully in an applied work situation.

References

Allan JS, Czeisler CA, Duffy JF, Kronauer RE 1988 Non-linear dose response of the human circadian pacemaker to light. *Abstracts,154th Annual AAAS Meeting,AAAS Publication No 897-30* 101

Boyce JW, Beckstead NH, Eklund RW, Strobel, Rea MS 1993 Report on the Influence of a Daylight-Simulating Skylight on the Task Performance and Mood of Night-Shift Worker.

Campbell SS, Dawson D. 1990 Enhancement of nighttime alertness and performance with bright ambient light. Physiol Behav.48:317-320.

Czeisler CA 1978 Internal Organization of Temperature, Sleep-Wake, and Neuroendocrine Rhythms Monitored in an Environment Free of Time Cues. Doctoral Dissertation, Stanford University, Stanford, California

Czeisler CA, Allan JS, Kronauer RE 1987 Rapid manipulation of phase and amplitude of the human circadian pacemaker with light-dark cycles. *Abstracts,5th International Congress of Sleep Research,Copenhagen,Denmark* S11 (Abstract)

Czeisler CA, Allan JS, Kronauer RE, Duffy JF 1988 Strong circadian phase resetting in man is effected by bright light suppression of circadian amplitude. *Sleep Res* 17: 367

Czeisler CA, Allan JS, Strogatz SH, et al 1986 Bright light resets the human circadian pacemaker independent of the timing of the sleep-wake cycle. *Science* 233: 667-671

Czeisler CA, Jewett ME 1990 Human circadian physiology: Interaction of the behavioral rest-activity cycle with the output of the endogenous circadian pacemaker. In: Thorpy MJ (ed) Handbook of Sleep Disorders. Marcel Dekker, Inc., New York p 117-137.

Czeisler CA, Johnson MP, Duffy JF, Brown EN, Ronda JM,Kronauer RE. 1990 Exposure to bright light and darkness to treat physiologic maladaptation to night work. N Engl J Med.322:1253-1259.

Czeisler CA, Kronauer RE, Allan JS, et al 1989 Bright light induction of strong (Type 0) resetting of the human circadian pacemaker. *Science* 244: 1328-1333

Czeisler CA, Richardson GS, Zimmerman JC, Moore-Ede MC, Weitzman ED 1981 Entrainment of human circadian rhythms by light-dark cycles: a reassessment. *Photochem Photobiol* 34: 239-247

Czeisler CA, Weitzman ED, Moore-Ede MC, Zimmerman JC, Knauer RS 1980 Human sleep: Its duration and organization depend on its circadian phase. *Science* 210: 1264-1267

Dawson D, Campbell SS. 1991 Timed exposure to bright light improves sleep and alertness during simulated night shifts. Sleep.14(6):511-516.

Eastman CI. 1992 High-intensity light for circadian adaptation to a 12-h shift of the sleep schedule. Am J Physiol.32:R428-R436.

Kronauer RE 1987 A model for the effect of light on the human "deep" circadian pacemaker. *Sleep Res* 16: 621

Kronauer RE 1990 A quantitative model for the effects of light on the amplitude and phase of the deep circadian pacemaker, based on human data. In: Horne J (ed) Sleep '90, Proceedings of the Tenth European Congress on Sleep Research. Pontenagel Press, Dusseldorf p 306-309.

Kronauer RE, Czeisler CA 1993 Understanding the use of light to control the circadian pacemaker in humans. In: Wetterberg L (ed) Light and Biological Rhythms in Man. 63rd edn. Pergamon Press, Oxford p 217-236.

Kronauer RE, Jewett ME, Czeisler CA 1991 Human circadian rhythms. *Nature* 351: 193

Kronauer RE, Jewett ME, Czeisler CA 1994 The human circadian response to light: strong and weak resetting. *J Biol Rhythms* 8(4): 351-360

Lewy AJ, Wehr TA, Rosenthal NE, et al. 1982 Melatonin secretion as a neurobiolical "marker" and effects of light in humans. Psychopharmacol Bull.18:127-129.

Myers BL, Badia P. 1993 Immediate effects of different light intensities on body temperature and alertness. Physiol Behav.54:199-202.

Strassman RJ, Qualls CR, Lisansky EJ, Peake GT. 1991 Elevated rectal temperature produced by all-night bright light is reversed by melatonin infusion in men. J Appl Physiol.71(6):2178-2182.

Thessing VC, Anch AM, Muchlbach MJ, Schweitzer PK, Walsh JK 1994 Two- and 4-Hour Bright-Light Exposures Differentially Effect Sleepiness and Performance the Subsequent Night. Sleep 17(2):140-145

TECHNICAL BASIS FOR STAFFING LEVELS AT NUCLEAR POWER PLANTS

by

Deborah A. Shurberg and Sonja B. Haber
Brookhaven National Laboratory
Upton, NY 11973-5000
and
Dolores Morisseau and Jay Persensky*
U.S. Nuclear Regulatory Commission
Washington, DC 20585

Abstract

The objective of this project is to provide a technical basis for the establishment of criteria for minimum staffing levels of licensed and non-licensed NPP shift personnel. Minimum staffing levels for the purpose of this study, are defined as those necessary for successful accomplishment of all safety and additional functions that must be performed in order for the licensee to meet applicable regulatory requirements.

This project involves a multi-faceted approach to the investigation of the issue. Relevant NRC documentation was identified and reviewed. Using the information obtained from this documentation review, a test plan was developed to aid in the collection of further information regarding the adequacy of current shift staffing levels. The test plan addresses three different activities to be conducted to provide information to the NRC for use in the assessment of current minimum staffing levels. The first activity is collection of data related to industry shift staffing practices through site visits to seven nuclear power plants. The second activity is a simulator study, which will use licensed operator crews responding to a simulated event, under two different staffing levels. Finally, workload models will be constructed for both licensed and non-licensed personnel, using a priori knowledge of the simulator scenarios with data resulting from one of the staffing levels studied in the simulator, and the data collected from the site visits. The model will then be validated against the data obtained from the second staffing level studied in the simulator. The validated model can then be used to study the impact of changing staffing-related variables on the plant shift crew's ability to effectively mitigate an event.

Introduction

The NRC has defined minimum staffing levels for ROs and SROs at U.S. commercial NPPs in Title 10 of the CFR Section 50.54(m). In addition, NRC policy (50 FR 43621, 1985) states that NPP licensees may provide the needed engineering expertise on-shift by having either a dedicated Shift Technical Advisor or one of the SROs specially qualified to perform that function. However, comparable minimum

---

*The views expressed in this paper do not necessarily represent the opinions of the U.S. Nuclear Regulatory Commission.

staffing level requirements have not been established for non-licensed shift personnel, although goals for some positions have been outlined in NUREG-0737, Supplement No. 1, "Clarification of TMI Action Plan Requirements" (1980).

Recent trends within the NRC to move away from compliance-based and towards performance-based regulation, as well as recent events within the U.S. nuclear industry with staffing-related implications, have led the NRC to re-examine the technical basis for staffing levels as they exist in 10 CFR 50.54(m). Numerous changes in NPP regulatory requirements and standards of operation have occurred since 10 CFR 50.54(m) was originally published in 1982. These changes have raised concerns that the demands placed upon NPP shift personnel have increased, although it is not clear that workload and function allocation have been considered by licensees in light of these changes. Additionally, there have been recent incidents at NPPs, where minimum staffing level requirements have been met, but problems have occurred that could be attributed to staffing levels. The concerns raised by these incidents are summarized in two recent Commission Papers, SECY-93-184, "Shift Staffing at Nuclear Power Plants," and SECY-93-193, "Policy on Shift Technical Advisor Position at Nuclear Power Plants." Finally, staffing level requirements for non-licensed personnel have not been systematically examined, although goals for some positions have been outlined in NUREG-0737.

The purpose of this project is to establish a technical basis for criteria for minimum shift staffing levels of licensed and non-licensed NPP personnel. Mechanisms through which this is to be accomplished are:

- Document review to identify issues related to NPP staffing levels;
- On-site data collection efforts to survey a sample of NPPs for information related to shift staffing practices;
- Simulator study designed to systematically vary staffing levels allowing an investigation of staffing level adequacy; and
- Model development in order to perform a computer-based workload analysis to assist in the establishment of criteria for the determination of NPP shift staffing levels for both licensed and non-licensed shift personnel.

Document Review

A framework of issues was developed for use in the document review to focus efforts and provide a consistent and comprehensive scheme for data collection. The framework was developed based on a cursory review of relevant documentation, as well as insights provided by project members with significant inspection experience. The categories identified in the framework are not all-inclusive, nor are they necessarily independent. The fourteen categories identified are listed and defined in Table 1.

The framework as developed and described below was found to be a useful tool in characterizing the information in the documents reviewed. However, it should be noted that the usefulness of the framework varied with the type of document reviewed. For example, the category "Event Type" was irrelevant to the Emergency Operating Procedure (EOP) inspection report review. Additionally, as will be noted later in this paper, information for all categories was typically not available in many of the documents reviewed.

Table 1. Framework of Issues Associated with Shift Staffing Levels

CATEGORY	DEFINITION
Automation, Aiding, Improved Layout	This category encompasses a) human-system interface issues and the suitability of their incorporation in the design of the system and the allocation of tasks among available staff given the system lay-out; b) the number of individuals necessary to operate equipment and the impact of this number on the crew's ability to respond to an event; and c) out-of-service equipment and the impact on event diagnosis/mitigation.
Communications	This category includes issues such as inter- and intra-crew communications and event notifications to appropriate parties, and how these communications issues either arose due to inadequate staffing levels or whether the need for communications contributed to task overload.
Crew Performance	This category includes issues such as crew experience and length of time the crew has served together.
Event Categorization	This category deals with the types of events that are associated with shift staffing level issues and includes the operational status of the plant.
Procedure Design	This category addresses whether or not administrative procedures exist to address issues such as shift and relief turnover during an event, and whether these procedures clearly allocate tasks and define roles and responsibilities of plant personnel. Another issue that falls into this category is whether or not procedures take minimum staffing levels into account.
Reactor Parameters	This category includes reactor type, age, region, and complexity.
Routine Tasks	This category includes performance of routine tasks (e.g., logkeeping, making/answering telephone calls, turnovers) which contributed to the shift staffing problem identified.
Staffing Level	This category includes specific references to staffing levels and whether any violation of minimum staffing requirements occurred.
Stressors	This category encompasses physical and psychological stressors (e.g., shift length, overtime, event timing, fatigue).
Task Allocation	This category addresses how tasks are allocated as well as who is responsible for task allocation. The role of procedures in addressing task allocation was also taken into consideration.
Task Complexity	This category covers event and/or task complexity from a cognitive point of view and includes the ability of the plant staff to coordinate/oversee on-going activities and the impact staffing levels have on this ability.
Task Location	This category addresses the location of equipment that must be operated, tested, and maintained, and includes the availability of a sufficient number of individuals to perform operations at remote locations.
Training	This category includes issues such as training event fidelity and crew size during training.

The following sources of information were chosen for review by the project team, using the framework developed above: Human Performance Event Investigations; Augmented Inspection Team Reports; Incident Investigation Team Reports; Emergency Preparedness Exercises; EOP Inspection Reports; and NRC Operator Licensing Examination Information.

A number of factors were identified in the documents reviewed that may be important in determining adequate shift staffing levels. These factors include (1) the design and content of the EOPs and support procedures, (2) allocation of tasks among the crew members, and (3) the implications of fire brigade requirements and out-of-service equipment on control room staffing levels. Because these factors, among others, interact to define overall crew and individual crew member workload, requirements for minimum shift staffing may have to be evaluated on a plant-specific basis with a methodology that considers more than the number of units at the site and the extent to which multiple units are operated from the same control room.

Little information was obtained on staffing levels for non-licensed shift personnel. The review suggests that staffing practices, training, procedure design, and equipment location, among other factors, should be examined to determine staffing for functions performed by support personnel outside the control room. Problems similar to those identified for the control room staff may also exist for the support staff. For example, although the EOP inspections addressed EOP support procedures, many of the deficiencies identified in the support procedures have implications for the number of personnel required to perform them.

Finally, the review of available documentation suggested certain parameters for incorporation into the remaining research activities associated with this project. Specifically, one important issue to be addressed is the concurrent implementation of EOPs and the Emergency Procedure Implementation Plan. Most NRC inspection activities do not involve concurrent implementation; thus, the information on this aspect of emergency response is limited. Additionally, the remaining activities in this project should be conducted at backshift staffing levels. Staffing levels have a tendency to be lower on the backshift and staff augmentation would likely take longer than on a day or swingshift. The other activities in this project should also take into account the impact of staffing a fire brigade. The fire brigade is typically staffed with on-shift personnel, since dedicated fire brigade members are rare. This decreases available staff support for event mitigation. Consideration also needs to be given in the remaining research activities to the format of the procedures. Specifically, the EOPs at BWRs are in a flowchart format, different than that of EOPs at a PWR. The impact of such format differences on staffing requirements remains to be determined. Lastly, attention needs to be focused on activities that take place in plant areas other than the control room, as limited information is currently available regarding staffing levels for non-control room personnel.

On-Site Data Collection

Seven U.S. NPPs were visited and information collected regarding current staffing practices for both licensed and non-licensed shift personnel necessary for effective event response. The methods used to collect the information include: table-top simulation of two accident scenarios (one chosen by the research team which involved a fire with a non-isolable release of low-level activity, and one chosen by the plant which, in the judgement of the plant staff represented the most limiting sequence of events that the site's on-shift staff could successfully mitigate for one hour before staff augmentation); plant documentation review; plant walkdowns of specific in-plant tasks related to the scenarios; and interviews

with individuals from different organizational units at the site that are familiar with shift staffing practices. Using these methods, data were collected that related to: the allocation of tasks by position; workload/conflicting requirements; normal staffing for position/shift; training practices relative to staffing; operational experience reviews conducted that relate to staffing; and the impact of plant parameters on staffing levels.

The seven sites visited are a sample of the plant types in the U.S. commercial nuclear industry. They varied along the dimensions of plant type (BWR and PWR), plant age (pre-Three Mile Island or post-Three Mile Island), and number of units on site (single or dual units). These variables were selected because procedure design (which is dependent on plant type), plant age, and number of units on site are issues that have been identified as having an impact on staffing needs by Shurberg, et al., 1994, and Melber, et al., 1994.

The data collected in the course of these site visits lent itself to the following types of analyses: comparisons between NRC staffing requirements, plant technical specification and administrative procedure staffing requirements, and normal staffing levels for day, evening and night shifts. Comparisons of these different staffing levels were conducted across the sites visited and explanations sought for any differences obtained. Scenario time lines were developed which detail the tasks performed, given the scenario, and the individuals required to perform the tasks. These timelines yielded important insights into where staffing resources were strained within a given scenario, and the impact that strain had on the outcome of the event. Finally, comparisons were made between plants regarding the allocation of personnel to perform certain activities that are common across all sites visited (e.g., staffing the fire brigade, performance of offsite dose assessment).

Simulator Study

The purpose of conducting a simulator study is to collect information to determine the appropriate criteria for the establishment of minimum staffing levels necessary to successfully accomplish all needed safety functions and meet all applicable regulatory requirements through the use of selected high workload off-normal events. The simulator study will incorporate both control room and in-plant personnel tasks so that staffing levels for all shift personnel can be investigated. The simulator experiment will be run as realistically as possible, using full-scope replica simulators and experienced shift crews. The results of the simulator study will also be used in the model development and validation efforts of this project.

Subjects will be recruited from two plants, one BWR and one PWR, which agree to participate in this study. Study participants will be control room crews that normally work together, including all personnel that would be in the control room during normal, backshift operations. In addition, one to two support personnel (e.g., chemistry technicians, auxiliary operators) will be requested to participate in the study to assist the research team in tabletop exercises of the in-plant tasks that will need to be performed as part of the scenario.

Both the BWR and PWR simulator scenarios that will be used will be predicated upon design basis accidents, although additional complications will be built in, such as a fire and a radiological release to the environment. Two variations on the basic scenario will be developed and will differ on the initiating conditions, equipment failure sequences, and amount of Reactor Coolant System activity. These variations will be used since each crew will participate in executing the scenario two times. These variations should help to inhibit anticipation of response actions on the part of the operators. Data will

be collected during the simulator scenarios that relate to task allocation, task sequencing, workload management strategies, and task timing.

Three research hypotheses will be tested by conducting the simulator study:

(1) A lower level of performance will be observed as the size of the shift staff decreases within the chosen scenarios;

(2) The use of workload management strategies will increase as the size of the shift staff decreases within the chosen scenarios; and

(3) Measures of subjective workload will be higher as shift staffing levels decrease.

Some ancillary issues will also be investigated, although they can not be experimentally tested hypotheses in this study. One such issue is the comparison of the findings from the BWR and PWR plants. A second issue relates to the appropriateness of current administrative staffing procedures for in-plant shift personnel to support the mitigation of the simulated scenario.

Model Development

For this study, a computer-based workload analysis will be performed in order to assist in the establishment of criteria for the determination of NPP shift staffing levels for both licensed and non-licensed shift personnel. The model will be developed from a thorough analysis of shift staff tasks and operational procedures for the identified scenarios. In addition, information obtained from the simulator study at one staffing level (i.e., the higher, administrative procedure staffing level) will be used in the model development. The model will then be validated based on the information collected from the simulator for the second staffing level (i.e., the lower, technical specification staffing level).

The modeling technique to be used is task network modeling. In task network modeling, the activities of an individual(s) performing a function (e.g., operating an NPP) are decomposed into a series of subfunctions which are subsequently decomposed into tasks. Task network modeling can be used to address the key question: "What are the expected changes in operator performance, both time and error rate, based on changes in shift staffing?" This assumes that (1) valid task network models of existing systems can be created from information collected in the course of the site visits; (2) once created, the task network model can be modified to reflect changes in NPP shift staffing levels; and (3) the modified task network models provide useful predictions of human performance times and error rates. Central to the concept of task network modeling is the ability to use these models to make predictions through computer simulation of the model. Micro Saint (Laughery, 1989) is a computerized modeling system that has been designed specifically to facilitate the simulation of task network models. Micro Saint provides all of the tools needed to build, run, and analyze complex computer models and has been determined to be an appropriate system to be used for this study.

Two separate models will be developed, one for the BWR and one for the PWR plants, and both models will incorporate in-plant as well as control room personnel. The models will be developed using plant procedures and subject matter experts. In addition, since the simulator study will be run using two different staffing levels, the parameters of the model will be set using the data collected under the higher staffing level. The model will then be modified to reflect any structural changes associated with a

reduced crew size, which will correspond to the second staffing level used in the simulator study. All changes made to the model to reflect this reduced crew complement will be made without any use whatsoever of the empirical data collected in the simulator study for the reduced staffing levels. The revised models will be run 10,000 times each and data will be collected for the purpose of model validation which will include comparison of the data obtained from the model to the actual data collected in the simulator experiments.

Products from this Research

Once this research is completed, numerous useful products will be obtained related to the adequacy of shift staffing levels within the U.S. commercial nuclear power industry. First, this study will provide insights on the shift staffing practices of the nuclear industry. Of particular importance is the fact that this study has placed special emphasis on non-licensed shift personnel, a group which has not received the same level of focus regarding staffing levels as that received by licensed personnel. This research will also provide an integrated perspective through the use of both simulator and on-site data collection studies. The on-site data collection studies will provide a reality base from which the simulator studies can be conducted. A model for use in workload analysis will also be obtained at the completion of this research. This model may be useful in moving towards performance-based regulation as well as in other applications where variables besides staffing levels are manipulated. Finally, a NUREG/CR will be prepared that will detail all of the results obtained in the course of conducting this research project.

References

10 CFR 50.54(m), "Energy: Conditions of Licenses," Code of Federal Regulations, Washington, DC, January 1, 1992.

50 FR 43621, "Policy Statement on Engineering Expertise on Shift," Federal Register, October 21, 1985.

Laughery, K.R., "Micro Saint - A Tool for Modeling Human Performance in Systems," in McMillan, G.R., Beevis, D., Salas, E., Strub, M.H., Sutton, R., and Van Breda, L., eds., Applications of Human Performance Models to System Design, Plenum Press, New York, 1989.

Melber, B., Roussel, A., Baker, K., Durbin, N., Hunt, P., Hauth, J., Terril, E., and Gore, B. "Staffing Decision Processes and Issues: Case Studies of Seven U.S. Nuclear Power Plants," NUREG/CR-6122, March 1994.

SECY-93-184, "Shift Staffing at Nuclear Power Plants," June 29, 1993.

SECY-93-193, "Policy on Shift Technical Advisor Position at Nuclear Power Plants," July 13, 1993.

Shurberg, D., Barnes, V., Plott, B., Haagensen, B., Diamond, D., Laughery, R., and Haber, S. "Identification of Issues Associated with Nuclear Power Plant Shift Staffing Levels," BNL Letter Report, Brookhaven National Laboratory, New York, July 20, 1994.

U.S. Nuclear Regulatory Commission, "Clarification of TMI Action Plan Requirements, Supplement 1," NUREG-0737, U.S. Nuclear Regulatory Commission: Washington, DC, 1980.

Operator Use of Procedures During Simulated Emergencies

Emilie M. Roth & Randall J. Mumaw
Westinghouse Science & Technology Center

Paul M. Lewis
U. S. Nuclear Regulatory Commission

Abstract

This paper summarizes the results of an empirical study of nuclear power plant operator performance in cognitively demanding simulated emergencies. During emergencies operators follow highly prescriptive written procedures. The objectives of the study were to understand and document what role higher-level cognitive activities such as diagnosis, or more generally 'situation assessment,' play in guiding operator performance, given that operators utilize procedures in responding to the events. The study examined crew performance in variants of two simulated emergencies: (1) an Interfacing System Loss of Coolant Accident and (2) a Loss of Heat Sink scenario. Data on operator performance were collected using training simulators at two plant sites. Up to 11 crews from each plant participated in each of two simulated emergencies for a total of 38 cases analyzed. Crew performance was videotaped and partial transcripts were produced and analyzed. The results revealed a number of instances where higher-level cognitive activities such as situation assessment and response planning enabled operators to handle aspects of the situation that were not fully addressed by the procedures. The paper summarizes these cases and their implications for the development and evaluation of training and control room aids, as well as for human reliability analyses. The full report of the study is published as NUREG/CR-6208.

Introduction

Human performance is a significant contributor to nuclear power plant (NPP) safety (e.g., Trager, 1985; Kauffman, Lanik, Trager, and Spence, 1992). During emergency situations operator action can have a substantial impact on the ability to return the plant to safe operation. Operators may take recovery actions that mitigate the emergency situation. Alternatively, errors in performance can delay or hinder plant recovery.

Examination of actual incidents both inside and outside the NPP industry indicates that incidents often involve complicating factors (e.g., failed sensors; multiple faults) that impose difficult cognitive demands on operators (Perrow, 1984; Wagenaar and Groeneweg, 1987; Reason, 1990; Woods, Johannesen, Cook, and Sarter, 1993). Complications include sensor failures that make situation assessment difficult, cases where available procedures do not map well to the

specifics of the situation, and situations where balancing of multiple goals related to safety is required (e.g., NRC, NUREG-1154; NRC, NUREG-1455; Kauffman et al., 1992).

As part of a U. S. Nuclear Regulatory Commission project to model the cognitive activities that underlie NPP operator performance in emergencies, an empirical study was conducted to examine operator performance in cognitively demanding simulated emergencies. The objectives of the study were to understand and document what role higher-level cognitive activities such as diagnosis, or more generally 'situation assessment,' play in guiding operator performance, given that operators utilize emergency operating procedures (EOPs) in responding to the events. This paper summarizes the results of the empirical study. A complete description of methods, results and conclusions of the study can be found in NUREG/CR-6208 (Roth, Mumaw, & Lewis, 1994).

In an emergency the role of the operator is to ensure plant safety. The operator monitors automatic plant safeguard systems, initiates recovery actions to minimize radiation release and equipment damage and return the plant to a stable condition, and ensures that critical safety functions are maintained. EOPs provide predefined strategies for accomplishing these functions. When an emergency arises that causes the reactor to trip, the operators are required to take out the EOPs and follow the procedures step by step[1]. The EOPs provide detailed guidance on what plant parameters to check, how to interpret the symptoms observed, and what control actions to take.

Given that operators utilize highly prescriptive procedures in responding to emergencies, a question arises regarding the nature and extent of cognitive activity required of operators to adequately handle emergencies. One view is that all that is needed of operators is that they understand and follow the steps in the EOP. Under this view what is needed for successful performance is that operators be able to read and understand the individual steps in the procedure, that they be able to locate and read the plant parameter values specified in the procedure steps, and that they be able to locate the controls and take the actions indicated in the procedure steps. Another view is that higher-level cognitive activities such as situation assessment and response planning continue to be important for successful operator performance, even when EOPs are employed. Under this view the role of situation assessment and response planning is to enable crews to identify and deal with situations that are not fully addressed by the procedures. These alternative views have very different implications for the kinds of training, procedures, displays and decision-aids that need to be provided to operators. They also have very different implications for the kinds of analyses that are required to assess human reliability.

The study we conducted was designed to shed light on the role of higher-level cognitive activities in guiding operator performance in emergencies.

Overview of Study Methodology

The study examined crew performance in cognitively demanding simulated emergencies. Variants of two base scenarios were run: an interfacing loss of coolant accident (ISLOCA) into the Residual Heat Removal (RHR) System and a Loss of Heat Sink (LHS) event complicated by a leaking pressurizer Power Operated Relief Valve (PORV). These emergency scenarios were

[1] Exceptions arise where operators are expected to use their judgment in determining whether to follow the literal interpretation of a step. These exceptions are often covered in training and background documents. Several examples of exception cases arose in the simulated events we ran and are discussed below.

designed to create situations where active situation assessment and response plan evaluation and adaptation were needed on the part of the operating crew to handle the events.

Data on operator performance were collected using training simulators at two plant sites. Two utilities were asked if they would voluntarily participate in an empirical study of operator performance in cognitively complex simulated emergencies. Both agreed to run an ISLOCA and a Loss of Heat Sink event as part of the regularly scheduled requalification training exercises at one of their nuclear power plant sites.

Up to 11 crews from each plant, including both actual operator crews currently on shift and staff crews, participated in each of two simulated emergencies for a total of 38 cases analyzed.

Analysis of Situations Where Operators Exhibited Higher-Level Cognitive Activity

Crew performance was videotaped and partial transcripts of the crew performance were produced. These transcripts were then analyzed to:

- Identify situations that arose where operators needed to engage in higher-level cognitive activities in order to deal with the situation;
- Document behaviors the operators engaged in to handle those situations that were not explicitly directed by a specific EOP step (hereforth referred to as *extra-procedural* activities).

The extra-procedural activities provided evidence of situation assessment and response planning. A model of cognitive activity provided the framework for linking the specific extra-procedural activities observed to the higher-level cognitive activities.

Analysis of Crew Interaction Skills

In addition to examining the role of higher-level cognitive activity in guiding operator performance, we also examined the role of crew interaction in handling the cognitively demanding scenarios. Under a separate program sponsored by the U. S. NRC, Montgomery et al. (1992) identified six dimensions of team interaction skill, and developed Behaviorally Anchored Rating Scales (BARS) for measuring crew performance on those dimensions. The dimensions of crew interaction skills are: communications; openness; task coordination; team spirit; maintaining task focus in transitions; and adaptability. In this study we examined crew performance in the scenarios to identify cognitively demanding situations that arose where good crew interaction skills appeared to be important for successful performance from a technical perspective (i.e., for correctly identifying plant malfunctions and taking appropriate action). We identified particular crew behaviors that characterized good performance on BARS dimensions, and appeared to be important for successful technical performance on the scenarios.

The analysis particularly focused on how crews organized themselves to manage the dual requirements of (1) following through the steps in the EOPs and (2) engaging in extra-procedural activities in order to handle aspects of the situation that were not covered by the EOPs. We focused on examining how different crews divided up these dual responsibilities, and whether differences in technical performance resulted. We also examined crew ratings on the BARS scales to assess (1) whether there was variability in crew scores on the BARS dimensions, and

(2) whether there was a relationship between BARS ratings of team skill and crew performance on the scenarios from a technical perspective.

Simulated Scenarios: ISLOCA Scenarios

The ISLOCA scenarios involved a leak from the high pressure Reactor Coolant System (RCS) to the low pressure Residual Heat Removal (RHR) System. In one variant of the event (ISLOCA 1) the RCS leak into the RHR eventually led to an RHR pipe rupture in the Auxiliary Building causing reactor coolant fluid to spill onto the floor of the Auxiliary Building. In the second variant (ISLOCA 2) the event started in the same way; however, the buildup of pressure in the RHR led to a break in the heat exchanger between the RHR system and the Component Cooling Water (CCW) system causing RCS fluid to get into the CCW system.

The ISLOCA scenarios were designed to be difficult from the point of view of situation assessment. The objective was to create a situation where the crews had to identify and isolate the leak into the RHR without explicit procedural guidance.

While the EOPs contain procedures for identifying and isolating an ISLOCA, it was possible to create a situation where the crews could not reach the ISLOCA procedure within the EOP network. This is because the plant symptoms generated early in the event are similar to the pattern of symptoms that would be produced by a Loss of Coolant Accident (LOCA) inside containment. By timing the dynamics of the event carefully we were able to create a situation where the EOPs directed the operators to a procedure for a LOCA inside containment.

In one variant of the event , ISLOCA 1, at Plant 1, once in the LOCA procedure there was no explicit transition to the ISLOCA procedure. The crews eventually reached a step in the LOCA procedure that asked them to "try and identify and isolate the leakage." Thus we were able to observe crew performance in a situation where the EOP explicitly required the crews to identify and isolate the leak without more detailed procedural guidance.

In the second variant of the event, ISLOCA 2, at Plant 2, while there was an explicit transition to the ISLOCA procedure from the LOCA procedure, either the transition step could not be reached, or the criteria for transitioning to the ISLOCA procedure were not met when the transition step was reached. Thus we were able to observe crew performance in a situation where the procedure containing relevant guidance could not be reached within the EOP transition network.

In both variants of the scenario the crews had to identify the ISLOCA into the RHR in attempting to isolate the leak. This situation assessment was cognitively demanding because initial symptoms were typical of a LOCA inside containment. Correct situation assessment required integrating multiple symptoms across different systems. The first alarms indicate pressure and level decreases in the pressurizer. These are soon followed by alarms indicating radiation inside containment. Radiation in containment strongly points to an RCS leak directly into containment (i.e., a LOCA). In fact, the radiation in containment was caused by the leak into the RHR. A relief valve in the RHR system vents to the Pressurizer Relief Tank (PRT) inside containment. The PRT eventually ruptures, resulting in radiation in containment. The crews needed to recognize these physical system interconnections in order to link the symptoms in containment with a potential problem in the RHR.

In ISLOCA 1 a correct situation assessment required the crews to connect the symptoms in containment with the symptoms in the Auxiliary Building. ISLOCA 2 was cognitively more demanding because it required the crews to integrate evidence across more systems and postulate a more complex causal chain of events to account for all the symptoms observed. In particular, the crews needed to recognize that the radiation in the CCW was due to RCS fluid that leaked into the RHR and entered the CCW via a heat exchanger between the RHR and the CCW.

Once the operators identified a leak into the RHR they needed to take action to attempt to isolate the leak. The appropriate action to take depended on the postulated source of the leak. In the event we ran there were two hypotheses for the source of the leak that were equally plausible in that they could fully explain the available evidence. One was a failure of the two isolation valves between the hot leg loop of the RCS system and the RHR on the suction side of the RHR pump. This is the event that we postulated. Given this hypothesis the actions required to isolate the leak are to call the Auxiliary Building to request that the valves be re-energized, to verify that they are closed, and to close them if they are not. The alternative hypothesis was that there was a leak back from the RCS through a series of failed check valves. Given this hypothesis, the leak could be isolated by closing an isolation valve on the discharge side of the RHR pump that is normally kept open.

In ISLOCA 2 the crews also needed to take action to isolate the leak from the RHR into the CCW. This step required that they identify the RHR heat exchanger as the source of the leak and take action to isolate it.

Simulated Scenarios: Loss of Heat Sink Scenarios

The Loss of Heat Sink event involved a total loss of feedwater flow complicated by a leaking pressurizer power operated relief valve (PORV). The objective was to create a situation where the EOPs focused operator attention on one high priority problem -- a loss of heat sink -- and then examine how the crews discovered and dealt with a second potentially serious fault that arose: a leaking pressurizer PORV.

The Loss of Heat Sink event was designed to be cognitively demanding from the perspective of both situation assessment and response planning. In this scenario feedwater to the steam generators is lost and the EOPs direct the operators to a Loss of Heat Sink procedure that specifies actions the operators should take in attempting to recover feedwater. While following the Loss of Heat Sink procedure, the operators are directed to open and then close the pressurizer PORV in order to reduce pressurizer pressure. In the event we ran the pressurizer PORV never fully closes (although it read closed), resulting in a leak on the primary side. The analysis focused on how the operators discovered and dealt with the leaking PORV, given that the EOPs provided no explicit guidance.

The scenario was demanding from the perspective of situation assessment because it created a situation where operator judgment was needed to discriminate plant behavior that was the result of known factors (i.e., an operator induced cooldown) from plant behavior that signaled an additional plant fault. Many of the early symptoms of the leaking pressurizer PORV (i.e., decreasing pressurizer level and pressure) could be attributed to a cooldown caused by the control actions that the operators were taking to recover the secondary side heat sink. As the event progressed the symptoms on the primary side became more severe (i.e., reactor vessel level decreased; a bubble formed in the vessel; the pressurizer became solid). Those symptoms could not be explained by a cooldown caused by activities on the secondary side.

The Loss of Heat Sink scenario was also designed to be challenging from the perspective of response planning. In one variant of the scenario, LHS 1, at Plant 1, secondary side feedwater is never recovered. As a result the crews remain in the Loss of Heat Sink procedure. This variant was designed to place crews in a situation where they had to decide whether to manually initiate a safety system under conditions where procedural guidance was minimal, and multiple goals needed to be considered and balanced.

Specifically, the crews had to decide whether to manually initiate safety injection (SI). There was a step early in the Loss of Heat Sink procedure that had the crews block SI.[2] This action has potentially serious safety consequences because it means that a major automatic safety actuation system is no longer in operation and must be manually initiated if needed. The only procedural guidance available to the operators regarding manual initiation of SI was in a caution that stated: "Following block of automatic SI actuation, manual SI actuation may be required if conditions degrade."

The LHS scenario was designed to place the crews in a situation where they had to decide whether to initiate SI under conditions where there were multiple goals that needed to be considered. The leaking pressurizer PORV created a situation where RCS conditions became progressively more abnormal. Eventually, RCS pressure decreased to the point where a bubble formed in the reactor vessel. Level in the reactor vessel continued downward, while level in the pressurizer started to go up. In some cases the pressurizer became full. The degrading RCS conditions could be mitigated by manually initiating SI; however, the decision of whether to manually initiate SI is made complex because it affects heat sink recovery efforts. Initiating SI would impede efforts to recover feedwater flow on the secondary side, and increase the probability that the crews would have to resort to a less desirable means of achieving a heat sink (i.e., bleed and feed). The objective of this aspect of the scenario was to examine how crews responded to the degrading conditions in the RCS, given that the only relevant procedural guidance available to them was in a caution. Specifically, the analysis focused on whether the crews chose to initiate SI and the rationale for their decision.

The second variant of the Loss of Heat Sink event, LHS 2, at Plant 2, was also demanding from the perspective of response planning. In this scenario the crews eventually got feedwater back. As a result the Loss of Heat Sink procedure transitioned them back to the procedure they had been in when feedwater was lost, which was the Reactor Trip Response procedure. This transition introduced new cognitive challenges because some of the steps in the Reactor Trip Response procedure were no longer appropriate. The crews were now feeding through the condensate system which involves a different plant configuration than is assumed by the Reactor Trip Response procedure. Some of the steps in the Reactor Trip Response procedure, if followed verbatim, would undo actions that had been performed to recover feedwater, causing a loss of heat sink. This variant of the Loss of Heat Sink scenario provided the opportunity to observe how operators respond in cases where actions specified in procedure steps are not perceived to be appropriate to the specific situation.

---

[2]SI is blocked to avoid spurious activation of safety injection when the steam generators are depressurized below an SI actuation set point later in the procedure.

Overview of Results

The Role of Higher-Level Cognitive Activity

The results of the study supported the view that crew situation assessment and response planning continue to play an important role, even when EOPs are employed. We found a number of situations where situation assessment and response planning enabled the crews to handle aspects of the situation that were not fully covered by the procedures. These included:

- An EOP step that explicitly requested that crews identify and isolate a leak on their own;
- A case where the procedure containing relevant guidance could not be reached within the EOP transition network;
- Cases where operators needed to determine whether plant behavior was the result of known manual and/or automatic actions (e.g., a controlled cooldown) or the result of a plant fault;
- A case where operators were required to evaluate the appropriateness of procedure steps given the specifics of the situation;
- Cases where operators had to evaluate the procedure path and take action to redirect the procedure path;
- A case where operators had to decide whether to manually initiate a safety system based on consideration and balancing of multiple goals related to safety.

In each of the simulated scenarios situations arose where operators needed to engage in situation assessment and response planning in order to handle aspects of the situation that were not fully covered by the EOPs.

ISLOCA Scenarios

In one variant of the ISLOCA scenario (ISLOCA 1) the crews were required to identify and isolate a leak into the Residual Heat Removal System (RHR) without explicit procedural guidance. In the second variant of the scenario (ISLOCA 2), while there was a procedure transition available to an ISLOCA procedure, it could not always be reached. Even in the cases where the ISLOCA procedure was reached, the procedure did not cover all aspects of the situation, i.e., a leak from the RHR into the Component Cooling Water System (CCW) in ISLOCA 2.

Most crews actively sought information to help identify the sources of leaks into the RHR and CCW, and identified and took actions in an attempt to isolate the leaks. They actively utilized resources beyond the EOPs, such as schematics and alarm printouts, to support their identification and isolation of the leaks. Without active situation assessment, and response planning, they would not have been able to identify and isolate the leaks.

At the same time most of the crews recognized the importance of continuing to proceed through the EOPs. They perceived getting to the Cooldown and Depressurization procedure as a high

priority activity. Balancing the dual requirements to pursue the leak into the RHR with the need to proceed expeditiously through the EOPs provided one of the most challenging aspects of the ISLOCA scenarios.

The ISLOCA scenarios also provided evidence of crews actively engaging in reasoning about the procedure logic. Clear instances were found of crews reasoning at two levels. The crews were engaging in situation assessment and goal identification. At the same time they were reasoning about the strategies underlying the EOPs, and the EOP transition network logic in order to assess whether the procedure they were following would enable them to achieve plant goals in a timely manner.

We found instances where monitoring the appropriateness of the procedure path enabled crews to identify when they were in an unproductive loop, and to identify another procedure path that would allow them to take necessary actions more expeditiously.

Loss of Heat Sink Scenarios

The Loss of Heat Sink scenarios provided further evidence that complex multiple fault conditions can arise where operators need to actively engage in situation assessment and response planning. In the Loss of Heat Sink scenarios the procedure provided no guidance in identifying and responding to the leaking pressurizer PORV. The majority of crews were successfully able to detect the symptoms on the primary system and integrate them to identify the leak. This was a difficult cognitive task that required recognizing that the primary side behavior could not be entirely accounted for by the ongoing cooldown caused by efforts to recover the heat sink. This task required qualitative reasoning about the size and direction of effects on the primary system that could be expected from the rapid depressurization of the steam generators.

In one variant of the Loss of Heat Sink scenario (LHS 1), the crews were faced with a decision regarding manual initiation of a safety system. The only EOP guidance available to them was in a caution that indicated that they had discretion to turn on the safety system if conditions in the plant "degraded." The decision of whether to turn on the safety system required balancing multiple goals. Manual initiation of the safety system would respond effectively to the degrading conditions in the primary system caused by the leaking PORV, but could potentially delay recovery of heat sink. The crews had some difficulty with this aspect of the scenario. Most of the crews did not recognize that they had the discretion to decide whether to turn on the safety system. Further, few of the crews showed evidence of considering the tradeoffs involved. The majority of crews chose to let conditions continue to degrade until a criterion was reached for which more explicit procedural guidance was available.

The second variant of the Loss of Heat Sink scenario (LHS 2) provided additional opportunity to examine the role of situation assessment in guiding crew performance. In this scenario a case arose where operators had to decide the appropriateness of specific procedure steps based on their own situation assessment. In LHS 2 the crews recovered feedwater on the secondary side using the condensate system, thus restoring the heat sink. As required by the EOPs they then returned to the procedure that had been in effect prior to the loss of heat sink, which was the reactor trip procedure. This procedure contained some steps that required them to undo actions they had just taken to recover feedwater. If they followed those steps it would result in a loss of heat sink again. The EOP background document explicitly recognized that this type of situation

could arise and indicated that in those cases operator judgment would be required in determining appropriate action.

Most of the crews correctly recognized that some of the steps in the Reactor Trip procedure were inappropriate to the situation and should not be followed. This included steps that called for initiation of a safety system if certain criteria were met. The decision that initiation of the safety system was not needed was based in part on situation assessment. The crews had to determine whether the conditions in the primary system were due to a controlled cooldown or a plant fault. This was not a simple determination, as attested by the fact that, in the case of two of the crews who faced that decision, there was a leak present (leaking pressurizer PORV), but the crews nevertheless initially attributed the primary side symptoms to cooldown, and decided against manual initiation of the safety system.

Evidence of the Importance of Situation Assessment

The scenarios provided extensive evidence of crews trying to develop an understanding of plant state. We observed operators engaging in knowledge-driven monitoring to confirm their understanding of a situation and seeking explanation for unexpected plant behavior. We also observed operators actively trying to form a coherent explanation to account for multiple symptoms across diverse systems. These activities enabled the crews to identify and respond to problems that were not fully addressed by the EOPs.

Situation assessment enabled the crews to:

- Detect abnormal plant behavior earlier in the event than would be possible if they waited for an alarm or a step in the procedure to check those parameters;
- Detect symptoms or alarms that they had missed earlier;
- Identify and deal with additional problems that were not addressed by the procedures.

It is reasonable to assume that situation assessment would play a similar role in enabling crews to identify and deal with problems in other cognitively demanding situations.

The importance of situation assessment is underscored by the frequency of recent actual incidents where crews were required to discriminate actual malfunctions from failed sensors or false alarms (Kauffman et al., 1992). The results of the present study as well as analyses of actual incidents suggest that it is important for operators to develop and maintain an accurate situation assessment in order to handle aspects of incidents that are not fully addressed by the procedures. Important elements of situation assessment include (1) an awareness of abnormal plant symptoms, (2) an assessment of the likely malfunctions that could produce those symptoms, and (3) an awareness of manual and automatic system actions that are being taken, and their effect on plant state.

Evidence of the Importance of Response Planning

The scenarios were designed to produce situations where operators were required to engage in response planning. In some cases this involved identifying and evaluating response actions on

their own. In other cases, it involved monitoring the appropriateness of response actions specified in the procedures, and adapting the procedures to the situation if judged necessary.

We found evidence of crews reasoning at two levels. They engaged in situation assessment and goal identification. At the same time they monitored the procedure path they were following to evaluate progress toward high priority goals.

Response planning enabled the crews to:

- Move through the procedures efficiently;
- Catch and recover from errors -- both operator errors and errors in the procedures;
- Assess whether the procedure path they were on was appropriate to the situation;
- Fill in gaps and adapt procedures to the situation; and
- Deal with unanticipated situations that went beyond the available procedural guidance.

It is reasonable to assume that the role of response planning in enabling crews to deal with these situations would generalize to other cognitively demanding emergencies.

The results provide evidence that it is important for operators to be able to develop and evaluate response plans. It is also important for them to understand the assumptions and logic behind the EOPs. This understanding includes the intent behind specific procedure steps, the overall response strategies inherent in the procedures, and the transition logic among particular procedures in the EOPs.

Variability in Crew Performance

In general, across scenarios, the majority of crews performed well. They identified the faults and took appropriate action in response. The behavior of these crews clearly indicated that they were actively engaged in situation assessment and response planning.

While most of the crews performed well, variability in performance was observed in all the scenarios. Crews differed in the extent to which they detected plant symptoms, actively sought an explanation for unexpected findings, and attempted to come up with a coherent explanation that accounted for all the observed symptoms. In each scenario there was at least one crew that had difficulty identifying the source of the problem and taking appropriate action to mitigate it (i.e., approximately 10% of crews run in the event). The fact that not all crews in the scenarios formed the correct situation assessment suggests that there is room for improvement.

The Role of Crew Interaction Skills

We also examined crew interaction in handling these cognitively demanding scenarios. The objectives of the analysis were: (1) to clarify the conditions under which crew interaction skills might be expected to affect technical performance of crews and (2) to begin the process of describing specific crew behaviors that potentially contribute to better technical performance.

Cognitively Demanding Situations Where Good Crew Interaction was Important

We identified three types of cognitively demanding situations where specific types of crew interaction appeared to contribute positively to successful crew performance from a technical perspective. These were:

- Cases where operators needed to pursue multiple objectives. Specifically, cases where they had to manage dual requirements to (1) proceed through the EOPs to cool down the plant and bring it to a more stable state in a timely manner and (2) engage in extra-procedural activities to handle aspects of the situation that were not covered by the EOPs;
- Cases where situation assessment required integration of information that was distributed across crew members; and
- Cases where crews had to evaluate the appropriateness of a procedure path and/or decide whether to take actions not explicitly specified in the procedures.

In each case we examined characteristics of crew interaction that appeared to contribute positively to crew performance from a technical perspective.

Cases Where Crews Needed to Pursue Multiple Objectives

In the two ISLOCA scenarios crews needed to engage in extra-procedural activity to identify and isolate the leak into the RHR. They also needed to proceed with the cooldown as rapidly as possible to reduce the effect of the leak and stabilize the plant. We examined how crews organized themselves to deal with these multiple objectives, and whether some crew styles of organization led to better performance than others.

Two crew styles of organization were identified. Some crews appeared to alternate between following the steps in the EOP and situation assessment and response planning activities. For example, when these crews got to the step in the LOCA procedure requiring them to identify and isolate the leak, they tended to stay a long time on that step. This crew style was labeled "alternate." A second crew style we identified was characterized by a tendency for the crew to divide into two subgroups, with one subgroup concentrating on trying to identify and isolate the ISLOCA and the second subgroup concentrating on moving through the procedures in order to get to the cooldown more quickly. For example, in the case of one crew (Crew F) the Supervising Operator explicitly requested that the SS and RO use the ISLOCA procedure to try and identify and isolate the leak into the RHR, while he and the BOP continued with the LOCA procedure. We labeled this crew style "divide and conquer."

We examined whether one crew style of organization enabled the crews to reach a cooldown state more quickly than the other. We computed the time in minutes from reactor trip to the time the crews started the Post-LOCA Cooldown and Depressurization procedure.[3] In both the case

[3] In the case of the two crews (Crew 6 and Crew 4) that transitioned to the ISLOCA procedure, the time to cooldown was computed as the time from reactor trip to the Loss of Emergency Coolant Recirculation procedure.

of ISLOCA 1 and ISLOCA 2 the crews that were identified as "divide and conquer" reached the cooldown procedure faster than the crews that were identified as "alternate."

In ISLOCA 1 seven crews reached the cooldown procedure. Of these, four crews were classified as "divide and conquer" and had a mean time of 34 minutes to get to the cooldown procedure. Three were classified as "alternate" and had a mean time of 42 minutes to get to the cooldown procedure. In the case of ISLOCA 2 two crews were classified as "divide and conquer" and had a mean time of 32 minutes to reach the cooldown procedure. Seven were classified as "alternate" and had a mean time of 56 minutes to get to the cooldown procedure. Collapsing across the two scenarios the mean time to cooldown for "divide and conquer" crews was 33 minutes (n=6), while the mean time to cooldown for "alternate" crews was 52 minutes (n=10). This difference is statistically significant using a two-tailed t-test ($p < 0.05$).

Since proceeding expeditiously to the Post-LOCA Cooldown and Depressurization procedure is a high priority goal, the results suggest that a "divide and conquer" crew organization style may have certain benefits over an "alternate" crew style because it is likely to allow the crews to proceed through the EOPs more rapidly. These benefits only hold if the two subgroups maintain close communication and coordination to ensure that they are not taking actions that interfere with one another. The groups that used a "divide and conquer" strategy tended to use the Supervising Operator as a focal point and alerted him of all major actions before taking them. An illustrative example arose in ISLOCA 2. This was a case where the actions taken by the subgroup that was pursuing the source of the leak into the RHR (isolating the CCW service loop) affected activities of the subgroup that was working through the Post-LOCA Cooldown and Depressurization procedure (procedure steps that assumed the CCW service loop was available). Because the two subgroups communicated their actions, a potential impasse was identified and resolved.

These results point to the importance of the team skills of communication, coordination, and adaptability to changing plant conditions in dealing with situations that require simultaneous pursuit of multiple objectives. More specifically, the results suggest particular crew behaviors that may lead to improved technical performance (i.e., crews breaking up into subgroups with the Supervising Operator as the point of focus for communication and coordination).

Cases Where Situation Assessment Required Integration of Information Across Multiple Crew Members

A second case where crew interaction skills appeared to be important to technical performance was in forming correct situation assessment in cases where the pieces of evidence that had to be identified and integrated were distributed across crew members. Two of the BARS dimensions of crew interaction skills appeared to be important to technical crew performance in these cases. One was communication. In the simulated scenarios cases arose where a piece of evidence that was needed to identify the plant fault was only seen by a single crew member, and there was no EOP step that specifically requested that piece of information. In those cases correct situation assessment depended on the crew member recognizing the value of the information and communicating it to the rest of the crew. A specific case in point was the rupture of the PRT in ISLOCAs 1 and 2. The crew member who noticed the symptoms in the PRT needed to communicate that information to the other crew members in order for the leak into the RHR to be identified. In one case (Crew 3, ISLOCA 2) one of the crew members knew the PRT had ruptured but failed to communicate it to the Supervising Operator and the rest of the crew. This crew did not identify the problem in the RHR until late in the event.

A second dimension of crew interaction skill that appeared to be important for correct situation assessment was openness. The results showed that crew members in all positions contributed positively to hypothesis generation and revision. This was shown most clearly in the case of ISLOCA 1. While the first hypothesis generated to explain the plant symptoms was most often generated by the Supervising Operator (five out of 11 cases), there were also cases where it was the SS or the BOP that generated the first hypothesis. Further, when we looked at cases where the initial hypothesis was revised, and examined which crew member suggested the revised hypothesis, we found that crew members in all positions were represented (i.e., RO, STA, SS, BOP). In cases where the first hypothesis that was generated was relatively implausible, and it was revised to a more plausible explanation, the crew member who suggested the revised hypothesis was different from the crew member who suggested the original hypothesis. These results suggest that having multiple crew members participate in the generation and revision of hypotheses contributes positively to correct situation assessment. In turn, this suggests that "openness" of crew members with respect to suggesting and critiquing hypotheses contributes positively to correct situation assessment.

Cases Where Crews Had to Evaluate Whether to Take Actions Outside the Procedures

A third type of situation where a positive role of crew interaction on technical performance was identified was when crews had to evaluate the appropriateness of a procedure path and/or decide whether to take actions not explicitly specified in the procedures. Analysis indicated that "openness" in crew interaction was important both from the perspective of generating proposed actions to take, and from the perspective of evaluating those proposed actions. A clear example occurred in ISLOCA 1 where crews considered whether to isolate the affected RHR train. Examination of crew performance in that case revealed that the initial suggestion to isolate the RHR was made by crew members in a variety of positions (i.e., Reactor Operator, Shift Technical Advisor, Shift Supervisor, Balance Of Plant, and Supervising Operator). In all cases the crews did decide to isolate the RHR train but only after examination of the possible consequences of the action by the crew as a whole. The final decision was made by the Supervising Operator after soliciting input from other crew members and approval from the Shift Supervisor. Similar results were observed in the LHS 2 scenario where crews had to decide whether to deviate from the literal requirements of procedure steps in the Reactor Trip Response procedure.

BARS Ratings of Crew Interaction Skills

The analysis provided above revealed cognitively demanding situations where contributions of multiple crew members appeared to play a role in successful crew technical performance. It also suggested some specific crew behaviors (e.g., dividing into subteams; communicating indications of abnormal plant behavior; volunteering hypotheses; critiquing hypotheses; proposing response actions; evaluating proposed actions) that fell under the BARS dimensions of crew interaction skills that appeared to contribute positively to the technical performance of the crews. The BARS ratings were examined to assess (1) whether there was variability in crew scores on the BARS dimensions and (2) whether there was a relationship between BARS ratings of team skill and crew technical performance on the scenarios.

Mean ratings of the crews on each of the BARS dimensions were examined for each scenario. There was variability in crew ratings on four of the six dimensions. Little or no variability was observed in the ratings of Team Spirit and Task Focus.

Crews varied extensively in degree of communication. Specific behaviors that contributed to a high score on the communication dimension included making sure that all important plant changes and crew actions were known to all crew members, providing periodic summaries of current situation assessment, and announcing activities that were about to be started that would strongly affect plant state (e.g., depressurizing a steam generator that would result in a cooldown). Cases where crews failed to communicate critical plant state information (e.g., that the PRT ruptured) or operator actions (e.g., closing the PORV block valve) resulted in lower scores on the communication dimension.

Crews varied in the 'openness' dimensions. Crews with a high openness score tended to include crew members who volunteered situation assessments or suggestions for actions, and SOs who explicitly solicited the opinion of crew members and sought consensus for all major situation assessments and decisions.

Crews also varied on the dimension of Task Coordination. There were several opportunities to observe the role of crew coordination. In the ISLOCA scenarios crews differed in how they organized themselves to deal with both the need to identify and isolate the leak outside containment and the need to proceed expeditiously to the Post-LOCA Cooldown.

In the Loss of Heat Sink scenarios crew coordination was required to depressurize the RCS and block the SI signal without inadvertently safety injecting. Crews that scored high on the coordination dimension tended to have SOs that provided the operators an overview of the steps about to be taken. These SOs tended to give the crew an overview of the whole maneuver before initiating the RCS depressurization and to explicitly assign specific roles for the different operators.

Crews also varied on the dimension of 'adaptability.' The 'adaptability' dimension was used to rate crews on how quickly they detected and responded to changing plant circumstances. High ratings on this dimension tended to be given to crews that detected and pursued the primary symptoms in each event while continuing to proceed through the EOPs. In the ISLOCA these were the symptoms of a leak outside containment. In the Loss of Heat Sink scenario the primary symptoms were those of a leaking pressurizer PORV.

The dimensions of 'team spirit' and 'maintaining task focus in transitions' seemed less useful in that there seemed to be less variance across crews on these dimensions. All the crews showed positive team spirit. Expressions of anger or frustration at each other were extremely rare.

The fact that variability in ratings occurred across crews on four of the six dimensions suggests that these dimensions may be useful in evaluating crew interaction performance. Previous attempts to use the BARS scales had found limited variability in crew ratings on the events examined. It is possible that there was more variability in crew interaction performance in this study because of the greater cognitive demands of the scenarios. As discussed in Section 3, a number of cognitively demanding situations arose in those scenarios where good technical performance depended on the contributions and coordination of multiple crew members. It is possible that these scenarios placed greater demands on team interaction skills and thus provided the opportunity to observe variability in performance.

We also examined whether a link could be established between crew performance on the BARS ratings of crew interaction and crew technical performance. In general, crew technical performance on the scenarios was very good. The large majority of crews correctly identified the leaks and took appropriate action in attempting to isolate the leaks. Nevertheless, in each scenario there was one crew whose technical performance was clearly less good than that of the other crews (Crew L in ISLOCA 1, Crew 3 in ISLOCA 2, Crew H in LHS 1, and Crew 11 in LHS 2.) These four crews failed to reach a correct situation assessment and as a result failed to take actions needed to isolate the leaks.

BARS ratings for these four crews on the events in question were compared to the BARS ratings for the remaining cases (33 cases). The mean ratings on the four BARS scales for which variability across crews was observed are presented in Table 1. Crews that were classified as 'good' from a technical perspective had higher mean BARS ratings on all four BARS dimensions than the crews that were classified as 'less good' from a technical perspective. Analyses of variance indicated that the mean differences in BARS ratings were statistically significant ($p < 0.05$) in the case of three of the four BARS dimensions: communication, coordination, and adaptation. In the case of the dimension of "openness" the mean difference in ratings was not statistically significant.

Table 1. Mean BARS ratings for crews that differed in technical performance. (Standard deviations appear in parentheses.)

Crew Technical Performance	*Number of Crews*	*Communic.*	*Openness*	*Coordination*	*Adapt.*
Good	33	4.9 (0.9)	5.4 (0.8)	5.0 (1.3)	5.2 (1.3)
Less Good	4	3.5 (2.1)	4.5 (1.9)	3.5 (1.3)	3.0 (0.8)

The statistically significant difference that was obtained on some of the BARS dimensions between crews that performed technically well on the scenarios and crews that performed less well is an important finding. Researchers have generally had difficulty establishing a link between team interaction skills and technical performance. If the finding is reliable it would support the position that team interaction skills contribute to better technical performance. However, because only a single rater (the first author) was used, the reliability of the BARS ratings obtained, and therefore the robustness of the evidence connecting BARS ratings to technical performance, is not clear. Because of the potential importance of the result it may be worthwhile to attempt to replicate the result using a larger group of raters.

General Discussion

Alternative Interpretation of Results

In the introduction we contrasted two alternative views of the nature and extent of cognitive activity required of operators to adequately handle emergencies. One view was that in emergencies the operator's primary role is to follow the EOPs by rote. According to this view all

that is needed of operators is that they be able to understand and follow the individual steps in the EOPs.

This position was contrasted with the view that situation assessment and response planning continue to be important for successful operator performance, even when EOPs are employed. According to this view situation assessment and response planning enable crews to identify and deal with situations that are not fully addressed by the procedures. The results of this study provide support for the second position.

We found a number of situations that were not fully addressed by the EOPs. In all these cases we found evidence of operators actively engaging in situation assessment and response planning in handling the situation.

There are three alternative interpretations of these results, each with distinct implications. If one starts from the premise that procedures should provide detailed guidance for every contingency, then one interpretation of the results is that they demonstrated deficiencies in the particular procedures that were included in the study. According to this view if situations are identified that are not covered by the procedures, then the procedures should be rewritten to handle those situations. Given this view, the results have primary implications for the specific procedures employed in the study.

A second view is that the EOPs are not intended to diagnose and respond to particular faults optimally. They are intended to provide a systematic approach to emergency response that minimizes the possibility of core damage. According to this view, while the operators may have engaged in situation assessment and response planning in these scenarios, these cognitive activities were not necessary, and were possibly not even desirable. Had the operators followed the procedures implicitly they would have eventually been directed to take actions that would have mitigated the consequences of the leaks and prevented core damage. Given this view, the primary contribution of the study is that it demonstrates that operators take a more active role in diagnosing and responding to events than might have been believed; however, the results have minimal implications for training and procedures.

A third view is that the types of situations that were identified in the study are generic classes that are likely to arise in other emergency scenarios. According to this view, the complexity of NPPs make it difficult to anticipate and develop EOPs that cover every possible contingency in detail; therefore it is reasonable to assume that situations may arise that are not fully addressed by the procedures. It will be important in such situations for the operators to have the ability to form accurate situation assessments and to generate response plans to cover aspects of the situation that are not fully addressed by the procedures. Examination of recent actual incidents support this position (Kauffman et al., 1992). A logical consequence of this third view is that in the development and evaluation of training and control room aids (e.g., procedures, displays, decision-aids), explicit attention should be paid to supporting operator situation assessment and response planning.

While the results of the study do not definitively support one view over the others, arguments are presented in favor of the third view: operators need to engage in situation assessment and response planning to handle unanticipated situations that are not fully covered by the EOPs. This view has implications for training, procedures, and decision aids.

View 1: Procedures should provide detailed guidance for every contingency

One view starts from the premise that procedures should provide detailed guidance for every contingency. Given this premise, the results could be viewed as providing evidence of deficiencies in the particular procedures that were included in the study. According to this view if situations are identified that are not covered by the procedures then the procedures should be rewritten to provide detailed guidance for those situations. While this position is viable in principle, in practice it is likely to be difficult to anticipate and provide detailed guidance for every possible contingency. This argument is supported by experience in attempting to develop detailed procedural guidance in other domains (Roth, Bennett, and Woods, 1987; Suchman, 1987). It is also supported by analyses of actual incidents that often involve multiple faults and complications whose possibility had not been foreseen (Kauffman, Lanik, Trager, and Spence, 1992; NRC, NUREG-1455; Perrow, 1984; Wagenaar and Groeneweg, 1987).

Some of the cases identified in the scenarios could be handled by rewriting the particular procedure to explicitly deal with the case. An example is the situation that arose in ISLOCA 1 where the EOPs asked the operators to identify and isolate the leak without providing further guidance. This procedure could be rewritten to provide more detailed guidance with respect to identifying and isolating the leak.

There were other cases, however, that could not be easily handled by rewriting the procedures. Examples include the case that arose in ISLOCA 2, where detailed guidance for identifying and isolating the ISLOCA was available but could not be reached through the EOP transition network. The reason the ISLOCA procedure could not be reached had to do with the detailed dynamics of the event that determined when symptoms came in relative to when procedure steps were reached. Developing procedures that anticipate and provide for the variety of possible event trajectories that could arise would be a difficult task.

Procedure writers recognize limits in their ability to foresee all possible situations. In some circumstances operators are explicitly directed by the EOPs to take action based on their own situation assessment. There were three cases in the simulated scenarios where the procedures or related background documents explicitly directed operators to determine appropriate action based on their own situation assessment:

1. A case in the ISLOCA scenarios where operators were asked whether pressure in all steam generators is "stable or increasing;"

2. A caution that appeared in the loss of heat sink procedure that provided the operators discretion in initiating a safety system;

3. A case that arose in LHS 2 where operators were expected to determine whether particular procedure steps in the Reactor Trip procedure were appropriate to the situation and should be followed.

View 2: Procedures Are Not Intended to be Optimal

A second view is that the EOPs are not intended to diagnose and respond to particular faults optimally. They are intended to provide a systematic approach to emergency response that minimizes the possibility of core damage. Had the operators followed the procedures by rote

they would have eventually been directed to take action that would have mitigated the consequences of the leaks and prevented core damage. According to this view, while the operators may have engaged in situation assessment and response planning in these scenarios, these cognitive activities were not necessary.

This position underlies the development of the EOPs and provides the rationale for requiring operators to follow procedures by rote. The results of this study do not contradict this position. In both the ISLOCA and the LHS scenarios, had the operators followed the procedures by rote they would have eventually been directed to take action that would have prevented severe core damage; however, conditions would have degraded significantly before the procedures directed the operators to take action to address the problem. This raises a concern because when conditions are allowed to degrade the potential for risk is increased.

View 3: Situation Assessment and Response Planning Enable Operators to Handle Unanticipated Situations

A third view is that the complexity of NPPs make it difficult to anticipate and develop EOPs that cover every possible contingency in detail. According to this view it is reasonable to assume that situations may arise that are not fully addressed by the procedures. In such situations the ability of operators to form accurate situation assessments and to generate response plans to cover aspects of the situation that are not fully addressed by the procedures will be important.

Several lines of evidence support this position including, experience in developing detailed procedural guidance in other domains (Roth, Bennett, and Woods, 1987; Suchman, 1987); experience in introducing automation (Norman, 1986); and analyses of actual incidents that involved multiple faults and complications that had not been foreseen (Kauffman, Lanik, Trager, and Spence, 1992; NRC, NUREG-1455; Perrow, 1984; Wagenaar and Groeneweg, 1987.)

The results of the study, taken in combination with evidence from actual incidents, and experiences in related domains support the position that situation assessment and response planning enable operators to handle unanticipated situations that are not fully addressed by procedures. In Section 5.5 we discuss the implications of this view for the development and evaluation of training and control room aids, as well as for human reliability analyses.

Implications of Results

The view that unanticipated situations may arise in actual incidents where operators need to engage in situation assessment and response planning to deal with aspects of the situation that are not fully addressed by the procedures has potential implications for:

- Training of operators;
- Development of displays and decision-aids to support operator cognitive performance; and
- Human reliability analysis.

Implications for Training

The view that situations may arise where crews need to engage in situation assessment and response planning suggests that in developing and evaluating operator training programs attention may need to be paid to the development of these cognitive skills. While most of the crews in the study were able to identify the leaks correctly and take appropriate action, not all the crews formed an accurate situation assessment. Crew performance might be improved by providing explicit training in situation assessment and response planning.

Figure 1 shows three kinds of operator knowledge required to support situation assessment and response planning:

1. Operators need accurate mental models of plant systems. In our study we found evidence of situations where crews needed to utilize mental models of physical plant systems and to reason qualitatively about expected effects of different factors influencing plant state in order to localize plant faults and identify actions to mitigate them.

2. Another type of knowledge needed is knowledge of important plant goals and means to achieve them. Our study found evidence that operators needed to reason about plant goals, and evaluate alternative means to achieving them, particularly in the Loss of Heat Sink 1 event.

3. Finally, operators need knowledge of the EOPs, which includes not only knowledge of how to follow the individual EOP steps, but also knowledge of the logic that underlies the EOPs. This includes knowledge of the goal prioritization inherent in the EOPs, knowledge of the response plans embodied in the EOPs and their rationale, and knowledge of the EOP transition network. It may be beneficial to explicitly address these types of knowledge in training programs.

Mumaw, Swatzler, Roth and Thomas (1994) provide a detailed review of training techniques for developing these types of knowledge and cognitive skills.

One way to foster situation assessment and response planning skills is to develop cognitively demanding training scenarios that provide the opportunity to practice specific cognitive skills (Roth, Mumaw & Pople, 1992). For example, training scenarios can be developed that specifically focus on the ability to form accurate situation assessments. An example is a scenario that requires crews to discriminate effects due to cooldown from effects due to actual malfunctions. Other scenarios can be developed that focus on response evaluation. For example, scenarios can be developed that require operators to evaluate the appropriateness of particular procedure steps to a given situation and to take discretionary action as appropriate.

The objective of the cognitive training would be to build operator skill in handling cognitively demanding events. Since actual incidents typically involve multiple factors that make them unique, cognitive training may better equip operators to handle these unique features resulting in improved safety.

Implications for Control Room Aids

The view that unanticipated situations can arise where operators need to engage in situation assessment and response planning also has implications for the development and evaluation of

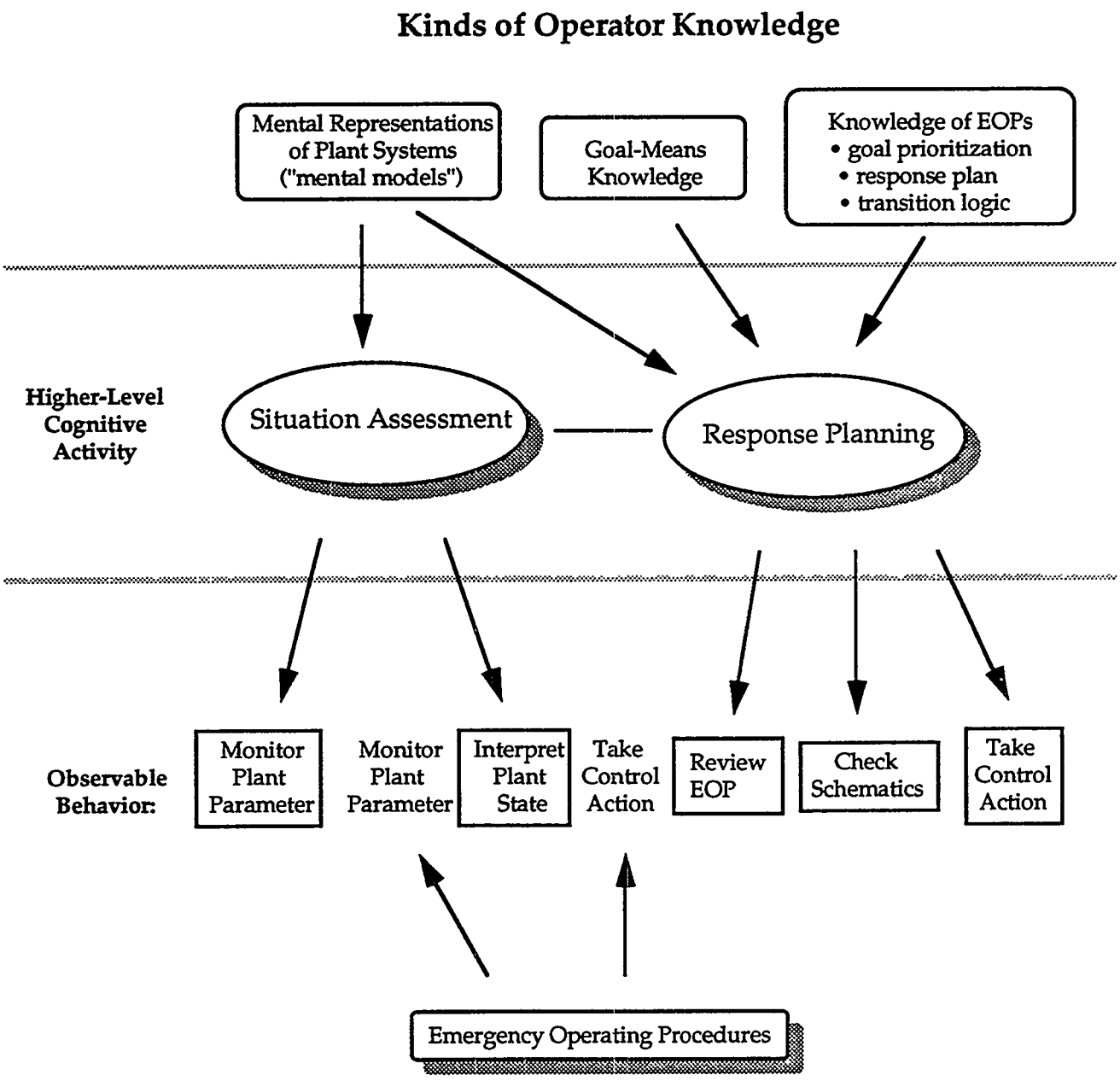


Figure 1. Operator knowledge required to support situation assessment and response planning.

control room aids. In particular, it suggests potential value for displays and decision-aids that are explicitly intended to support situation assessment and response planning.

The results of the study showed that operators sometimes had to engage in situation assessment activity that required tracking multiple influences on plant state and distinguishing plant behavior due to known influences (e.g., a cooldown) from unexpected plant behavior due to an unidentified fault. These judgments often required integrating evidence across space and time. Displays and decision-aids could be developed to support these situation assessment activities.

Similarly, situations arose where crews had to evaluate responses for potential negative consequences. This evaluation step occurred in the ISLOCA incident where crews needed to consider the implications of isolating systems for future recovery activities. It also occurred in the Loss of Heat Sink event where crews had to consider the positive and negative consequences of initiating SI. Displays and decision-aids that facilitate identification of side effects and consequences of contemplated actions could be developed to support response evaluation.

The results also have implications for procedures. Two findings in the study have potential implications for design of procedures, particularly computerized procedures. One finding is that it was important for operators to understand the logic and rationale behind the procedures. This has implications for the content and organization of procedures. Another finding is that operators did not necessarily move linearly through a single procedure path. Crews looked ahead in the procedures, they moved back to earlier steps, and they looked at other procedures in parallel as guidance. This finding has implications for the design of computerized procedures. It suggests that ease of navigation through the procedure network is likely to be important for facilitating performance in complex emergencies.

Implications for HRA

The view that operator performance is partly guided by situation assessment and response planning has potential implications for human reliability analyses (HRA). The results indicated that operators are engaged in a number of activities in addition to following the steps in the EOP. Moreover, the results showed that following the EOP steps was not always straightforward. In some cases determination of how to respond to a procedure step depended on situation assessment These results suggest that analyses that focus on the ability of crews to follow individual steps in the EOPs may be insufficient.

The results highlighted the importance of the dynamics of the event in determining what evidence is likely to be available at different points in the event, and what procedure transitions are likely to be made as a consequence. These results suggest that the dynamics of an event play an important role in determining human reliability. An implication is that human reliability assessments are likely to be more accurate if the dynamics of the event are explicitly considered in performing them. This can best be accomplished by running several crews through the specific events using a high fidelity dynamic simulator.

A second implication of the results is that more accurate human reliability assessments are likely to be obtained if analysts take explicit consideration of factors in the events that may complicate situation assessment or response planning. We have developed a 'cognitive demands checklist' that lists many of these factors that can be used to support human reliability assessment. Appendix D of NUREG/CR-6208 contains the 'cognitive demands checklist.'

Conclusions

While symptom-based EOPs have greatly reduced the need for operators to develop diagnostic and response strategies on their own in real time, they have not entirely eliminated the need for operators to engage in situation assessment and response planning. In our scenarios a number of cognitively demanding situations arose where operators were required to exercise judgment and take action based on their own assessment of the situation.

The types of situations we identified are generic classes that are likely to arise in other emergency scenarios. The ability of operators to form accurate situation assessments and to generate response plans that adequately address the situation were shown to be important for these situations.

The results are consistent with the view that situation assessment and response planning enable operators to handle unanticipated situations that are not fully addressed by procedures. This view has implications for the development and evaluation of training, and control room aids (e.g., procedures, displays, decision-aids); specifically it suggests that attention should be paid to the need to support and augment operator situation assessment and response planning activities.

The results also have potential implications for human reliability analyses. They suggest that analyses that focus only on the ability of crews to follow individual steps in the EOPs may be insufficient. Human reliability assessments are likely to be more accurate if the dynamics of the event, and the factors that are likely to complicate situation assessment and response planning, are explicitly considered.

The results also served to clarify conditions under which crew interaction skills may be expected to affect technical performance of crews. They revealed specific crew behaviors that may characterize good crew interaction and contribute to technical performance. Examples include splitting into subteams, having all crew members participate in situation assessment and response planning activities, ensuring that all crew members are cognizant of key plant state information and control actions that are taken, and providing periodic recaps of current situation assessment and upcoming activities. Understanding the specific behaviors that characterize team skills is important for guiding development of team skills training programs. While the present results are suggestive, more research is needed to establish a definitive link between specific crew interaction behaviors and crew technical performance.

There was more variability in BARS ratings of crew interaction skills in this study than in previous studies (Montgomery et al., 1992). One possible explanation is that the scenarios used in the present study were more cognitively demanding. A number of cognitively demanding situations arose in these scenarios where better technical performance depended on the contributions and coordination of multiple crew members. These scenarios may have placed greater demands on team interaction skills and thus provided the opportunity to observe variability in performance. This argument suggests that future studies that attempt to establish a link between team interaction skills and technical performance should employ scenarios that are specifically designed to be demanding from the perspective of team interaction. The scenarios should be designed so that technical performance depends on the contributions and coordination of multiple crew members.

A final conclusion of the study regards the value of empirical studies of operator performance in simulated emergencies for addressing human performance issues of concern to the NRC. Well

designed empirical studies can provide specific, clear conclusions for practical decision making. The present study illustrates how empirical studies of operator performance in simulated emergencies can be used to investigate a human performance issue -- in this case the role of higher-level cognitive activity in operator response to cognitively demanding emergencies. The study provided: (1) evidence that situations can arise where higher-level cognitive activity on the part of operators is needed and (2) objective data on how different operator crews responded to these situations.

References

Kauffman, J. V., G. F. Lanik, E. A. Trager, and R. A. Spence, *Operating Experience Feedback Report - Human Performance in Operating Events*, NUREG-1275, Office for Analysis and Evaluation of Operational Data, U. S. Nuclear Regulatory Commission, Washington, D. C., December, 1992.

Montgomery, J. C., C. D. Gaddy, R. C. Lewis-Clapper, S. T. Hunt, C. W. Holmes, A. J. Spurgin, J. L. Toquam, and A. Bramwell, "Team Skills Evaluation Criteria for Nuclear Power Plant Control Room Crews," working draft, 1992. (Available in NRC Public Document Room.)

Mumaw, R. J., D. Swatzler, E. M. Roth, and Wm. A. Thomas, *Cognitive Skill Training for Decision Making*. NUREG/CR-6126, U. S. Nuclear Regulatory Commission, Washington, D. C., June, 1994.

Norman, D. A. "The Problem with 'Automation': Inappropriate Feedback and Interaction, Not 'Over-Automation'," *Philosophical Transactions of the Royal Society of London*, B327, 1990.

NRC, NUREG-1154, *Loss of Main and Auxiliary Feedwater at the Davis-Besse Plant on June 9, 1985.* U. S. Nuclear Regulatory Commission, Washington, DC 200555, 1985.

NRC, NUREG-1455, *Transformer Failure and Common-Mode Loss of Instrument Power at Nine Mile Point Unit 2 on August 13, 1991*. U. S. Nuclear Regulatory Commission, Washington, DC 20555, October, 1991.

Perrow, C., *Normal Accidents. Living with High-Risk Technologies*, Basic Books, 1984.

Reason, J., *Human Error.* Cambridge, England: Cambridge University Press, 1990.

Roth, E. M., K. B. Bennett and D. D. Woods, "Human Interaction with an 'Intelligent' Machine". *International Journal of Man-Machine Studies*, 27, 479-525, 1987.

Roth, E. M., Mumaw, R. J., & Lewis, P. M. *An Empirical Investigation of Operator Performance in Cognitively Demanding Simulated Emergencies.* NUREG/CR-6208, U. S. Nuclear Regulatory Commission, Washington, D. C., 1994.

Roth, E. M., R. J. Mumaw and H. E. Pople, "Enhancing the Training of Cognitive Skills for Improved Human Reliability: Lessons Learned from the Cognitive Environment Simulation Project," in *Proceedings of the 1992 IEEE Fifth Conference on Human Factors and Power Plants,* 1992.

Suchman, L. A. *Plans and Situated Action: The Problem of Human-Machine Communication.* Cambridge: Cambridge University Press, 1987.

Swezey, R. W. and E. Salas, eds., *Teams: Their Training and Performance,* New Jersey: Ablex Publishing Corp., 1992.

Trager, Jr., E. A., *Case Study Report on Loss of Safety System Function Events.* Technical Report AEOD/C504, Office of Analysis and Evaluation of Operational Data, U. S. Nuclear Regulatory Commission, 1985.

Wagenaar, W., and J. Groeneweg, "Accidents at Sea: Multiple Causes and Impossible Consequences," *International Journal of Man-Machine Studies*, 27, 587-598, 1987.

Woods, D. D., L. J. Johannesen, R. I. Cook and N. B. Sarter, *Behind Human Error: Cognitive Systems, Computers and Hindsight,* CSERIAC State-of-the-Art Report, November, 1994.

Methods Development to Evaluate the Risk of Upgrading to DCS: The Human Factor

Lee T. Ostrom and Cheryl A. Wilhelmsen
Idaho National Engineering Laboratory
P.O. Box 1625
Idaho Falls, ID 83415-3855

Abstract

The United States Nuclear Regulatory Commission (NRC) recognizes that a more complete technical basis for understanding and regulating advanced digital technologies in commercial nuclear power plants (NPPs) is needed. A concern is that the introduction of digital safety systems may have an impact on risk. A review of available standards and literature disclosed that there is currently no standard methodology for measuring digital system reliability. A tool currently used to evaluate NPP risk in analog systems is the probabilistic risk assessment (PRA). The use of this tool to evaluate the digital system risk was considered to be a potential methodology for determining the risk. To test this hypothesis, it was decided to perform a "limited" PRA on a single dominant accident sequence. However, a review of existing human reliability analysis (HRA) methods showed that they were inadequate to analyze systems utilizing digital technology. A four step process was used to adapt existing HRA methodologies to digital environments and to develop new techniques. The HRA methods were then used to analyze an NPP that had undergone a backfit to digital technology in order to determine, as a first step, whether the methods were effective. The very small-break loss of coolant (LOCA) accident sequence was analyzed to determine whether the upgrade to the Eagle-21 process protection system (PPS) had an effect on risk. The analysis of the very small-break LOCA documented in the Sequoyah PRA (NUREG/CR-4550, 1990) was used as the basis of the analysis.

The analysis of the results of the HRA showed that the mean human error probabilities for the Eagle-21 PPS were slightly less (approximately 2%) than those for the analog system it replaced. However, this change was not statistically significant. One important observation from the analysis is that the operators have more confidence in the plant control system since the upgrade to the Eagle-21 PPS. This increased confidence stems from the better level of control provided by the digital system. The analysis of the PRA results, which included the human error component and the Eagle-21 PPS, disclosed that the reactor protection system had a higher failure rate than the analog system, although the difference was only 15% and was not statistically significant. The HRA methods adapted and developed for this project worked well for performing the analysis, however, not all facets of the methods could be tested. It is planned that two more analyses will be performed, one involving an evolutionary plant, CE80+, and one involving an advanced passive reactor design, AP600.

Work supported by the U.S. Nuclear Regulatory Commission Office of Regulatory Research, under DOE Idaho Field Office Contract DE-AC07-761D01570. Views expressed in this report are not necessarily those of the Nuclear Regulatory Commission or the Department of Energy.

1.0 Introduction

The United States Nuclear Regulatory Commission (NRC) recognizes that a more complete technical basis for understanding and regulating advanced digital technologies in commercial nuclear power plants (NPPs) is needed. The introduction of digital technology and advanced display systems may have at least the following four effects, all of which may have a direct impact upon risk:

1. The configuration of the plant will change physically
2. The allocation of functions between humans and hardware may be modified
3. There will be different failure modes and associated failure rates for hardware, software, and human actions and decisions
4. More data will be available to the control room.

A review of available standards and literature disclosed that there is currently no standard methodology for measuring digital system reliability. A tool currently used to evaluate NPP risk in analog systems is the probabilistic risk assessment (PRA). The use of this tool to evaluate the digital system risk was considered to be a potential methodology for determining the risk. To test this hypothesis, it was decided to perform a "limited" PRA on a single dominant accident sequence. However, a review of existing HRA methods showed that they were inadequate to analyze systems utilizing digital technology. Therefore, the project focus was shifted to adapting currently available HRA methods for use in analyzing digital environments.

This paper reports on the progress of this project. It is divided into two sections. The first section discusses the HRA method development process. The second section discusses how the HRA methods adapted for this project were used to analyze a plant that had undergone a backfit to digital technology.

2.0 Human Reliability Analysis Method Development

The HRA method development process was broken into four steps. They were: 1) Review or formal HRA methods, 2) Development of an HRA modeling framework for digital environments, 3) Development of human error probabilities for digital environments, and 4) Development of an HRA/PRA integration framework. These are discussed below.

2.1 Step 1: Review of Formal HRA Methods

Formal HRA quantification methods were reviewed to determine the applicability of the methods to assess human performance in digital environments and to determine whether new quantification methods were needed. A number of HRA methods were reviewed. Analysis showed that no single currently available HRA method is adequate for analyzing digital operating environments and that HRA methods needed to be adapted for analyzing systems utilizing digital technology. The currently available methods were ranked for use for analyzing digital environments based on robustness (applicability of the method to a

wide range of scenarios) of the method, ease of use, availability, validity criteria (accuracy of the method in estimating failure rates), completeness criteria (ability of the method to present failure-rate estimates under a variety of conditions), and sensitivity of the method to static versus dynamic differences in requirements for crew performance. The five quantification methods selected for use in the limited PRA were the Technique for Human Error Rate Prediction (THERP), Success Likelihood Index Method (SLIM) and Direct Numerical Estimation (DNE), Simulation, and Confusion Matrix.

2.2 Step 2: Development of an HRA Modeling Framework for Digital Environments

An HRA modeling framework was developed for use in the limited PRA. The development of this framework began with a of review of existing HRA methods. These included event tree, fault tree, influence diagrams, and simulation. Based on the identification of needs determined during this review, two methods were adapted for analyzing digital operating environments. The first was modifying HRA event trees to represent aspects of cognition. We refer to this cognitive event tree system as the COGENT system. The second, a conceptual cognitive modeling framework was developed based on the inadequacies of the methodologies reviewed. For example, existing models fail to represent intelligence allocation of human-machine, function, workload shifts, memory, crews ability to predict future system states and responses, and awareness of system feedback. The conceptual cognitive modeling framework represents plant status, and context, crew-machine interface, cognitive processes, performance shaping factors (PSFs), and potential errors. The conceptual cognitive modeling framework has six interactive modules. They are: 1) plant status during the accident sequence, 2) plant interface, 3) crew cognition, 4) PSFs, 5) representations for success and failure for decisions regarding plant status, and 6) performance modes associated with potential error mechanisms. An error taxonomy was developed to this model and is related to the cognitive factors and PSFs found in automated environments and included the following error types; misinterpretations, errors in judgment, misperceptions, over reliance on systems, and failure to anticipate future system response. Based on information collected during a literature survey and operational data collection, a new task analysis form for use in automated environments was developed. Additionally, this project identified a standardized workload measure for use in HRA--The NASA TLX (Hart, et al., 1984).

2.3 Step 3: Development of Human Error Probabilities for Digital Environments

A review of human error probability (HEP) data bases showed that there were very few HEPs for errors of commission pertaining to digital operating environments. Expert estimation sessions were held at the INEL for the purpose of determining HEP estimates for use in HRA for automated environments. Eleven subjects were surveyed by means of a written questionnaire. Six experts had a high level of operations experience and five experts had a lower level of operations experience, but were PRA analysts familiar with plant operations. The questionnaire listed 36 decision-based errors of commission roughly sorted into three bins of low, medium and high probability of error. The questionnaire had been developed based on input from a literature survey and interviews with operators of automated equipment. A median HEP was developed for each error type from the results of the sessions. The results from this determination were statistically analyzed to determine relationships among and within the two groups of experts. A statistical analysis of the results showed that group membership had a significant effect on the relative values for the three probability bins. The overall failure rates assigned were also significantly influenced

by group membership. PRA analysts were more conservative in assigning failure-rate estimates to errors of commission than were operations personnel. The failure-rate estimates obtained ranged on the order of E-2 to E-3.

2.4 Step 4: Development of an HRA/PRA Integration Framework

An PRA/HRA integration framework was developed that ensures that an integrated approach to assessing NPP risk in advanced digital environments is followed. This method provides a process for HRA in automated environments that incorporates the models and methods developed in this report. The process developed is based on the Electric Power Research Institute's (EPRI) systematic human action reliability procedure (SHARP) (Hannaman and Spurgin, 1984). Proposed improvements to the SHARP procedure are described in EPRI NP-6937 (Spurgin, et al., 1990). The INEL incorporated those proposed improvements along with others to develop the EPRI/INEL hybrid procedure which consists of ten steps. They are:

1. Select and train the PRA/HRA team.
2. Construct the initial plant model of systems.
3. Define key human actions.
4. Screen human actions.
5. Perform qualitative analysis.
6. Represent human actions and decisions in event tree structures.
7. Perform integration and determine effect of human actions on systems and core melt frequency.
8. Perform quantification via HRA methods.
9. Review results for completeness.
10. Document models, methods, and assumptions.

The steps the INEL added to the process are 1, 2, and 9. These steps were added based on the suggested improvements contained in EPRI NP-6937 and from the experiences of INEL PRA/HRA analysts. Step 1, Select and Train the PRA/HRA Team, concerns ensuring team members are trained on the system they will be analyzing. Step 2, Construct Initial Plant Models of Key Systems, concerns developing a model of the system that shows all the interconnections, including hardware and software by reviewing all pertinent documentation including procedures. Step 9, Review Results for Completeness, pertains to ensuring the analysis is auditable, traceable, and credible.

2.5 Summary of HRA Method Adaptation

The need for HRA methods for analyzing systems utilizing digital technology was apparent from the review of existing methods. A four step process was used to adapt currently available methods for this project. The methods developed included a method for deciding which HRA method to use given information about a task, a cognitive model framework, a method for integrating cognitive actions into HRA event trees (COGENT), a task analysis data collection form for use in digital environments, an initial set of HEPs pertaining to decision making in digital environments, and a PRA integration framework based on the EPRI SHARP process. The testing of the methods will be discussed in Section 3.0 of this paper.

3.0 HRA Methods Testing

The HRA methods which were developed, as discussed in Section 2, are to be tested. There are currently three classifications of automation being used or planned for NPPs. The first is called a backfit case in which the NPP upgrades a safety grade control system from analog to digital. The second type is an evolutionary case like the CE 80+ design. The third is an advanced digital instrumentation and control case like a passive reactor design that is primarily digital technology. The HRA methods are to be tested under all three levels of automation to ensure the methods work for all types of automated environments. At the present time, testing of the methods has been successfully accomplished for the backfit case.

3.1 Introduction to the Backfit Case Analysis

The INEL identified a candidate plant (Sequoyah NPP) and an accident sequence (very small-break loss of coolant accident [LOCA]) for the analysis.

The HRA/PRA analysis to test the methods was a pre- and post-Eagle-21 upgrade comparison to determine if the HRA methods were usable and how well they worked for analyzing the sequence in the advanced digital operating environment. The Sequoyah NPP was selected primarily because: 1) it had replaced its existing analog control system with the Westinghouse Eagle-21 PPS (Eagle-21), 2) it had several years experience with the digital control system (DCS), 3) Sequoyah plant management demonstrated a willingness to support the project, and 4) Sequoyah has an existing, well-documented PRA.

The very small-break LOCA sequence was selected because it accounted for approximately 25% of the risk of CDF at the NPP (NUREG/CR-4550, 1990) and the sequence involved several critical human actions.

3.2 HRA Techniques

The accident sequence, discussed above, was analyzed using the HRA techniques described in Section 2.0 of this paper. The NUREG/CR-4450 PRA was used as the basis of the analysis. This PRA was not sufficiently detailed regarding the modeling of the reactor protection system (RPS) for the current work. Also, the control room design had changed and the emergency operating procedures were updated during the same time frame the Eagle-21 was implemented. Therefore, to ensure a balanced analysis, the original analog system was analyzed using the more detailed EPRI/INEL HRA/PRA modeling

techniques to provide a true basis for comparison. Also, this was done so that the same analysis team performed both the pre- and post-analyses to ensure there was no difference in analysis techniques.

The NPP was visited in October, 1993, and May, 1994. Interviews were conducted with operators and technical staff and formed the basis of the task analysis. The NPP's emergency operating and supporting procedures and other plant documentation augmented the task analysis. The interviews with each operator pertained to how the plant was operated both for the analog and digital control systems. The HRA event trees developed for the current analyses were much more detailed than the original analysis contained in the NUREG/CR-4550. These trees were developed to correspond with the original events in NUREG/CR-4550. This was done so that the human error probabilities (HEPs) quantified from the trees could be imported directly into the Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 5.0 analysis program (NUREG/CR-6116, 1993) in order to quantify the overall change in risk. The trees were quantified using the Technique for Human Error Rate Prediction (THERP) (Swain and Guttman, 1983) and the Accident Sequence Evaluation Program (ASEP) (Swain, 1987) methodologies. This was possible because, in general, the operators were using the same controls and displays after the upgrade as before. However, the pre- and post-Eagle-21 PPS upgrade analysis took into account other changes in the NPP operating environment that occurred since the analysis was originally reported in NUREG/CR-4550.

3.3 Results of the HRA

A comparison was made between the pre- and post-Eagle-21 PPS upgrade HRAs. This comparison was made by comparing the HEPs for the original NUREG/CR-4550 analysis for the very small-break LOCA sequence with the HEPs calculated for the current analysis. This comparison showed that the HEPs calculated for the current work pre-Eagle-21 PPS were significantly higher than the original NUREG/CR-4550 HEPs. The increase in HEP values is due to: 1) the modeling of both errors of omission and errors of commission in the current analysis (this was not done in the original analysis), 2) the level of detail of the human actions is much greater (in the original HRA the tasks were not decomposed to the sub-task level and several key human actions were not considered), and 3) the current analysis only credited up to two independent verifications of key human actions (in the original analysis up to three independent verifications were credited).

A comparison was also made of the pre- and post-Eagle-21 PPS upgrade HEPs. The pre- and post-Eagle-21 PPS analyses showed very little difference between the HEPs primarily because the layout of the control room, the human actions the operators performed, and the EOPs did not change with the upgrade. However, during interviews, the operators expressed that they had much more confidence in the plant since it had been upgraded. Therefore, the level of stress was reduced for those human actions involving cognitive processes (rule-based mistakes). This was done because the operators having more confidence in the plant would be more sure the plant was going to behave in a predictable way and, therefore, less stressed. The decrease in the HEPs for the post-Eagle-21 PPS analysis was approximately 2% improvement for some of the HEPs over the pre-Eagle-21 PPS analyses; others did not change.

3.4 Hardware PRA Process

The PRA process utilized techniques described in Galyean (1994). (Note that the PRA process is not presented in detail in this paper since the focus is on the HRA.) For the

current work, the PRA analysts decomposed the control system to the component level to quantify the failure probabilities of the system. This was done both for the pre- and post-Eagle-21 PPS upgrades. The failure rate data used for the analysis was obtained from existing data, using published sources and modified with Sequoyah's experience with the Eagle-21 PPS using a Bayesian update process. The failure rate for the Eagle-21 software was calculated to be 1E-4/demand. This failure rate was estimated based on expert opinions in published literature (Galyean, 1994).

3.5 Results of the PRA Process

The fault tree analysis provided several insights concerning the upgrading from an analog system to a Eagle-21 PPS. The first and foremost is that upgrading to the Eagle-21 PPS does not significantly affect Sequoyah's CDF for the sequence analyzed. The CDF for the analog system for the very small-break LOCA sequence is 1.965E-4. The CDF for the Eagle-21 PPS for the very small-break LOCA sequence is 1.937E-4. The change is less than 2% improvement for the Eagle-21 PPS, however this is not statistically significant due to the level of uncertainty in the analysis. As a rule of thumb, the difference in CDF would have to at least be an order of magnitude before there would be a statistical significant difference.

3.6 Change in Risk due to the Upgrade to the Eagle-21 PPS

The comparison of the failure probabilities of the analog system to Eagle-21 PPS (which includes the human component, hardware and software) for the current analysis showed that there is very little difference. The Eagle-21 PPS had a slightly higher failure rate (< 15%), but this was not statistically significant due to the level of uncertainty in the analysis. As a rule of thumb, the difference in CDF would have to at least be an order of magnitude before there would be a statistical significant difference. The failure probability for the Eagle-21 PPS was calculated to be 1.52 E-4. The failure probability for the analog system is 1.32E-4. Therefore, the contribution to CDF did not change with the implementation of a Eagle-21 PPS at the Sequoyah NPP *for the sequences analyzed.* The only Eagle-21 failure that showed up in the first five dominant cut sets for the Eagle-21 PPS was the failure of the Eagle-21 software. However, the estimated failure rate is likely conservative. More detailed analysis of the Eagle-21 software is needed to refine this estimate.

4.0 Effectiveness of the HRA Methods

This section summarizes the effectiveness of those techniques for use in analyzing the very small-break LOCA sequence at the Sequoyah NPP, considering the Eagle-21 PPS. The effectiveness of the modeling techniques will be discussed by either qualitative or quantitative analysis.

4.1 Qualitative Analysis

The qualitative analysis procedures used in analyzing systems utilizing digital technology were: 1) the task analysis data collection process for automated environments, 2) the COGENT event tree system, and, to a lesser degree, and 3) the cognitive modeling framework.

The task analysis data collection process for automated environments was utilized to a great degree for this analysis. The process proved useful for aiding in collecting all the information necessary to perform the analysis. However, the data collection form was too long for this type of data collection effort. During the analysis it was found that only certain sections were necessary. In other analyses, however, the whole form might be needed.

The COGENT event tree system proved very effective for aiding in the development of event trees. It aided by helping to that reflect the nature of the types of errors operators could possibly commit. This information was utilized in the quantification of the HEPs for the human action by providing the analysts with information as to whether the possible error was a slip, lapse, or mistake and whether it was rule- or knowledge-based.

The cognitive modeling framework was used in aiding the analysts in deciding which were the important PSFs to be considered in the analysis.

Certain techniques were not utilized. For example, influence diagrams were not used because the control room had not changed and it was determined from the task analysis what the influences on the operators were.

4.2 Quantitative Analysis

The HRA quantification method selection process was not exercised to its fullest for this analysis because the human actions being quantified were essentially the same for both the analog and digital RPS. Also, only traditional PSFs were considered in this analysis because the design of the control room had not changed due to the upgrade to the Eagle-21 PPS. Therefore, THERP was the most useful quantification method. In a few cases when THERP could not be used to quantify human actions, ASEP was used. These cases involved human actions that were not well defined and, therefore, a screening level HEP appeared to be the more useful quantification method.

5.0 Conclusions

There are a number of benefits which can be realized utilizing the methodology discussed in this paper. The HRA method used to perform this analysis is much more detailed than is currently used in most PRAs/HRAs. This methodology provides a greater benefit to vendors and regulators. Vendors could use this detailed analysis method to determine what human actions are required by the operators to mitigate a certain transient based on available information concerning the reactor design. Upon completion of the initial analysis, the reactor designers would have a greater ability to modify the design to reduce the number of critical human actions and/or provide means to reduce the likelihood of errors, thus reducing the risk of CDF. Regulators could use this methodology as a bench mark to compare vendor submittals. The limitation of this method is the level of detail of task analysis data needed to perform the analysis. It is much greater than needed for most HRAs.

Using COGENT to classify the human errors provided insights into the types of errors the operators could make. Also, it provided insights on the influences of the various PSFs on the probability of the operator committing an error. The output of this classification was used in the quantification of the human actions.

The original NUREG/CR-4550 modeled the human actions required to perform the tasks at a very high level (little detail). Because of the type of task analysis performed there was a much greater ability to decompose the tasks to a much lower level (more detail). Doing so provided more and better information concerning what is required of the operator to perform a task, helped determine the important PSFs for the task, and helped quantify the human actions. The cost of doing this is higher, however. It is estimated that it required twice the amount of resources to perform this analysis than to perform a traditional HRA. The methods used to perform the analysis and the added cost have great benefit for critical applications of digital technology. Therefore, in cases where the risk is much higher than desired, application of these methods can result in identifying the major contributers to the risk.

It is important to note that not all the facets of the methods developed were tested in the course of this analysis because, for example, the Sequoyah control room lacked the implementation of video display terminals. Therefore, general conclusions concerning the methodology cannot be made. These other facets will be tested during the two other test cases, the evolutionary NPP and the design of an advanced passive reactor.

6.0 References

Bertucio, R.C., and Brown, S.R., *Analysis of Core Damage Frequency: Sequoyah, Unit 1 Internal Events*, NUREG/CR-4550, US Nuclear Regulatory Commission, Washington, DC, 1990.

Hannaman, G.W., and Spurgin, A.J., Systematic Human Action Reliability Procedure, (SHARP), Electric Power Research Institute Report NP-3583, 1984.

Hart, S.C., et al., "The Impact of Response Selection and Response Execution Difficulty on the Subjective Experience of Workload," *Proceedings of the Human Factors Society*, pp. 732-736, 1984.

Nuclear Regulatory Commission, *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 5.0,* NUREG-6116 Vol. 2, December 1993.

Russel, K.D., et al., *Integrated Reliability and Risk Analysis System (IRRAS)*, Ver. 4.0, NUREG/CR-5813, U.S. Nuclear Regulatory Commission, Washington, D.C., 1992.

Spurgin, A.J., et al., Operator Reliability Experiements Using Power Plant Simulators, 2, Technical Report, Electric Power Research Institute Report EPRI-NP-6937-V2, 1990.

Swain, A.D. and H. Guttmann, *Handbook for Human Reliability Analysis with Emphasis on Nuclear Power Plant Operations: Technique for Human Error Rate Prediction*, NUREG/CR-1278, US Nuclear Regulatory Commission, Washington, D.C., 1983

Swain, A.D. *Accident Sequence Evaluation Program Procedure (ASEP)*, NUREG/CR-4772, US Nuclear Regulator Commission, Washington, DC, 1987.

OPERATOR-BASED METRIC FOR NUCLEAR OPERATIONS AUTOMATION ASSESSMENT

Greg L. Zacharias, Adam X. Miao, and Ayse Kalkan
Charles River Analytics Inc.
Cambridge, MA

Shih-Ping Kao
Simulation Expert Systems, Inc.
New Haven, CT

Abstract

Continuing advances in real-time computational capabilities will support enhanced levels of smart automation and AI-based decision-aiding systems in the nuclear power plant (NPP) control room of the future. To support development of these aids, we describe in this paper a research tool, and more specifically, a quantitative metric, to assess the impact of proposed automation/aiding concepts in a manner that can account for a number of interlinked factors in the control room environment. In particular, we describe a cognitive operator/plant model that serves as a framework for integrating the operator's information-processing capabilities with his procedural knowledge, to provide insight as to how situations are assessed by the operator, decisions made, procedures executed, and communications conducted. Our focus is on the situation assessment (SA) behavior of the operator, the development of a quantitative metric reflecting overall operator awareness, and the use of this metric in evaluating automation/aiding options. We describe here the results of a model-based simulation of a selected emergency scenario, and metric-based evaluation of a range of contemplated NPP control room automation/aiding options. The results demonstrate the feasibility of model-based analysis of contemplated control room enhancements, and highlight the need for empirical validation.

1. Introduction

Decision-making in nuclear plant operations is often characterized by **time pressure, dynamically evolving situations,** and **high expertise levels** on the part of the operators. Contemplated automation and decision aids proposed for plant operations often fail to recognize these critical aspects of the problem, having been designed under assumptions that are better suited for *novice* decision makers working under *low time pressure* in relatively *static* scenarios. In particular, current decision aids often view the decision-maker as "faced with alternatives, and considering the consequences of each alternative in terms of analysis for future states (odds/probabilities) weighted against alternative goals (preferences/utilities)" (Klein (1989a)). In short, these decision aids have concentrated on helping the decision-maker *generate* options, *propagate* their various consequences, and *evaluate* the relative merits of a given option. They attempt to overcome the limitations and biases that the human decision-maker shows in generating, propagating, and evaluating the decision options (Klein, Orsanu, Calderwood, et al. (1993)).

Considerable evidence, however, suggests that this classical decision-aid design philosophy may need re-examining. Klein (1989a) and his associates report on the decision-making behavior of experts under high time pressure (Klein, Calderwood and Clinton-Cirocco (1986); Klein, Calderwood and Macgregor (1989); and Klein (1989b)). Their findings are that *expert* decision-makers do not generate or evaluate options, but only *assess the situation.* Once the situation is assessed, the reaction strategy and resulting decision is almost automatic. McDonnell Aircraft Company reports similar findings, in which Tactical Air Command (TAC) line fighter pilots flew

in very realistic *man-in-the-loop* simulations. Situation awareness was identified as the single most important factor in mission success. The study concluded that "success is tied to good situation assessment, and generally speaking the better the situation assessment the better the outcome" (Stiffler (1987)). This point of view on human decsion-making has been formalized by Klein (1989a) as the Recognition-Primed Decision (RPD) model to distinguish it from the classical option-selection model. Situation Assessment (SA) centered decision making behavior has also been assumed by Baron, Zacharias, Muralidharan, et al. (1980) to model time-pressured commercial aircraft landings; by Zacharias, Miao and Riley (1992) to understand fighter pilot tactical awareness; and by Zacharias and Miao (1994) to relate situation awareness to information flow in the commercial aircraft cockpit.

Our general approach to modeling the NPP operator's situation assessment and decision-making behavior has its roots in the RPD approach and in several generations of systems-theoretic and cognitive-operator models. A recent review of NPP operator models by Dang and Siu (1994) contrasts three models: the Cognitive Environment Simulation or CES, developed at Westinghouse (Roth, Woods and Pople (1992); Woods, Roth and Pople (1989)); the Cognitive Simulation Model or COSIMO currently under development by Cacciabue, Decortis, Drozdowicz, et al. (1992); and the CREWSIM model, currently under development at MIT by Huang, Dang and Siu (1993). All three are simulation-based models, but, as described by Dang and Siu (1994), are different in scope, as shown in table 1-1. Note that CES represents the integrated crew/machine system (including decision aids), COSIMO represents the individual operator, and CREWSIM the multiple individuals as members of the operating crew. Note also the different levels of representation of the different cognitive processes, from monitoring and situation assessment, to procedure execution and communication.

Cognitive Process	CES	COSIMO	CREWSIM
Representation:	Crew	Individual	Y
Monitoring	Y	Y	Y
Situation Assessment	Y	Y	Y
Decision-Making	Y (planning)	Y	Y
Procedure Executor		Y	Y
Communication			Y

Table 1-1: Scope of Three NPP Operator/System Models (adapted from Dang and Siu (1994))

On the basis of this work it is clear that to support the development of an automation/aid assessment metric, an integrated operator/system model must account for the operator, any automation systems, the NPP, and the environment. It should support the systematic exploration of issues revolving around automation, information transfer, procedure definition, and operator performance. These requirements, in conjunction with continuing efforts focusing on operator/system modeling of complex dynamic systems, lead us to propose a general system architecture for automation system assessment based on the Crew/System Integration Model, or CSIM. CSIM is an interactive framework that represents the plant characteristics, the automation/aiding parameters, and the operator's information processing capabilities. It allows us to combine and integrate the system-related and operator-related components of the system and task that drive overall operator awareness and performance. The model architecture integrates the operator's basic functions of: 1) information processing (IP) of the man-machine interface displays to generate estimated system states and event cues; 2) situation assessment (SA) using event cues

to drive procedure selection; and 3) procedure selection and execution (PE) based on the assessed situation and estimated system states to select among alternative procedures and to effect motor commands and communication. The model has been used recently in an air-superiority tactical SA modeling effort (Zacharias, et al. (1992)); and has been proposed for use in flight deck automation assessment (Zacharias and Miao (1994)).In addition Van DeGraaf (1988) and Visser (1988) have conducted extensive model validation efforts, with inflight performance and workload measures.

CSIM provides a natural framework for modeling the NPP operator's SA functions and for supporting the development of an SA-based metric for assessment of automation/aiding options. Key to this approach is the development of an SA model that represents the structural and temporal SA relations/constraints, reflects the incremental evidence-accumulation of the SA reasoning process, and demonstrates *why* a situation is assessed, *how* it is assessed, and *what* evidence is used for assessment.

An approach that satisfies all these requirements makes use of **belief network (BN)** modeling of the SA process (Pearl (1986); Zacharias and Miao (1994)). A BN representation of the operator's SA behavior centers on human diagnostic reasoning under uncertainty, namely, the process by which humans integrate evidence from multiple sources and generate a coherent interpretation of the evidence via an internal source-evidence model. Simply speaking, BNs (also called Bayesian networks, inference nets, causal nets) are a unified probabilistic reasoning framework that provides a consistent and coherent solution to problems of diagnostic reasoning under uncertainty. A BN consists of a set of nodes, which represent deterministic or random variables (propositions), connected by directed links, which represent dependent or associative relationship between nodes. After receiving evidential information on affected nodes, BNs propagate and fuse the information in such a way that, when equilibrium is reached, each variable is assigned a belief measure consistent with the axioms of probability theory.

BNs give us the capability and flexibility to model human SA in its full richness (or simplicity as the case might be), without arbitrary restrictions. They provide several advantages over other approaches for modeling SA. First, BNs provide a comprehensive picture of the SA problem by indicating the dependent relationships among the situations to be assessed and the event cues to be detected. Second, belief updating by a Bayesian reasoning logic reflects the continuity in time of SA: it is an evidence accumulation process where the new evidence of the event cues is combined with the old evidence of the network node belief values. Third, Bayesian reasoning logic is mathematically sound and provides a consistent and coherent automatic reasoning process for the given evidence. It is a normative reasoning process that prescribes what a human *should* do, given situation-event relationship and evidence cues. Moreover, the belief updating process provides a clear view of how each new piece of evidence (event cue) affects situation assessment. Fourth, BNs allow the consideration of evidence at any level of abstraction and from any sources. Finally, the computation algorithm is simple and easy to implement in the case of singly connected networks.

An SA model-based evaluation of candidate automation/aiding design options also requires the development of a metric. We define this metric by computing the difference between the actual situation and the perceived (multi-dimensional) situation assessed by the operator model. An appropriately defined scalar of this situation disparity (SD) is then used as a measure of the operator's SA. In conjunction with the SA model, the awareness metric thus provides a direct means for evaluating different automation concepts in terms of their support for maintaining a high level of operator SA.

This paper presents a summary of our work in developing a model-based SA metric for assessing automation/aiding in the NPP control room. Section 2 briefly describes the plant/operator model that serves as the overall integrating framework for analysis. Section 3 presents a generic SA model based upon the BN approach, develops a specific SA model of a selected NPP

emergency scenario, and defines a model-based SA metric. Section 4 describes the results of our model-based simulation of the selected scenario, and our model-based analysis of a range of contemplated NPP automation/aiding options. Section 5 presents conclusions to be drawn from the results, and recommendations for further development.

2. Operator/System Model

We developed our general system architecture for plant/operator representation using the Crew/System Integration Model, or CSIM, illustrated in figure 2-1 below. In block diagram fashion, we show specific information processing functions, and information flow between those functions. Three major components are shown: the **system** itself, the display and control portion of the **human-machine interface (HMI)**, and the **operator**.

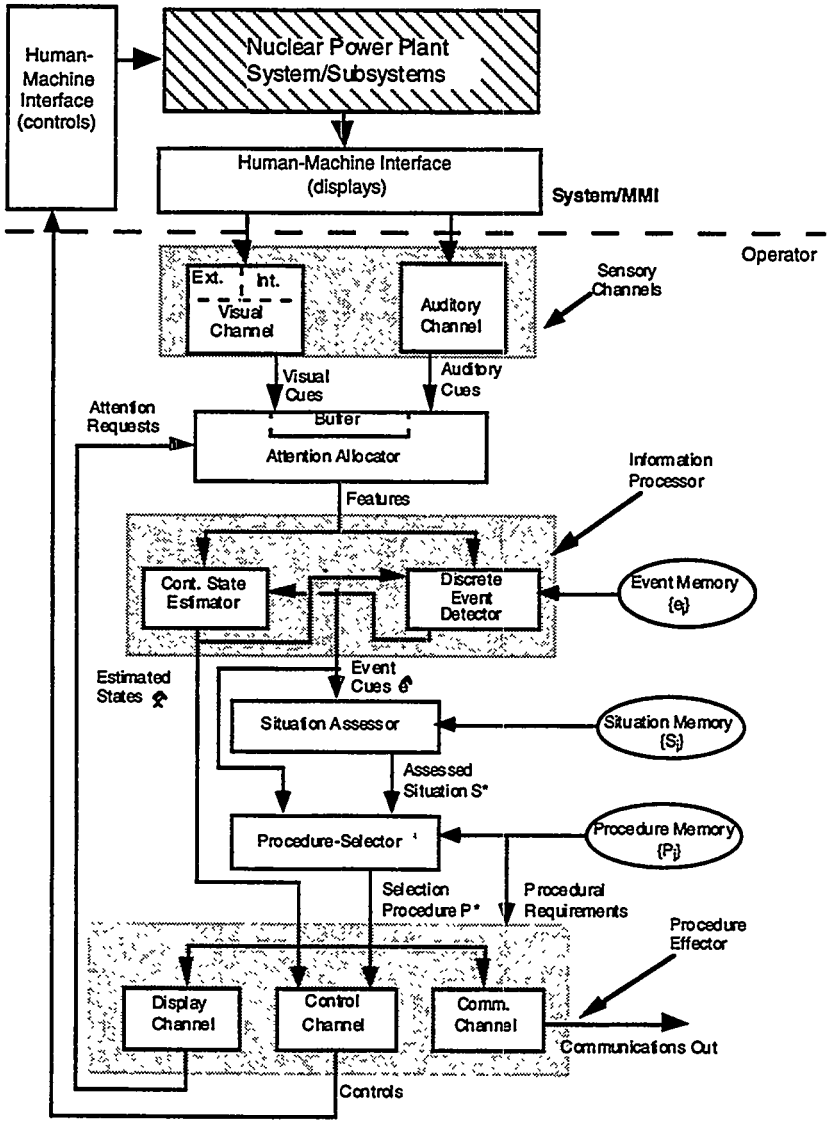


Figure 2-1: System Architecture for CSIM

The **NPP system** is modeled using the Pressurized Reactor Interactive Simulation Model (PRISM) (Kao (1991)), which simulates the dynamic behavior of the Pressurized Water Reactor

(PWR). The plant design is that of a standard Westinghouse 1200 MWe, 4-loop PWR. The PRISM system model consists of several dynamic modules written in Microsoft FORTRAN. The Nuclear Steam Supply System (NSSS) module, illustrated in figure 2-2, simulates the thermal-hydraulic behavior of the system. The neutronic module calculates the reactor power. The control module includes models for most of the plant controllers required to operate a PWR. The reactor protection module checks the plant conditions against the protection setpoint for setting alarms and automatically shutting down the reactor. The validation of the PRISM model has been verified via comparison with plant data as given in Kao (1988) and Kao (1991).

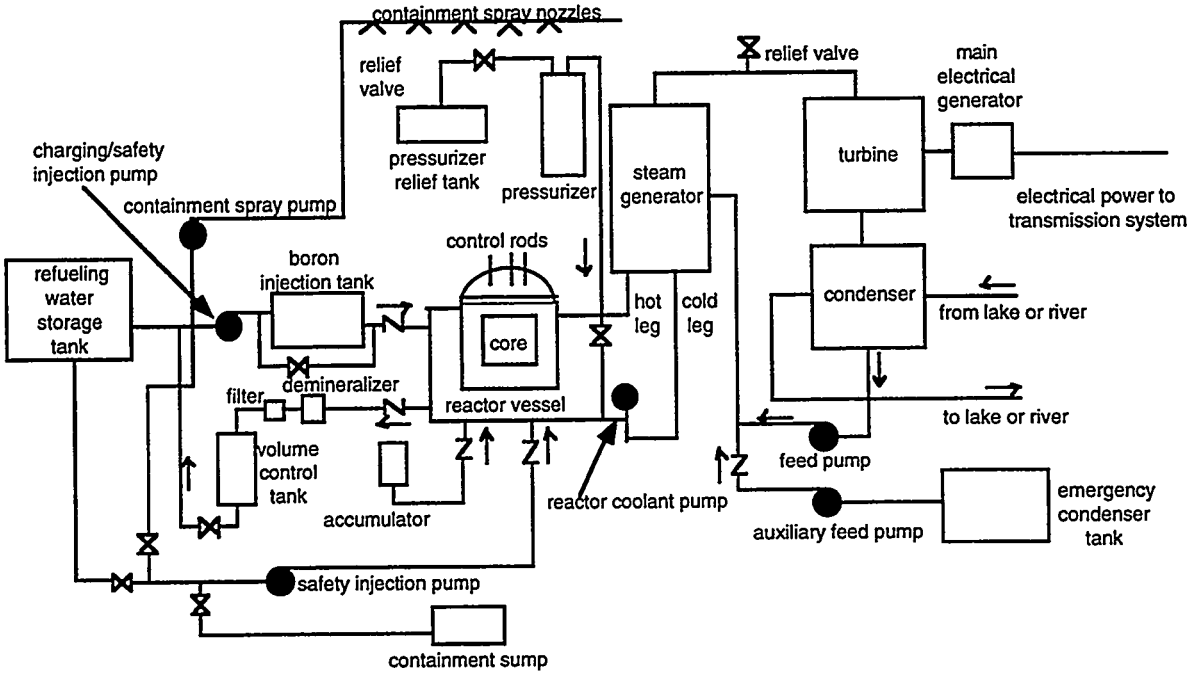


Figure 2-2: Model of Nuclear Steam Supply System

The **human-machine interface (HMI) model** defines the interface between the plant and operator. Since it is difficult to model the displays from a purely representational aspect, we model the displays from an information content aspect. For example, for modeling plant state displays, we use the plant states generated from PRISM to represent the display information content. Different displays are regarded as different quality *blackboards*, where the information content of each is perceived with different uncertainties. Specifically, the ith display is specified by a display set $\{x_i, \sigma_i\}$, where x_i represents one element of the information content displayed on the blackboard, and σ_i represents the uncertainty level at which the information can be perceived. In our display model, σ_i is denoted as the covariance of the error in the information x_i. At any given time, if no information is available for an element in the display set, the corresponding covariance σ_i is set to infinity to indicate total uncertainty for that element (Levison, Baron and Kleinman (1969)).

The **operator model** simulates the NPP operator's information processing, situation assessment, decision-making, and communication behaviors. The diagram indicates via the dashed line a fairly clean interface between the HMI and the operator's **sensory/motor channels.** On the sensory side we provide for two modalities: a visual channel driven primarily by fully-programmable CRT displays; an auditory channel which can be driven by conventional alarm or alerting signals, verbal communications, or even unconventional auditory localization signals, such

as one might find in a *virtual world* control configuration. The **attention allocator** submodel accounts for the operator's sensory limitations and for the attention allocation among competing sources of information. An *observation noise* and a *threshold* can be associated with each observed visual quantity to account for limitations imposed by resolution and attention limitations. Attention allocation reflects the fact that there is a fundamental choice as to where to fixate, both in scope across a *multi-window display*, and in depth within a *menued display*. The **information processor** submodel consists of two submodels, a **continuous state estimator** and a **discrete event detector**. The **estimator** is identical to that used in the optimal control model (Kleinman and Baron (1971): a time-varying Kalman filter designed to generate optimal estimates of the current reactor state. The outputs of the estimator are the estimates of the system state, **x**, and the covariance of the estimation error, Σ. In the NPP scenario, these states would include all those nominally displayed or available in the control room, as well as significant subsystem states that might influence operator situation assessment and procedure execution. The **discrete event detector** generates occurrence probabilities of operationally-relevant event cues, as perceived by the operator on the basis of his dynamically-changing information base. The event cue may be an annuciated alarm (that did or did not result in a detected alarm by the operator), a request for action (say, from another operator), an operations-related milestone (say, during power down), or some other annuciated condition (e.g., turbine ramp down started). The **situation assessor (SA)** block takes in the event cues **e**, and generates an assessed situation **S** which is a multi-dimensional vector defining the occurrence probabilities of the possible situations facing the operator. For model tractability, we assume a fixed and pre-defined set of candidate situations, determined solely by their task relevance. The situation assessor is the key to SA centered decision-making behavior and will be presented in detail in section 3. The **procedure selector** block takes in the assessed situation state **S**, and generates a selected procedure **P**, defined in the procedure memory shown. It is important to note that the term procedure can apply to tasks in general; a procedure in these terms can have considerably more cognitive content than might normally be considered. The selection and execution of a procedure will result in an action or a sequence of actions. Three types of actions are considered: **control actions**, **attention requests**, and **communications**. The control actions can include continuous control inputs to the system and its subsystems, as well as discrete or mode control settings. Attention requests result from procedural requirements for specific information and, therefore, raise the attention allocated to the particular information source; they are basically internal to the operator. Communications are verbal requests or responses as demanded by a procedure, and are modeled directly as the transfer of either state, command, or event information to an extrinsic node. Further details on the individual modules can be found in Zacharias and Miao (1994).

This model was specialized for a selected nominal scenario and a range of contemplated NPP control room automation/aiding options. The implementation integrates a high-fidelity FORTRAN-based simulation model of a four-loop PWR, a C++ language executive model of the operator, and a C++ implementation of the critical SA submodel. This overall implementation provides a natural hybrid architecture for future expansion in automation/aiding options, operator activities, and simulation fidelity.

To illustrate information and action flow of the model in the NPP control room context, consider the sequence of activities depicted in figure 2-3, which outlines the basic information flow during initial diagnosis of a serious plant anomaly (a steam generator tube rupture or SGTR). Here, we show in the operator's display space two sets of relevant system displays: alarm displays which are, by definition, attention getting, and status displays, which call for explicit or implicit attention-sharing strategies on the part of the operator. Both types of displays are transformed into a task-relevant feature or event space. Some of these events (shown here, the "alarm on" feature) are used by the operator to progressively resolve and eventually define the operating status in the situation space. Here, we have illustrated a network representation, with an initial detection of an

emergency situation, but with no follow-on identification of the emergency particulars. The emergency situation selected in the situation space then calls for the selection and execution of one or more procedures in the procedure space. Here, the procedure space shows the selection of the baseline emergency procedure (denoted EP-0) which is called up to begin the diagnostic task of identifying the plant anomaly. Note the if/then rule-based structure, which, through the action space, generates attention requests to the display space, as well as control actions for plant system intervention.

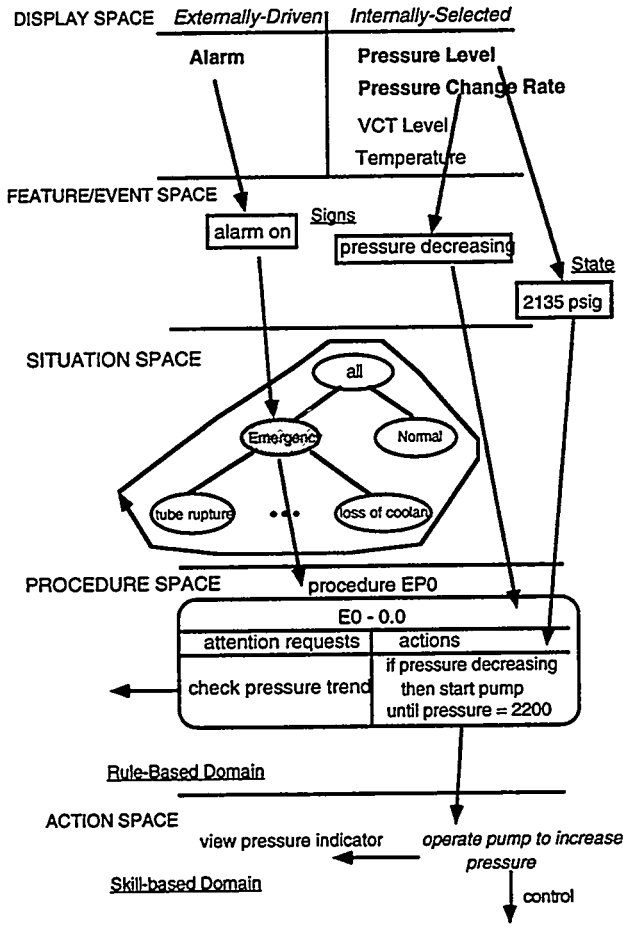


Figure 2-3: Operator Model Information and Action Flow Diagram

3. Situation Assessment Model and Metric for NPP Operations

We now present a generic situation assessment (SA) model, specialize this model to the NPP control room environment, and define a corresponding model-based metric for automation/aiding system evaluation.

Figure 3-1 shows a BN representation of the generic SA problem. In the figure, a round node represents a situation; a square node represents an event that can take on a set of mutually exclusive and exhaustive discrete values, and a round-corner square node (dummy node) represents an event cue, or a piece of *evidence* of the event, in the terminology of the BNs. The shadow on one of event cue node indicates that it is an active cue node. Non-shadowed cue nodes are inactive. Finally, an arrow, pointing toward an affected node, indicates either an associative or an inferential dependency between nodes.

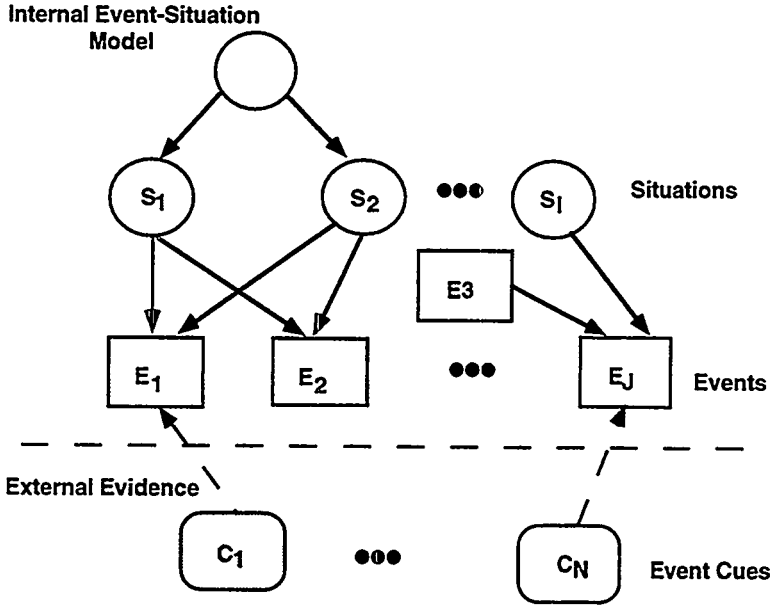


Figure 3-1: Belief Network for Situation Assessment

Each situation node S(t) is quantified with a belief measure Bel(S), indicating the belief on the situation assessment based on all the event cues so far received $\{C_i(\tau), \tau \leq t\}$, where t is the current time. For computational and explanatory reasons, we also keep an equivalent vector representation of the belief:

$$\text{Bel}(S) = (\text{Prob}(S), \text{Prob}(\neg S))^T \tag{3.1}$$

where $\text{Prob}(S) + \text{Prob}(\neg S) = 1$ and T denotes transpose. An event node of J values is similarly quantified via a column belief vector:

$$\text{Bel}(E) = [\text{Prob}(E = e_1), \text{Prob}(E = e_2), \cdots, \text{Prob}(E = e_J)]^T \tag{3.2}$$

An active event cue node, however, will not be quantified by its belief value, but by a likelihood measure indicating the relative degree that the event is believed to take on each value:

$$L(C) = [L(C = c_1), L(C = c_2), \cdots, L(C = c_J)]^T \tag{3.3}$$

Note that the likelihood values need not sum up to unity, thus permitting the likelihood of an event taking on a specified value to be formed independently of any other likelihood. In other words, the BN model allows for inconsistency in evidence gathering.

The relationship among situations is modeled via associative tree links. Specifically, when the situations in a set are mutually exclusive, this is represented by a one-level tree connecting all the situations; while lack of the tree association indicates a set of inclusive situations, as shown in figure 3-2.

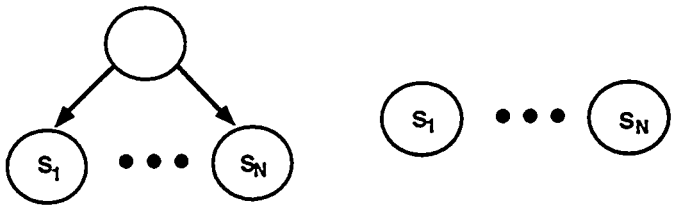


Figure 3-2: Exclusive and Inclusive Situations

The relationships between situations and events are defined by arrow links pointing from situation nodes to event nodes. Each link represents an inferential dependency between a situation and an event, quantified by a conditional probability matrix, M_{ES}. Specifically, let E denote an event that has I (i = 1, 2, ... I) values. Each arrow link is then associated with a 2 by I conditional probability matrix, where the ith element of the first row M_{1i} represents an if-then rule of the type

If the situation is S, then event E_i is expected to occur with a probability M_{1i}

The second row of the matrix represents if-then rules for the case of S being not true. Similarly, an arrow pointing from an event node of I values to another event node of J values represents an inferential dependency between two event nodes, and is associated with an I by J conditional probability matrix **P**, where element P_{ij} of **P** represents the if-then rule:

If the event is E_i, then event E_j is expected to occur with a probability P_{ij}

A dotted arrow link (dummy link) between an event cue node and an event node represents an instantiation of the affected event node by the evidence from the event cue. There is no conditional probability matrix associated with the dummy link, and the link carries information in only one direction, from the event cue (evidence) to the event node affected by it. Once the BN representation of an SA problem is completed, we can then use Pearl's algorithm (Pearl (1986)) to update the BNs at each point in time to generate a belief update of the situation, given the event cues so far detected.

BNs thus model SA as an inferential diagnostic process, in which situations are considered as causes, events as effects, and event cues as symptoms (detected effects). SA starts with detection of symptoms (event cues), from which the actual effects (events) are deduced (via inferential reasoning) and their likelihood (belief) impacts on the situations are evaluated by backward tracing the situation-event relation (diagnostic reasoning) using Bayesian logic. The evaluated situation likelihood then drives belief propagation and updating of a set of hierarchically structured situations, again using Bayesian logic. Based on the updated situation beliefs, projection of future events is achieved to guide the perception of future event cues (via anticipation). When a unique situation is to be assessed, a threshold assessor is used to select a situation (or several situations when inclusive situations are considered) with a belief greater than a preset threshold to assess it as the current situation.

For this study, we developed a two-level SA model specialized for a limited NPP operations scenario. First, a high level SA problem, illustrated in figure 3-3, assesses whether the plant is operating normally, abnormally but in a non-emergency mode, or abnormally and in an emergency mode. If the plant is operating in an emergency abnormal situation, the low level SA problem, illustrated in figure 3-4, then assesses four possible emergency abnormal situations: SGTR (Steam Generator Tube Rupture), LOCA (Loss Of Coolant Accident), Loss of Secondary Coolant (LOSC), and Other emergency abnormal situations (to account for other situations not dealt with in this study). For clarity, the illustrations in figures 3-3 and 3-4 contain fewer events and event cues than are present in the actual SA problem.

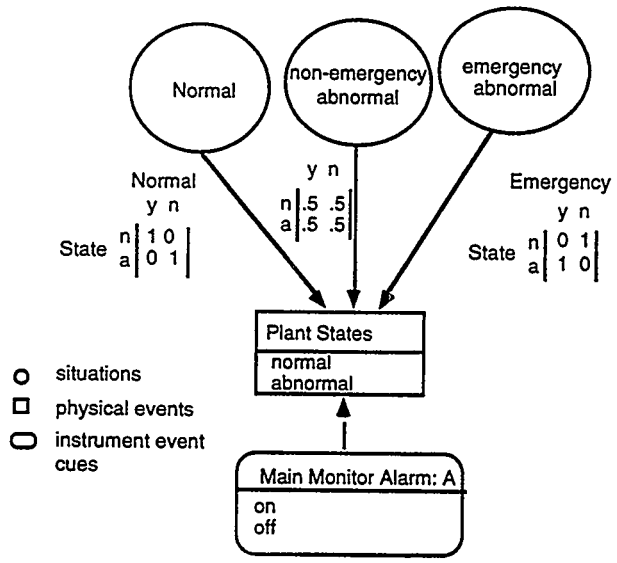


Figure 3-3: Nuclear Power Plant High Level SA Problem

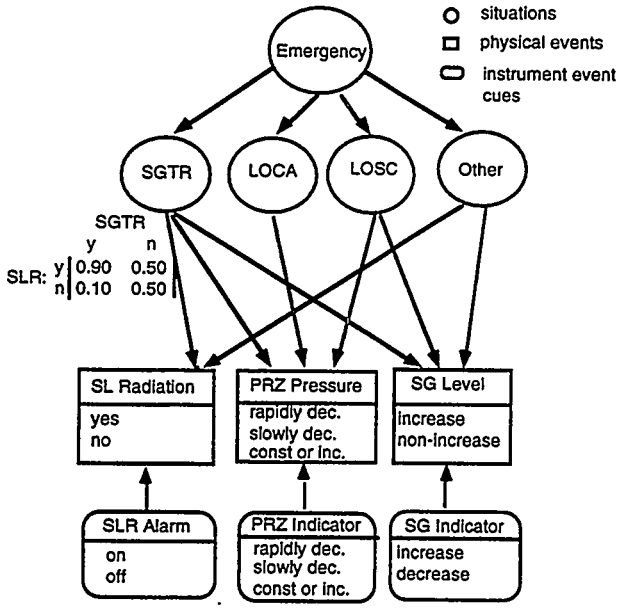


Figure 3-4: Nuclear Power Plant Low Level SA Problem

For the high level SA problem of figure 3-3, we assume that the operator maintains the following ruleset for defining the situation-event relations:

- If the plant is operating normally, all plant states monitored by the main monitor alarm will be within normal range.
- If the plant is in a non-emergency abnormal situation, there is a 50:50 chance that some of the plant states will be out of normal range.
- If the plant is in an emergency abnormal situation, some of the plant states will be out of normal range.

The conditional probability matrices representing these three relations are shown next to the corresponding links in figure 3-3.

For the low level SA problem of figure 3-4, we assume that the operator maintains the following ruleset for defining the situation-event relations:

- If SGTR occurs, the chance of steam line radiation (SLR) is 99%. If SGTR does not occur, steam line radiation may or may not happen, depending on other situations.
- SGTR causes the pressurizer (PRZ) pressure level to decrease rapidly 95% of the time, decrease slowly 4% of the time, and not change 1% of the time.
- SGTR causes the SG pressure level to increase 99% of the time. Without SGTR, there is only a 20% chance the SG pressure level will increase.
- LOCA leads to a rapid decrease, a slow decrease, and no change at pressurizer pressure level 85%, 10%, and 5% of the time, respectively.
- LOSC has the same impact on the pressurizer pressure level change as LOCA does.
- LOSC causes the SG pressure level to increase 60% of the time.
- In the case of emergency abnormal situations other than SGTR, LOCA, and LOSC, there is an 80% chance that steam line radiation will occur.
- Other emergency situations may cause the SG pressure level to increase 60% of the time.

We have taken some liberties in assuming these relations between the situations and physical events, and assigning the associated conditional probabilities, since our current emphasis is on the feasibility of the approach and not the fidelity of the model representation of the actual NPP. For model validation, a careful study of the actual NPP under consideration will need to be conducted to determine the relevant situation-event relations and their associated conditional probabilities, so that the operator model can faithfully reflect the actual situation-event relations.

This SA model, now specialized to the NPP control room scenario, provides us with an *internal* assessment $\hat{\mathbf{S}}$ of the *actual* situation **S** facing the operator. Under the simplifying assumption that the operator's situation memory spans the range of possible situations he might face, we can then define the *situation disparity (SD) vector*, given by the difference between the actual and the perceived situation beliefs via:

$$SD(t) = |(Bel(\mathbf{S}(t)) - Bel(\hat{\mathbf{S}})(t))| \tag{3.4}$$

The average SD across the entire scenario is then:

$$SD = \frac{1}{T}\int_0^T SD(t)dt \tag{3.5}$$

which reflects overall operator awareness across the full span of the selected scenario.

4. Model-Based Analysis

This section describes the results of our model-based simulation of the selected emergency scenario, and our model-based analysis of a candidate NPP automation/aiding option. Section 4.1 describes the results of operator/system modeling of the SGTR scenario, and focuses on operator SA and procedure performance over the course of the scenario. Section 4.2 describes the results of model-based analysis of a candidate control room aid designed to assist in SGTR diagnosis. The study assesses the aid's effect on operator awareness, as a function of aid reliability, operator confidence, display quality, and operator understanding of the aid's performance.

4.1 Model-Based Analysis of SGTR Scenario

We now summarize the results of a model-based analysis of the SGTR scenario.* We do this via a simulation of the plant/operator model, instantiating a specific scenario and its procedures. The scenario and procedures are generated based on the Steam Generator Tube Rupture (SGTR) event that occurred in the North Anna Power Plant Unit 1 on July 15, 1987. A detailed description of the actual event is given in Virginia EPC (1987).

A model-generated operator activity timeline is presented for the case of an ideal display, and is shown in table 4-1. The timeline effectively captures the evolution over time of the important NPP states and events, and the explicit actions of the NPP crew. The table includes four columns. The first column shows the time. The second column shows the actual plant states and events; here we show the SGTR event, and, for simplicity, only pressurizer pressure (in psig). Some of the state variables that are critical for procedure execution (PE) during emergency operating procedure EP-0 (Reactor Trip and Satety Injection) are also included. The third column shows event cues that are used by the operator for SA and PE. The last column shows the operator's actions, in response to the event cues and states.**

---

* A detailed description is given in Zacharias, Miao, Kalkan, et al. (1994).

** Throughout the EP-0 procedure, some of the actions were executed automatically. These steps are not included in the timelines.

Table 4-1: Model-Generated Timeline

Time	Plant States and Events	Event Cues	Actions
06:30:00	2235 SGTR		
06:30:14	2218	Radiation Alarm	Operator observes that the radioactivity alarm for "A" steam line is ON
06:30:21	2209	Low Pressure Alarm	
06:30:34	2198	Pressurizer level and pressure are decreasing rapidly	Charging FCV full open
06:30:44	2190	Pressurizer pressure and level are still decreasing	Letdown isolation
06:30:54	2182	Decrease in over- temperature-delta-temperature limit	10% decrease in turbine load
06:32:34	2105	Decreasing pressurizer pressure and level cannot be stopped from decreasing Emergency	Manual trip
06:32:41	1850	•	Automatic SI actuated
06:32:44	1824	Reactor is tripped	EP-0 Procedure starts
06:33:44	1798	Very low value of FW is present	FW is isolated
06:37:04	1709	Pressurizer pressure less than 2350 psig	PORVs are closed
06:37:24	1696	Radiation alarm, pressure decrease and SG Level increase in loop "A"	SGTR is identified & isolated

We can see from table 4-1 that the first event of the simulated scenario is SGTR at 06:30:00. The pressurizer pressure is 2235 psig at this point, which is the normal value for 100% power. After 14 sec a radiation alarm is received. The operator observes a rapid decrease in the pressure level, and a low pressure alarm follows. The charging flow control valve (FCV) is opened completely at 06:30:34 and letdown isolation occurs 10 sec later, at 06:30:44. The resulting full open FCV and letdown isolation slow down the pressure decrease in the pressurizer. A 10% decrease in the turbine load is initiated 10 sec later, at 06:30:54. Manual trip is entered at 06:32:34 when the pressurizer pressure reaches approximately 2100 psig. Automatic SI actuates 7 seconds after the manual trip. The EP-0 procedure is started immediately after the manual trip. With the manual trip, SG pressure jumps to a high value, and the condenser steam dump valve opens full. After the trip, pressurizer level, pressurizer pressure, and SG levels drop to low values, while the SG pressure increases. The Main Feed Water (MFW) isolation is automatically executed and the Auxiliary Feed Water (AFW) pumps start to run when the SG Narrow Range (NR) level drops below 15%.

The EP-0 procedure starts with the MFW isolation, entered manually at 06:33:44. Although this isolation is executed automatically, low MFW flow is measured at the time. The Auxiliary Feed Water (AFW) pumps are started to provide 200 gpm of flow to each SG. The NR level of SG

"A" recovers at 06:34:20 (reaching a value exceeding 6%), while the other three SGs remain off-scale low. No control is entered to increase the AFW flow, which is below the required value of 525 gpm, and SG NR level values, since the AFW valve is already 100% open. SG level in "A" loop, which has the ruptured tube, increases much faster than the other three, and is one of the symptoms of SGTR after the reactor trip. The RCS temperature is stable around 560° degrees F due to steam dump control. The average RCS temperature time history is shown in figure 6-8. The MSIVs remain open. At 06:37:04 the Power Operated Relief Valves (PORVs) are closed since pressurizer pressure is less than 2350 psig. All four Reactor Coolant Pumps (RCPs) run during the event. The SGTR in SG "A" is identified at Step 25 of the EP-0 procedure, with the indications of the steamline "A" high radiation alarm and the SG "A" NR level at 06:37:24.

This timeline describes the operator's *external* activity in response to the explicit display in the control room. We now focus on the operator's parallel *internal* situation assessment (SA) activities, triggered by the implicit SGTR event. We examine these SA activities within the model context described previously in section 2, and the scenario context set by the timeline itself.

For the SA modeling effort, we assume at the start of the scenario (t=6:30) that the operator has assessed the current situation as normal with a belief value of 99%; the threshold for SA is set as 90%. At 6:30, the NPP incurs an SGTR event which immediately triggers a main steam radiation alarm. For modeling purposes, we assume that the operator believes that the alarm is very reliable as an abnormal state indicator. Consequently, we posit the following rule specifying the deduction relation between the event cue (alarm) and the event (abnormal plant states):

- The operator believes that if the alarm is on, the probability is 99.5% that the plant states are abnormal. He also believes that 5% of the time the alarm might sound falsely.

Note that the belief network approach allows inconsistency in describing the relationship between the event cue and the event. We consider this to be one of the BN approach's advantages, since it allows the determination of an evidential inference rule independently of the other possible cues.

After receiving the event likelihood information on the abnormal plant state, the SA block of the operator/plant model yields its SA result: an *emergency abnormal* situation (recall definitions earlier in Section 3) with a belief of 99%. The assessment of the emergency abnormal situation then starts the low-level SA process to determine which of the four possible emergency situations is the cause of the alarm. The immediate assessment of the emergency abnormal situation from the alarm cue is expected, since in our situation-event model we have assumed a one-to-one deterministic relation between the emergency abnormal situation and the abnormal plant state. This leads to a simple if-then assessment rule for situation assessment, given the high likelihood assessment on the abnormal plant state from the alarm cue.

At 6:31, the operator model notices that the pressurizer (PRZ) pressure level indicator is decreasing rapidly. He also knows that a steam line radiation alarm (which he has detected) means that steam line radiation (SLR) may have occurred. However, since it is the first time that he has seen them, the operator puts low confidence on the evidential value of those cues. We model this via the following evidential deduction rules, which are used to deduce event likelihood from the cues:

- The radiation alarm cue is viewed by the operator as implying steam line radiation with a probability of 95%. However, since the alarm has only been on for a short period, the operator also believes there to be a 50% chance that the alarm may be triggered by reasons other than actual steam line radiation.
- The pressurizer indicator cue is viewed by the operator as implying a 60% chance of rapidly decreasing pressurizer pressure, a 50% chance of slowly decreasing pressure, and a 10% chance of no change.

After receiving these two pieces of evidence (the PRZ indicator and the SLR alarm), the SA model is updated accordingly. After two minutes have passed, the operator model notices that the SLR alarm is still on. He now has almost no doubt that steam line radiation has occurred. Specifically, he assesses the possibility of the radiation event using the following new deduction rule:

- There is a 99% chance that steam line radiation has occurred.

Let us now have an inside look at how the arrival of this cue information on the radiation event affects the beliefs throughout the network. All of the belief updates are shown in figure 4-1, where a number in a circle indicates the order of information propagation and network state updates. The detailed belief updating steps are described below.

1. The new alarm cue is treated as new evidence and causes the cue node SLR Alarm to update its likelihood value, from 0.95 to 0.99.
2. After receiving the new cue information, the event node also updates its event likelihood. It then sends out a λ_e message, which is the incremental likelihood due to the change in the SLR alarm cue.
3. From the incremental likelihood, the situation likelihood vector is computed by multiplying the likelihood with the transpose of the conditional probability. Situation likelihood ratios are then computed via $\lambda_e = \frac{P(e \mid S)}{P(e \mid \neg S)} = \frac{\lambda(1)}{\lambda(2)}$ and sent to two nodes: SGTR and Other.
4. Upon receipt of the incoming likelihood ratio information, the beliefs of each situation node at the current level in the hierarchy are updated using Pearl's algorithm (described in Appendix B).
5. The updated belief values are sent to each situation node to reflect the revised belief based on the evidence received so far.
6. The new situation belief values are then used to compute the prior event beliefs by multiplying the new situation belief with the conditional probability matrix.
7. Upon receipt of the incoming prior belief message, each event node updates its prior belief, reflecting the revised belief based on the new situation assessment.
8. Finally, the prior belief is multiplied with the cue likelihood on a term by term basis, and is normalized to generate the new event belief.

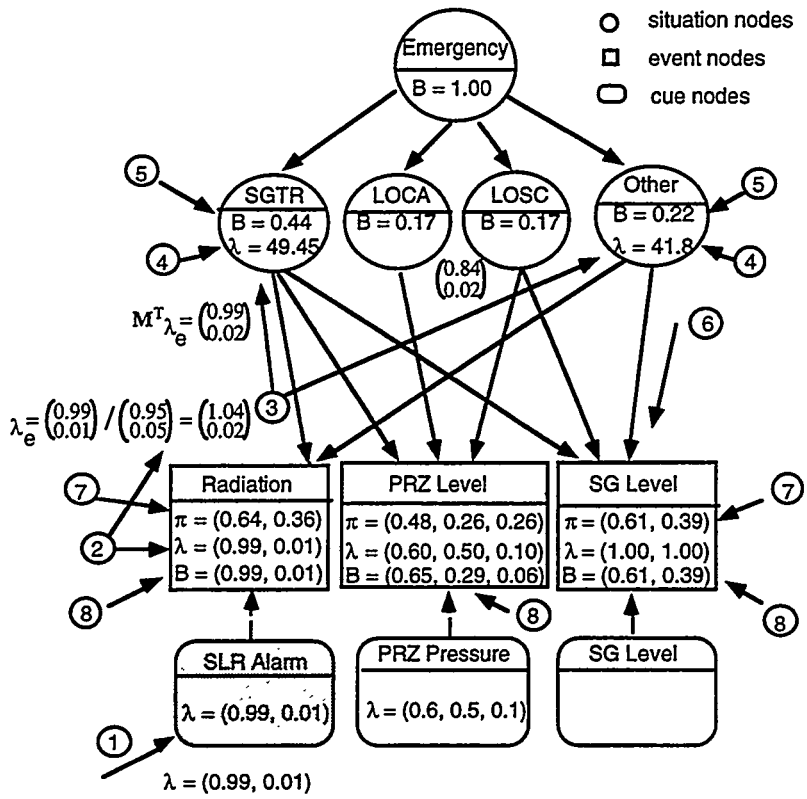


Figure 4-1: Belief Propagation in SA Belief Network

This process is repeated by the SA module every time new evidence is made available to it, through the information processor (IP) module. This occurs throughout the course of the scenario, so that the operator model generates an on-going assessment of the situation. By comparing this with the actual situation, we can then compute a model-based situation disparity (SD) metric as described earlier: the resulting time history is shown in figure 4.2. In the figure, each black dot represents a situation assessment update due to the incoming event cues at the time. Each cue is denoted by its abbreviation and a small arrow that indicates the change in the likelihood value due to that cue. An upward arrow implies that the operator considers the event referred by the cue as more possible, whereas a downward arrow implies the opposite.

From the model-generated timeline of table 4-1 and the disparity history of figure 4-2, we obtain a clear picture of how situation awareness evolves with the accumulation of the event cues. The operator starts with low SA, as shown by a high disparity metric and a low belief in the actual situation, SGTR, although SGTR is viewed as one of four equally possible situations. Each partial incoming cue then contributes to the situation awareness of the operator: some positively, some negatively, and some insignificantly as shown by the up, down, and flat trend of the SD time history. The accumulation of the cue evidence eventually drives the operator to correctly assess the situation in approximately 6 minutes.

The SD history also gives an individual account of how each partial cue contributes to overall SA. Specifically, we can see from the timeline that the SG level cue at time 6:35 plays a significant role in the operator's eventual correct assessment of the situation. We can also see that the contribution of each partial cue to overall SA is limited, as shown by the SD and belief changes between 6:33 and 6:34. During this period, the operator has increased the event probability of rapidly decreasing PRZ pressure from 0.95 to 0.999, using the pressurizer indicator cue. The situation disparity and belief in the actual situation (SGTR), however, stays almost unchanged. As

a matter of fact, if the operator has available only two partial event cues he will not be able to assess the SGTR situation (relative to the given threshold), no matter how he improves the likelihood estimate of his observable events.

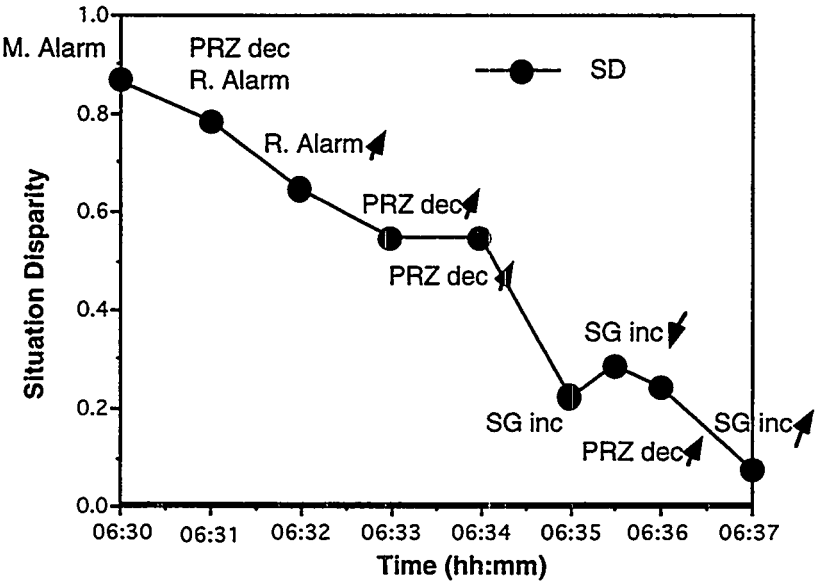


Figure 4-2: Time History of Situation Disparity for Nominal SGTR Scenario

This inability to perform correct SA with partial cues is especially surprising considering how strong an individual correlation we have assumed between a situation and an event. Remember that it is assumed that an SGTR event will cause steam line radiation 99% of the time with a 95% chance of causing a rapid pressurizer pressure decrease. However, even when the operator has assessed that radiation has occurred (with a 99% probability), *and* that the pressurizer pressure is decreasing rapidly (with a 99.9% probability), using his alarm and pressurizer indicator cues, he is only able to achieve a 54% belief in SGTR. The reason, of course, is that both alarm and pressurizer level cues are also highly correlated with other situations. We can thus conclude that when there are cross situation-event relations, reliable and accurate SA requires cues from *multiple independent sources*. The lack of a critical discriminating cue makes SA impossible.

This simulation also shows the ability of the belief network approach to coherently and consistently combine cue information at whatever level of abstraction (hierarchy) is appropriate for the SA task. For example, we have assumed that a main alarm cue only indicates an abnormal plant state (thus an emergency abnormal situation), and says nothing about the situation's four constituent situations. Consequently, the belief update is conducted at the emergency abnormal situation level without any knowledge of the existence of the four possible constituent sub-situations. This feature can greatly simplify model development and computational time, since a hierarchical approach can be employed with varying levels of situation granularity.

Furthermore, belief updating clearly shows how severely a single cue's impact on SA is affected by the cross situation-event relations. For example, an SGTR event is assumed to cause steam line radiation 99% of the time. At 6:33, the operator is assumed to have a 95% belief that steam line radiation has occurred, with a 5% possibility for a false alarm. The resulting belief in SGTR, however, is much smaller than 95% since we have assumed that other emergency situations may also have caused the steam line radiation.

Finally, the simulation clearly demonstrates the capability of the BN approach to support tentative situation assessment and to deal with both positive and negative evidence. At time

6:35:30, the operator observes the SG level increase. He attaches a high likelihood (0.90, 0.05) to the cue and uses it for SA. A tentative SA assessment is then conducted to assign each situation node a belief value that is consistent with this new evidence. Thirty seconds later, the operator feels that he may have put a higher confidence on the cue than it deserves. He corrects the likelihood to (0.6, 0.05). That is, negative or disconfirming evidence is applied for SA at 6:35:30. We can thus see that the belief assignment is updated to properly handle this piece of negative information so as to have a negative impact on SA.

4.2 Effect of Automation on SA

The model-based analysis we have just described demonstrates the difficulties the operator faces in maintaining adequate awareness when there exist complicated cross situation-event relations. This is reflected by the relatively long time spent to assess the SGTR event in the actual timeline described in the previous chapter. The operator/system model also identifies the major reason for SA difficulties: the intricate relation between situations and events requires the operator to integrate various cues for SA, since no single-cue signs suffice. Missing one critical cue may make SA impossible. On the other hand, when there exists a simple relation between a situation and an event, SA almost reduces to a simple if-then process. This motivates a possible solution to facilitate SA: develop an SA aid that fuses the intricate situation-event relations, via automation, and represents the resulting simple relations with a new set of cues.

We now assess the effect of such an SA aid on the operator's situation awareness. We presume the existence of an SA aid that integrates various pieces of plant event information through automation, to generate an event that has a simple one-to-one relation with a situation, and that provides the needed event cue information to the operator via the display.

We first evaluated two key attributes of the SA aid: aid *reliability* and operator *confidence* in the aid. Aid *reliability* reflects aid correctness in declaring a given situation in the face of the actual situation. Low reliability will lead to a high number of incorrectly assessed situations by the decision aid. Operator *confidence* in the aid reflects the operator's confidence in using the cue generated by the aid for SA, independent of actual aid reliability (i.e., the operator *could* have high confidence in a low reliability aid, although probably not for long). Our interest lies in how the twin attributes of automation *reliability* and operator *confidence* affect the operator's SA when he uses such an SA aid.

We then proceeded to evaluate the effect of displayed cue quality on SA. When ideally displayed, a cue should be a faithful indicator of its represented event. The cue should bring to the operator the same amount of information that the event itself does. There should be no doubt of the operator deducing the event from its cue. A non-ideal display, however, should distort the equivalent relation between the cue and event. Consequently, uncertainty arises in deduction of an event from its cue. We postulated that the quality of a display would be proportional to this cue-event deduction uncertainty. The worse the display quality, the higher the uncertainty that an operator has in deduction of an event from its cue. Our interest lies on how the display cue quality, represented by the cue-event deduction uncertainty, affects the operator's SA.

Finally, we evaluated the effect of the operator's subjective assessment of aid reliability on SA. In an ideal situation, after a careful knowledge engineering process we would develop a BN model that correctly and faithfully represents every situation-event relation in an actual SA problem. This may not be possible in complex NPP operations, so our interest lies in how BN modeling error affects operator SA.

The BN model of the SA problem provides a powerful and natural tool for evaluation of all these effects, since the model explicitly represents the operator's internal model of the SA problem and his subjective judgment of cues.

To illustrate, suppose that an SA aid is developed for declaring an SGTR event. The aid represents a simple relation from many SGTR cues to an integrated event, which we will name SGTR_ALARM, with a *reliability* level α, where $\alpha = 0$ indicates a zero reliability and $\alpha = 1$ indicates 100% reliability. In other words, we have the following rule-based relation between SGTR and SGTR_ALARM:

- SGTR activates SGTR_ALARM 100a% of the time, while no other emergency situation activates the SGTR_ALARM

or the following probabilistic transition matrix representation:

$$M = \begin{pmatrix} \alpha & 1-\alpha \\ 1-\alpha & \alpha \end{pmatrix} \tag{4.1}$$

Note that as a result of the exclusive relation between SGTR and SGTR_ALARM, the SA aid is, in fact, related to two events: an SGTR_ALARM event and its negation, the lack of an SGTR_ALARM event. That is, the operator also can be sure that if SGTR does not occur, the occurrence probability of an SGTR_ALARM event would be (1 - α) for the SGTR_ALARM event, and α for its negation.

We further assume that a cue generated by the SA aid will always be sensed by the operator. However, the operator can choose to either use or ignore the cue. Specifically, let C, $0 \leq C \leq 1$, represent the operator's *confidence* in the SGTR_ALARM. We model the effect of operator confidence in the aid as follows:

- The operator believes that the SA aid is right only 100C% of the time, and therefore uses it 100C% of the time.

where $C = 0$ represents a zero confidence in the aid since the operator will always ignore the cue, and while $C = 1$ represents full confidence in the aid since the operator will use it all the time.

We can evaluate the twin attributes of automation reliability and operator confidence via multiple Monte Carlo simulation runs, in which the SA aid generates cues consistent with aid reliability over long runs.

In the BN model of the SA problem, the *quality* of a displayed cue is represented by the subjective judgment rule of what a cue implies, i.e., the uncertainty level of the cue event deduction rule. Specifically, we assume that the operator uses the following deduction rule to determine the likelihood of the SGTR event from an SGTR_ALARM cue:

- The operator believes that an SGTR_ALARM cue implies an SGTR event via the following likelihood vector:

$$\lambda = 0.5(1+\beta, 1-\beta)^T \tag{4.2}$$

where $\beta = 0$ represents the worst display since the cue implies equivalently the occurrence of an SGTR event and its negation (i.e., λ=(0.5,0.5)), and $\beta = 1$ represents the ideal display where the cue is equivalent to the event (i.e., λ=(1,0)). Consequently, we can evaluate the effect of display quality on the operator's situation awareness by varying the display quality parameter β in simulations.

Finally, consider the relation between SGTR and SGTR_ALARM. The actual relation is defined by α and the transition matrix M of (6.1) above. Independent of this actual relation, the operator's internal BN model can have its own representation of the relation. Specifically, we assume that

- The operator believes that SGTR activates SGTR_ALARM 100g% of the time, while no other emergency situation activates SGTR_ALARM

where $0 \leq \gamma \leq 1$. That is, the operator uses a subjective reliability to model the situation event relation in his internal BN model. When $\beta < \gamma$, the operator has a model error (or bias) that assumes a stronger correlation between SGTR and the SGTR_ALARM event; while $\beta > \gamma$ implies the opposite.

We first evaluated the effect of **automation reliability** and **operator confidence**, using Monte Carlo simulation runs. The nominal simulation described in section 4.1 was adopted where SGTR occurred at the beginning of the simulation. In each simulation, the SGTR_ALARM event and cue were created 1 min 30 sec after SGTR, using a uniformly distributed random variable ε, ranging between 0 and 1. The SGTR_ALARM event and cue were created if $\varepsilon \geq \alpha$. Whether the cue was to be used for SA was determined in a similar fashion, using another uniformly distributed random variable based on the confidence level β. An ideal display was assumed for the aid. This was modeled by having the operator deduce the occurrence likelihood of the SGTR_ALARM event from its cue via the following rule:

- An SGTR_ALARM cue implies SGTR_ALARM with a likelihood vector (1, 0), while the lack of an alarm cue implies the opposite, with a likelihood vector (0, 1).

Figure 4-3 shows the impact of different aid reliability levels on operator Situation Disparity (SD), when the SGTR_ALARM cue is used for SA. The figure shows that an SA aid that represents a simple situation-event relation can help SA significantly. A highly reliable SA aid (99%) can be used by itself for the confident assessment of the situation intended by the aid. Even a moderately reliable SA aid (75%) contributes more to SA than does a much more reliable event cue that leads to cross situation-event relations. For example, the radiation alarm event (cue) is more reliably linked to the SGTR event, since SGTR triggers the radiation alarm 99% of time. However, the SA aid cue which is only moderately reliable (75%) generates a much larger SD reduction than does the radiation alarm cue, because the latter has more complex cross situation-event relations compared with the former. This result clearly shows the benefit of developing even moderately reliable SA aids when there are intricate cross situation-event relations involved.

Figures 4-4, 4-5, and 4-6 illustrate the time averaged Situation Disparity (SD) of 50 simulation runs, plotted as a function of confidence in the decision aid, for three different levels of decision aid reliability (99%, 75%, 55%), respectively. For the *high* reliability aid (99%) illustrated in figure 4-4, it can be seen that the more confidence the operator has on the decision aid, the better his situation awareness (the lower his SD). Here, when the operator has full confidence in the decision aid (100%), we obtain a 3-fold reduction in SD compared with the unaided (zero confidence) case. For the *medium* reliability aid (75%) case illustrated in figure 4-5, the operator still achieves better situation awareness with higher confidence in the aid, although the SA improvements are not as dramatic as those obtained with the high reliability aid. For the *low* reliability decision aid (55%) case illustrated in figure 4-6, we see a converse trend from the other two cases: SD *increases* with the level of confidence put on the (low reliability) SA aid.

On the basis of these results, we would conclude that, when developing an SA aid, the key is to make sure that the aid represents a simple situation-event relation *and* has a high reliability. The use of a high reliability aid always helps SA since higher reliability tends to encourage operator use. Low reliability aids, however, can hurt operator SA, if they are held in high confidence. A safe strategy would be for the operator to have a *confidence level* in the decision aid that is consistent with or slighter lower than the aid's *reliability*, thus achieving the best SA improvement in high and medium reliability cases while not risking too great a decrease in SA in a low reliability case.

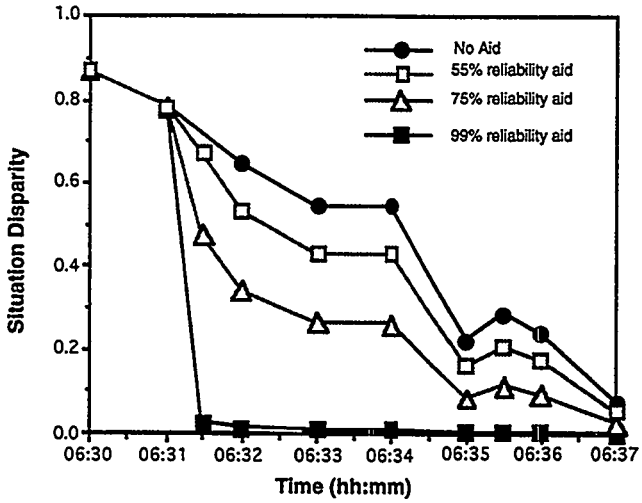


Figure 4-3: Effectiveness of SA Aid

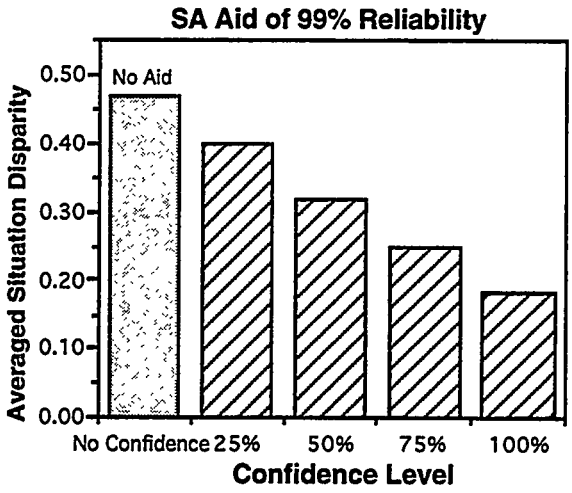


Figure 4-4: SD vs. Decision Aid Confidence (99% Reliability)

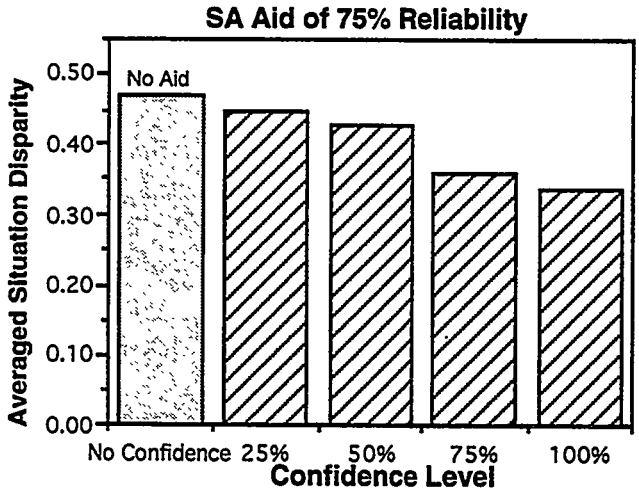


Figure 4-5: SD vs. Decision Aid Confidence (75% Reliability)

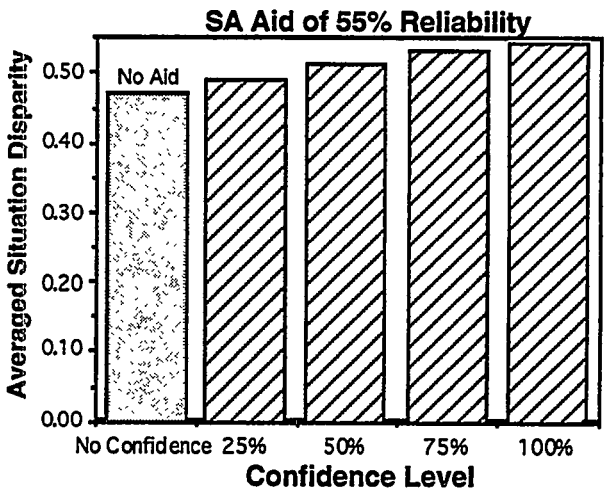


Figure 4-6: SD vs. Decision Aid Confidence (55% Reliability)

We then evaluated the effect of aid **display quality** on operator SA, again using Monte Carlo simulations. Each simulation followed the nominal timeline, with a 99% reliable SGTR_ALARM aid cue created 1 min 30 sec after SGTR. We modeled the display quality by linking it to the uncertainty level of the cue event deduction rule: the poorer the display quality, the greater the uncertainty the operator has in deducing the event from its cue. In this way, a cue presented on the *worst* display implies both an event and its negation (i.e., a 50:50 chance), while a cue presented on the *best* display implies the event with total certainty.

Figure 4-7 shows the SD time history for five levels of display quality, ranging from the worst to the best. The worst case profile follows the unaided profile illustrated earlier in figure 4-2. As

the display quality improves, we see a monotonic decrease in operator SD, at all times in the scenario following aid cueing after the event. Note the rapid achievement of operator SA with the best display, immediately following display aid cueing at t=06:31:30.

Figure 4-8 shows the time-integrated effect of SA improvement (SD reduction) over the unaided case. A clear monotonic relation holds here, with better quality aids leading directly to greater operator SA.

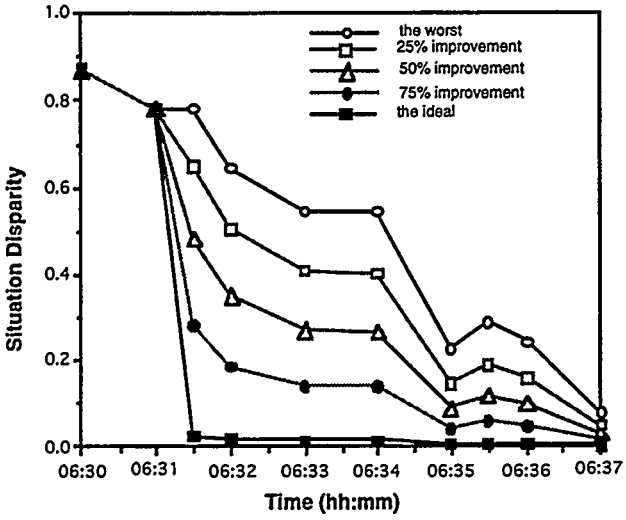


Figure 4-7: Effectiveness of Display Quality on SD

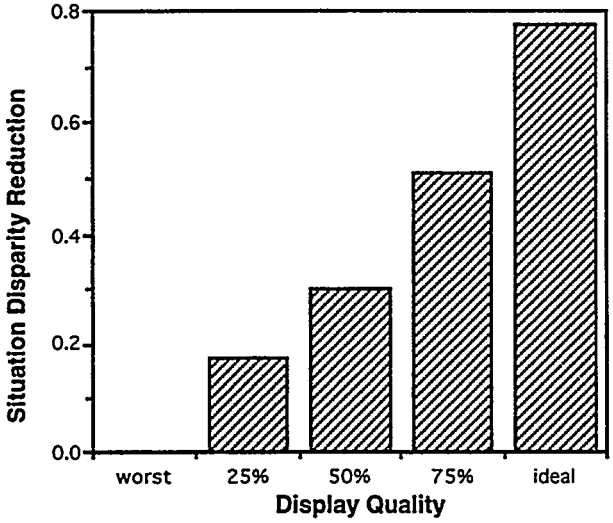


Figure 4-8: SD Reduction vs. Display Quality

We also evaluated the effect of the **operator's subjective assessment of aid reliability** on operator SA, again using Monte Carlo simulations. To isolate the impact of this factor from other sources, we assumed that the operator had 100% confidence in the aid, and an ideal display for the cue. The SGTR_ALARM event and cues were generated 1 min 30 sec after SGTR, using a uniformly distributed random variable ε, ranging between 0 and 1. The SGTR_ALARM event and cue were created if $\varepsilon \geq \alpha$. Otherwise, the cue at the time would be the lack of SGTR_ALARM. Based on this cue, the situation beliefs in the BN model were updated using the operator's *subjective* reliability assessment, rather than *actual* aid reliability. The resulting SD reduction or increase was then computed, and fifty Monte Carlo simulation runs were conducted to generate the average SD reduction and the variance in that reduction.

Figure 4-9 shows the resulting SD reduction as a function of the operator's subjective assessment of aid reliability, plotted for three different actual reliability levels: 55%, 75%, and 99%. It can be seen that the SD reduction resulting from using the SA aid is positively correlated to actual reliability: the higher the actual reliability, the greater the SD reduction to be achieved, for the same subjective reliability. In addition, both the average SD reduction and the standard deviation are proportional to the subjective reliability, which determines the actual SD reduction capability of an SA aid. For example, a 99% reliable aid will perform at a 75% level, if the operator *thinks* that it is a 75% reliable aid. This implies that the operator should not under-estimate aid reliability since it will reduce its effectiveness. On the other hand, the greater SD reductions achieved with higher subjective reliability should not be regarded as a recommendation for exaggerating aid reliability, since the SD reductions are achieved with high standard deviations, which implies considerable uncertainty in interpreting the SA result achieved by using the aid. In other words, exaggerating aid reliability leads to better *average* SA but also to a greater chance of incorrect aiding, because of a greater *variance* in SA. Note that the amount of variance increase is larger than the amount of SD

reduction achieved by exaggeration. This suggests that, in general, it is not appropriate to exaggerate aid reliability to achieve better average operator awareness.

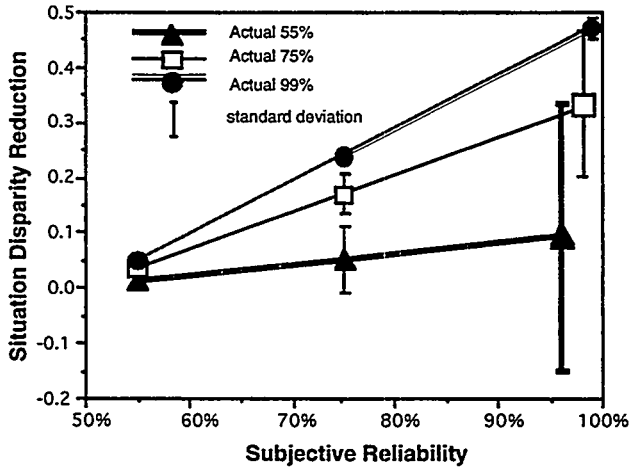


Figure 4-9: SD Reduction vs. Subjective Reliability Assessment

5. Conclusions

This paper **described an integrated operator/system model architecture** that allows us to combine and integrate the system-related and operator-related components of the system and task that drive overall operator awareness and performance. The model architecture integrates the operator's basic functions of: 1) information processing (IP) of the man-machine interface displays to generate estimated system states and event cues; 2) situation assessment (SA) using event cues to drive procedure selection; and 3) procedure selection and execution (PE) based on the assessed situation and estimated system states to select among alternative procedures and to effect motor commands and communication.

We also **developed a situation awareness submodel and metric** using BNs to support a demonstration of its use in assessment of plant automation and aiding options. The submodel is used to generate a dynamic estimate of the operator's internal assessment of the current operating situation. A direct comparison with the actual situation being played out in the external world provides the basis for defining a situation disparity vector, given by the difference between the actual and the perceived (multi-dimensional) situation. An appropriately defined scalar is used as a measure of the operator's SA. In conjunction with the SA model, the awareness metric thus provides a direct means for evaluating different automation concepts in terms of their support for maintaining a high level of operator SA.

The **belief network (BN)** approach to SA modeling gave us the capability and flexibility to model human SA in its full richness (or simplicity as the case might be), without arbitrary restrictions. They provide several advantages over other approaches for modeling SA. First, BNs provide a comprehensive picture of the SA problem by indicating the dependent relationships among the situations to be assessed and the event cues to be detected. Second, belief updating by a Bayesian reasoning logic reflects the continuity in time of SA: it is an evidence accumulation process where the new evidence of the event cues is combined with the old evidence of the network node belief values. Third, Bayesian reasoning logic is mathematically sound and provides a consistent and coherent automatic reasoning process for the given evidence. It is a normative reasoning process that prescribes what a human *should* do, given situation-event relationship and evidence cues. Moreover, the belief updating process provides a clear view of how each new piece of evidence (event cue) affects situation assessment. Fourth, BNs allow the consideration of

evidence at any level of abstraction and from any sources. Finally, the computation algorithm is simple and easy to implement in the case of singly connected networks. A BN representation is thus a very natural choice for modeling the human operator SA process.

To demonstrate the modeling approach, we **implemented and demonstrated a prototype model/metric**, for a selected nominal scenario and a range of contemplated NPP control room automation/aiding options. The prototype demonstrator integrated a high-fidelity FORTRAN-based simulation model of a four-loop PWR, a C++ language executive model of the operator, and a C++ implementation of the critical SA submodel. This overall implementation provided a natural hybrid architecture for future expansion in automation/aiding options, operator activities, and simulation fidelity. Using the prototype model, we demonstrated operator SA and procedure performance during the course of a steam generator tube rupture (SGTR) event. Via the metric, we evaluated the impact of a diagnostic situation assessment aid on operator situation awareness and demonstrated how the model-based metric can be used to evaluate decision aid effectiveness as a function of the aid's reliability, the operator's confidence in that aid, the display quality, and the operator's subjective model of the aid.

Our **proof-of-concept demonstration** focused on a steam generator tube rupture (SGTR) event occurring in a three-loop PWR. The demonstration focused on the event itself and the immediate sequence of operator activities dealing with the assessment of the situation and emergency procedure execution. This prototype demonstration provided a basis for evaluating the requirements for problem setup, supported an objective evaluation of nominal and automated system operation, and provided the foundations for a detailed timeline analysis of operator activities during and following the event. The major findings of our demonstration effort can be summarized as follows:

- We demonstrated that an integrated operator/system model is capable of simulating a complete nuclear power plant emergency scenario, in this case a steam generator tube rupture (SGTR), from its occurrence to its diagnosis. We did this using the CSIM model and an object oriented implementation of it, specialized to the particular scenario under analysis.
- The simulation supported the general evaluation of operator performance and situation awareness. The model-generated timeline and SA metric explicitly showed the cause-effect relationships among key displays, cues, plant state and events, situations, and controls. Furthermore, the timelines showed the values and status of these key plant and operator variables, and their progress with time. We generated both internal and external views of the ongoing operator SA process via an SA metric, and an individual account of the SA reasoning process. Together, they showed: 1) how each individual cue contributes to overall SA; 2) how internal SA is achieved, starting with a triggering cue and ending with the belief updating of all related situations and events; and 3) how SA evolves via the accumulation of cues over time.
- We showed that correct SA is difficult when there exist intricate situation-event relations among the situations to be assessed, and the events caused by these situations. Under such circumstances, correct SA requires integrating cues from multiple independent sources rather than relying on highly reliable individual cues. The lack of a critical discriminating cue makes reliable and accurate SA impossible.
- We demonstrated that an NPP control room SA aid that simplifies situation-event linkages can help improve operator SA greatly. Furthermore, we demonstrated how to use model-based SA metrics to assess the effects of the aid on overall operator awareness. In particular, we showed the effects of aid reliability, operator confidence, and aid display quality, as well as the impact of the operator's subjective model of the aid, in a repeatable and quantitative fashion.

- We showed that when developing an SA aid, the key is to make sure that the aid represents a simple situation-event relation, *and* has a high reliability. The use of a high reliability aid always helps SA, since higher reliability tends to encourage operator use. Low reliability aids, however, can hurt operator SA, if they are held in high confidence. A safe strategy would be for the operator to have a *confidence level* in the decision aid that is consistent with or slighter lower than the aid's *reliability*, thus achieving the best in high and medium reliability cases while not risking too great a decrease in SA, in a low reliability case.
- We showed that an aid's effectiveness on the operator's SA is proportional to display quality, the higher the quality: the better the SA improvements.
- Finally, we showed that the most critical aspect determining effective use of an aid is the operator's understanding of the aid's reliability. This must not be underestimated, since it will reduce the effectiveness of a high reliability aid. Conversely, reliability must not be overestimated, since this can lead to a high level of SA uncertainty.

Our **recommendations for further development** focus on the development, validation, and demonstration of a full-scope design tool for assessing NPP automation/aiding design options. This would require expansion of the model and metric to a broader scope of scenarios and design options, transitioning the research software into an applications-oriented software toolbox, validation of use via full-scope design analysis and simulation, and demonstration of toolbox utility to the control room design community.

6. References

Baron, S., Zacharias, G., Muralidharan, R., et al. 1980. "PROCRU: A Model for Analyzing Flight Crew Procedures in Approach to Landing." *16th Annual Conf. on Manual Control.* Cambridge, MA.

Cacciabue, P.C., Decortis, F., Drozdowicz, B., et al. 1992. "COSIMO: A Cognitive Simulation Model of Human Decision Making and Behavior in Accident Management of Complex Plants." *IEEE Transactions on Systems, Man, and Cybernetics*, Vol. 22, No. 5, SEPT.OCT: pp. 1058-1074.

Dang, V.N. and Siu, N.O. 1994. "Simulating Operator Cognition for Risk Analysis: Current Models and Crewism." *Proceedings of PSAM-II, An International Conference Devoted to the Advancement of System-Based Methods for the Design and Operation of Technological Systems Processes.* San Francisco, CA.

Huang, Y., Dang, V. and Siu, N. 1993. "Modeling Control Room Crews for Accident Sequence Analysis." *Proc. Probabilistic Safety Assessment International Topical Mtg. (PSA '93).* La Grange Park, IL. American Nuclear Society.

Kao, S.P. 1988. "Seabrook Simulator Model Upgrade: Implementation and Validation of Two-Phase, Nonequilibrium RCS and Steam Generator Models." *Conference on Power Plant Simulators and Modeling*, Vol. EPRI GS/NP-6670.

Kao, S.P. 1991. "PRISM: An Integrated RCS and Steam Generator Simulation Model." *ANS International Topical Metting, Advances in Mathematics, Computation, and Reactor Physics*, Vol. 3, No. 12.2.5.

Klein, G.A. 1989a. "Recognition-Primed Decisions." *Advances in Man-Machine Systems Research*, Vol. 5: 47-92.

Klein, G.A., et. al. 1989b. "Critical Decision Method for Eliciting Knowledge." *IEEE Trans. on Systems, Man and Cybernetics*, Vol. 19, No. 3: 462-472.

Klein, G.A., Calderwood, R. and Clinton-Cirocco, A. 1986. "Rapid Decision-Making on the Fire Ground." *Proc. Human Factors Society 30th Ann. Meeting.*

Klein, G.A., Calderwood, R. and Macgregor, D. 1989. "Critical Decision Method for Eliciting Knowledge." *IEEE T-SMC*, Vol. 19, No. 3: 462-472.

Klein, G.A., Orsanu, J., Calderwood, R., et al. 1993. *Decision Making in Action: Models and Methods.* Norwood, NJ: Ablex Publishing Corporation.

Kleinman, D.L. and Baron, S. 1971. *Analytic Evaluation of Display Requirements for Approach to Landing.* NASA. CR-1952 (November).

Levison, W.H., Baron, S. and Kleinman, D.L. 1969. "A Model for Human Controller Remnant." *IEEE Trans. on Man-Machine Systems*, Vol. 10.

Pearl, J. 1986. "Fusion, Propogation, and Structuring in Belief Networks." *Artificial Intelligence*, Vol. 29, No. 3: 241-288.

Pearl, J. 1986. "On Evidence Reasoning in a Hierarchy of Hypotheses." *Artificial Intelligence*, Vol. 28: pp. 9-15.

Roth, E.M., Woods, D.D. and Pople, H.E. 1992. "The Cognitive Simulation as a Tool for Cognitive Task Analysis." *Ergonomics*, Vol. 35, No. 1163.

Stiffler, D.R. 1987. *Exploiting Situational Awareness Beyond Visual Range.* Maxwell AFB, AL. 87-2370, ACSC/EDCC (April).

Van DeGraaf, R.C. 1988. *An In-Flight Investigation of Workload Assessment Techniques for Civil Aircraft Operatiosn.* National Aerospace Laboratory NLR. NLR TR87119U (1988).

Visser, J. 1988. *PROCRU Simulation Results Compared with Metro II IN-Flight ILS Approach Data.* National Aerospace Laboratory NLR. NLR TR 87180L.

Woods, D.D., Roth, E. and Pople, H. 1989. *Cognitive Environment Simulation: An Artificial Intelligence System for Human Performance Assessment.* U.S. Nuclear Regulatory Commission. NUREG-CR-4862.

Zacharias, G.L. and Miao, A. 1994. "Timeline Analysis and Crew Modeling of Datalink Simulation." *Conference Proceedings of Cognitive Modeling Workshop.* NASA Ames Research Center, Moffett Field, CA.

Zacharias, G.L., Miao, A.X. and Riley, E.W. 1992. *Situation Awareness Model for the BVR Mission.* Charles River Analytics Inc. R90011 (December 1992).

Zacharias, G.Z., Miao, A., Kalkan, A., et al. 1994. *Operator Model for Nuclear Operations Automation Assessment.* Charles River Analytics Inc. R93141 (August 1994).

Simulation and Experimental Studies of Operators' Decision Styles and Crew Composition While Using an Ecological and Traditional User Interface for the Control Room of a Nuclear Power Plant

Najmedin Meshkati, Brian J. Buller and M. Ali Azadeh

Institute of Safety and Systems Management
University of Southern California
Los Angeles, California 90089-0021
U.S.A.

Abstract

The goal of this research is threefold: 1) use of the Skill-, Rule-, and Knowledge-based levels of cognitive control -- the SRK framework -- to develop an integrated information processing conceptual framework (for integration of workstation, job, and team design); 2) to evaluate the user interface component of this framework -- the Ecological display; and 3) to analyze the effect of operators' individual information processing behavior and decision styles on handling plant disturbances plus their performance on, and preference for, Traditional and Ecological user interfaces.

A series of studies were conducted:. In Part I, a computer simulation model and a mathematical model were developed. In Part II, an experiment was designed and conducted at the EBR-II plant of the Argonne National Laboratory-West in Idaho Falls, Idaho It is concluded that: The integrated SRK-based information processing model for control room operations is superior to the conventional rule-based model; operators' individual decision styles and the combination of their styles play a significant role in effective handling of nuclear power plant disturbances; use of the Ecological interface results in significantly more accurate event diagnosis and recall of various plant parameters, faster response to plant transients, and higher ratings of subject preference; and operators' decision styles affect on both their performance and preference for the Ecological interface.

Introduction

A traditional human factors (i.e., microergonomic) approach to complex human-machine systems is only concerned with improving the workstation (user interface) design. This approach, by ignoring the importance of the integration of the user interface with job and organizational design, results in systems which lead, at best, only to sub-optimization and are therefore inherently error- and failure-prone (Meshkati, 1991a). Such systems, when eventually faced with the concatenation of certain fault events, will suffer from this 'resident pathogen' and, as such, are doomed to failure (Reason, 1990). Also, when complex technological systems, such as nuclear power plants, move

from routine to non-routine (normal to emergency) operation, the controlling operators need to dynamically match the system's new requirements. This mandates *integrated* and *harmonious* changes in information presentation (display), changes in (job) performance requirements in part because of operators' inevitable involuntary transition to different levels of cognitive control, and reconfigurations of the operators' team (organizational) structure and communication (Meshkati, 1991b). It is also demonstrated that the skill, rule, and knowledge (SRK) model, developed by Rasmussen (1983; 1986), is a high-potential and powerful framework that could be utilized for the proposed integration purpose.

The objective of this research is threefold: 1) using the SRK model, to develop an integrated information processing conceptual framework (for integration of workstation, job, and team design); 2) to evaluate the user interface component of this framework -- the ecological display, and 3) to analyze the effect of operators' individual information processing behavior and decision styles on handling plant disturbances, on their performance and preference for traditional and ecological user interfaces.

Part I: Simulation Studies

In the first phase of this NRC-sponsored research, a computer simulation methodology is used to compare the performance and evaluate the validity of the SRK-based integrated information processing model with the conventional framework. The properties of the integrated model are: 1) The panels and displays are designed such that the operators are responsible for all parts of the plant rather than specific units. This requires the *integrated display systems* that present information about all the relevant operations in the plant; 2) The operators are *generalists*. They are trained to perform any task in the control room; and 3) Operators employ *teamwork* in case of a complex and uncertain situation by considering the *optimal decision styles* mixes of the operators (see below). Advantages of the Integrated Information Processing model are reflected in the following measures of effectiveness: 1) smaller probability of error during detection and monitoring of non annunciated events, flux tilt and inadvertent safety injection, 2) smaller average waiting times of incidents during rule- and knowledge-based situations, and 3) smaller average waiting times of routine events, 4) better balance of workload for the reactor operators and senior reactor operators, and 5) average number of emergency and routine events during multiple failure situations is substantially smaller.

In addition, a survey was designed and given to experts in the field to evaluate the robustness of the outcomes of the simulation models. Nine nuclear power plant disturbances were considered in the simulation. These were: 1) small loss of coolant accident, 2) nuclear instrumentation malfunction, 3) steam generator tube rupture (leak), 4) inadvertent safety injection at power, 5) resistance temperature detector, 6) flux tilt event, 7) dropped control rod failure, 8) loss of main feedwater, and 9) reactor trip. The results of computer simulations revealed that integrated information processing was superior to the conventional rule-based systems. The two systems were tested at the 0.05 significant level. The time to process incidents were not significant at 0.05 level, however, the different processing times of some disturbances, including flux tilt event and nuclear instrument malfunction, are significant at the 0.10 level. The findings of the task data survey which evaluate the amount of perceived difficulty and information used for typical incidents are very close and corroborate the results of computer simulations for both integrated and conventional models.

The advantages of the integrated information processing model were due to: 1) smaller probability of error during detection and monitoring of an incident, 2) minimization of average waiting times for incidents during rule- and knowledge-based scenarios, 3) minimization of average waiting

times for routine events, and 4) a better balance of workload for the reactor operators and senior reactor operators.

Furthermore, the effect of operators information processing behavior and their individual differences are analyzed by the Decision Style model (Driver, Brousseau, and Hunsaker, 1993). This model suggests that environmental pressures (or load) systematically affect the complexity of information processing in an inverted-U-shaped function. Each individual can be considered to have a unique and consistent curvilinear information-use pattern, referred to as their decision style. Every individual has acquired at least one basic or "dominant" decision style that is normally exhibited under moderate environmental load. For most people, a second or "backup" style emerges in extreme environmental load conditions, such as uncertainty and time pressure. Environmental load is defined as the sum of the effects of four basic factors: (a) information complexity (e.g., information load, time pressure); (b) noxity or negative input (e.g., threat); (c) eucity or positive input (e.g., support from others); and (d) uncertainty (Driver, 1979).

The decision style model is based on two primary dimensions: information use and focus. Information use refers to the amount and complexity of information actually used in thinking and decision making. Focus is defined as the number of alternatives which are contained in the final solution reached. Focus is a continuous dimension ranging from unifocus, in which a single alternative forms the outcome, to multifocus, in which many different options are included in the final solution. The unifocus style takes a given amount of data and connects it around a single solution or decision alternative, whereas the multifocus style takes the same amount of data and integrates it to several outcomes simultaneously or within a very short time. The information use dimension can be split at some point between two extremes; at one extreme are those individuals who habitually use as much non-redundant information as is available, termed maximizers. At the other extreme are those individuals who use just enough information to generate one or two useful alternatives, termed satisficers. The maximizer/satisficer dimension suggests a high vs. low degree of integration, or the type and amount of connections between information units during analysis. By combining the dimensions of focus and information use, five distinct decision styles can be recognized: Decisive (unifocus, satisficer), Hierarchic (unifocus, maximizer), Flexible (multifocus, satisficer), Integrative (multifocus, maximizer), and Systemic (combination of Integrative and Hierarchic).

The results of analytical decision styles which evaluate the optimal decision styles mix for a crew of three operators show the preference for integrative, hierarchic, or flexible decision style operators, which is a function of the predicament the operators may be encountering in the control room. The findings of the attribute rating survey, which evaluates operators' optimal decision styles, confirm the previous results from the analytical decision styles model. Moreover, all studies indicate a non-decisive pattern and preference for hierarchic, integrative or flexible decision styles. In other words:

- Small Loss of Coolant Accident (LOCA) -- Integrative or Hierarchic decision style operators.
- Steam Generator Tube Leak (SGTL) -- Integrative or Hierarchic decision style operators.
- Loss of Main Feedwater (LOMF) -- Flexible decision style operators.
- Reactor Trip -- Hierarchic decision style operators.

The results of task data survey, which also estimates the preferred decision styles for small LOCA and steam generator tube leak, indicate the inclination for hierarchic or integrative operators.

Part II: Experimental Studies

The second phase of the project was conducted at the Experimental Breeder Reactor-II (EBR-II) located at the Argonne National Laboratory-West, Idaho Falls, Idaho. Plant operators were asked to respond to a set of plant incident scenarios, which were designed to vary in complexity, on either a Traditional interface or an Ecological interface. The Traditional interface was a computer emulation of the current EBR-II control room console. The Ecological interface was an enhancement of a control room display designed for EBR-II that was based upon the Ecological interface principles (Lindsay, 1990, Lindsay and Staffon, 1988) and the work of Beltracchi (1989 & 1990).

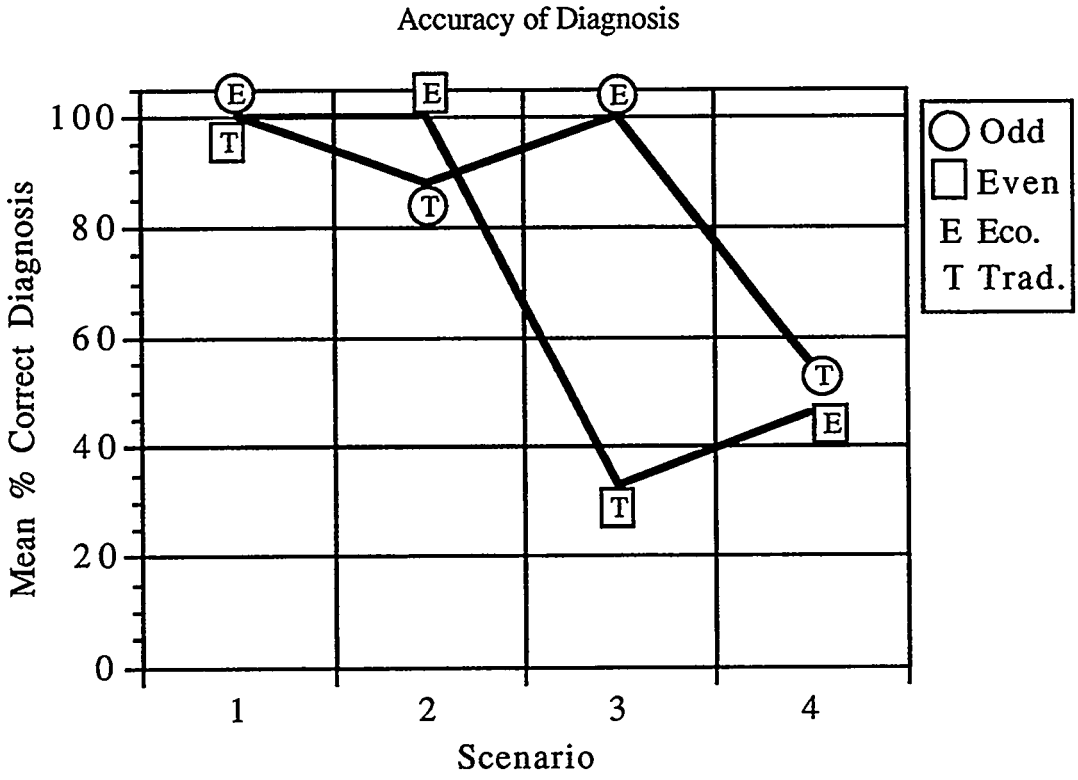
The plant incident scenarios included: 1) a rod run-in to the reactor unit with failed indicator, 2) a run-down of primary pumps, 3) a run-down of the secondary pump with failed indicator, and 4) a simultaneous run-down of one primary pump and run-up of the secondary pump. Performance measures, including recall of plant parameters, event diagnosis, and time to press scram button were collected. Subjective ratings of preference of various aspects of the two interfaces were also collected.

Data were collected measuring the speed of response to the events, the accuracy of event diagnosis and of memory recall of plant parameters, as well as ratings of preference for the two user interfaces. Results indicated that the Ecological interface contributed to improved performance while receiving higher ratings of operator preference. The differences in operator decision style were found to have a significant effect on performance, with Unifocus operators being significantly more accurate in the recall of certain plant parameters.

While the operators as a group generally preferred the Ecological interface to the Traditional interface over numerous measures, this preference was mediated by their decision style. When the operators were categorized by decision style, information satisficers were found to prefer the Ecological interface significantly more than did the information maximizers for handling all of the event scenarios presented. These operators showed a significantly higher preference for the integration of the plant data in the Ecological interface and its support for the comparison of plant parameters. These findings are partially depicted in the two figures on the following two pages.

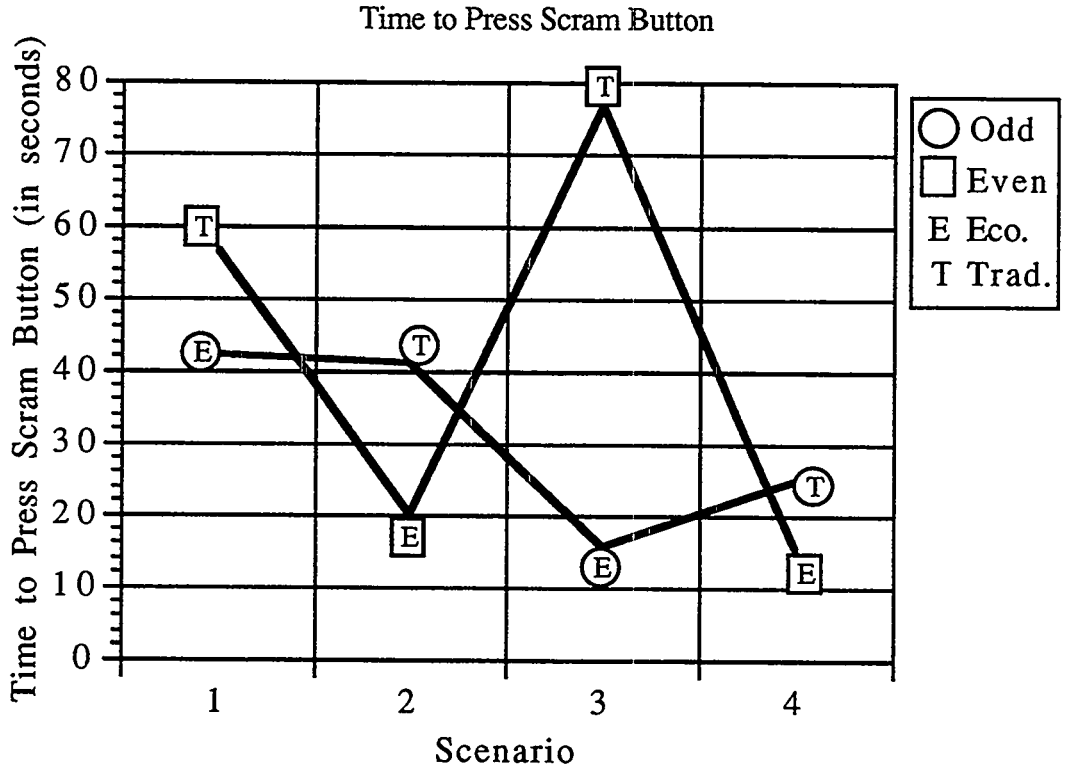
As can be seen in Figure 1, an overall chi-squared analysis found significantly better diagnosis of the event scenarios by subjects using the Ecological interface [X^2=5.23, df=1, p=.02].

Figure 1



As Figure 2 shows, a significant interaction between presentation order and interface contrast was found, indicating faster detection of a major fault by subjects using the Ecological interface [F(1,6)=9.94, p=.020].

Figure 2



The difference in preference was also reflected in the performance of some of the groups of operators. For example, the Systemic operators scored the Traditional interface significantly lower than the Integrative operators in terms of how well it matched their understanding of plant parameters and, in turn, exhibited significantly lower recall of plant parameters when using the Traditional interface. Similarly, the Hierarchic operators, which as information maximizers were less favorable toward the Ecological interface, displayed significantly lower recall of plant parameters when using the Ecological interface.

These results indicate that operator decision style can have important implications for both the acceptance of, and performance with, an Ecological interface. The recall of plant parameters has been cited as an indicator of the degree to which an interface matches the user's mental model of the system represented. Variation in recall performance may indicate that different mental models of the plant are developed by operators using different decision styles. If this is the case, then the design of an Ecological interface must account for these differences in mental representation. This also has implications for the initial introduction of a new interface design into an established plant. Since the operators' mental model of the plant is shaped by the design of the previous user interface, resistance to a new type of representation can be expected. This resistance may be especially acute from information maximizers, which have already developed a particularly intricate mental model of the system.

An analysis of the distribution of decision styles across operator levels showed that plant supervisors were significantly more likely to be information satisficers while plant operators were significantly more likely to be information maximizers. Also, plant supervisors were significantly more likely to be unifocus while plant operators were significantly more likely to be multifocus. Although the Integrative decision style had the highest overall frequency, none of the individuals from this group were plant supervisors. Plant supervisors were exclusively Decisive or Flexible in decision style.

These findings, when looked at in conjunction with the differences found in preference and performance across decision styles, pose a number of important implications. Ecological interface design must take into consideration the different informational needs presented by operators performing these different levels of plant monitoring. This points out the importance of the Ecological interface guideline of presenting information in a form that supports various levels of cognitive processing. In addition, it raises questions concerning the optimal team structure for dealing with various plant events that a more through understanding of the effect of decision styles on performance may help to answer.

Research indicates that different decision styles have a different but predictable tolerance for, and response to, different task dimensions such as complexity, uncertainty and information load. It is expected that those decision styles which are categorized as multifocus (i.e., Integrative and Flexible) will have more options and perform better when responding to events containing high levels of uncertainty. In addition, those with information maximizing styles (i.e., Integrative, Hierarchic and Systemic) experience less strain (respond more smoothly) to high levels of complexity than those with information satisficing styles (i.e., Decisive and Flexible). This is particularly critical during events requiring Knowledge-based reasoning and diagnosis where uncertainty and complexity are typically high. To illustrate this point, consider an individual who has a unifocus, information satisficing style (Decisive) that is required to contend with a Knowledge-based event. This individual will experience a high degree of stress when attempting to diagnose the situation. On the other hand, this kind of knowledge-based scenario is the type of situation where multifocus, information maximizers (i.e., Integrative) would feel comfortable, provided the time pressure was not excessive. On the other hand, a routine situation which

requires a quick decision would be best handled by Decisive (unifocus, information satisficers) as compared to those who are multifocus, information maximizers (i.e., Integrative).

Conclusions

Based on this research it is concluded that:

- Integrated SRK-based information processing model for control room operations is superior to conventional rule-based model.

- Individual decision style of operators and the combination of their styles play a significant role in effective handling of nuclear power plant disturbances. In other words, when there is a 'fit' between the decision style of operators and a particular disturbance, the operators handle the event more effectively.

- Use of the Ecological interface results in significantly more accurate event diagnosis and recall of various plant parameters, faster response to plant transients, and higher ratings of subject preference.

- Decision style of operators have an effect on both operator performance and preference for the Ecological interface. One of important implications is that the ecological interface design must take into consideration the different informational needs of operators performing different levels of plant monitoring.

Acknowledgments

The authors would like to thank Mr. Leo Beltracchi of the Human Factors Branch, Office of Nuclear Regulatory Research of NRC, for his technical advice and oversight during the course of this study. The authors also acknowledge the invaluable support the personnel at Argonne National Laboratories East and West for their contributions to this research project. We are particularly indebted to Mr. Richard W. Lindsay, Ms. Alenka Brown-VanHooser and all of the supervisors and operators at EBR-II plant. This work, however, should not be construed as representing NRC and Argonne views.

References

Beltracchi, L., 1989. Energy, mass, model-based displays, and memory recall. *IEEE Transactions on Nuclear Science, (36)*3: 1367-1382.

Beltracchi, L. (1990, June). *A direct manipulation system-process interface.* Paper presented at Advances in Human Factors Research on Man/Computer Interactions: Nuclear and Beyond, Nashville, Tennessee.

Driver, M.J. (1979). Individual decision making and creativity. In S. Kerr (Ed.), *Organizational Behavior.* Columbus, Ohio: Grid Publishing, Inc., 59-91.

Driver, M.J., Brousseau, K. R., & Hunsaker, P.L. (1993). *The Dynamic Decision Maker: Five Decision Styles for Executive and Business Success.* San Francisco, CA.: Jossey-Bass.

Lindsay, R.W. (1990, June). *A display to support knowledge based behavior.* Paper presented at Advances in Human Factors Research on Man/Computer Interactions: Nuclear and Beyond, Nashville, Tennessee.

Lindsay, R.W. and Staffon, J.D. (1988, October). *A model-based display system for the experimental breeder reactor-II.* Paper presented at the Joint Meeting of the American Nuclear Society and the European Nuclear Society, Washington, DC.

Meshkati, N. (1991a). Human Factors in Large-Scale Technological Systems' Accidents: Three Mile Island, Bhopal, Chernobyl. *Industrial Crisis Quarterly, 5,* 133-154.

Meshkati, N. (1991b) Integration of workstation, job, and team structure design in complex human-machine systems: A framework. *International Journal of Industrial Ergonomics, 7,* 111-122.

Rasmussen, J. (1983). Skills, rules, knowledge: signals, signs, and symbols and other distinctions in human performance models. *IEEE Transactions on Systems, Man, and Cybernetics,* 13:257-267.

Rasmussen, J. (1986). *Information processing and human-machine interaction.* New York: North Holland.

Reason, J. (1990). *Human error.* Cambridge, England: Cambridge University Press.

CURRENT AND FUTURE APPLICATIONS OF PRA IN REGULATORY ACTIVITIES

Themis P. Speis
Deputy Director for Research

Joseph A. Murphy
Acting Director, Division of Safety Issue Resolution

Mark A. Cunningham
Chief, Probabilistic Analysis Branch

James W. Johnson
Probabilistic Analysis Branch

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

INTRODUCTION

Probabilistic Risk Assessments (PRAs) have proven valuable in providing the regulators, the nuclear plant operators, and the reactor designers insights into plant safety, reliability, design and operation. Both the NRC Commissioners and the staff have grown to appreciate the valuable contributions PRAs can have in the regulatory arena, though I will admit the existence of some tendencies for strict adherence to the deterministic approach within the agency and the public at large. Any call for change, particularly one involving a major adjustment in approach to the regulation of nuclear power, will meet with a certain degree of resistance and retrenchment. Change can appear threatening and can cause some to question whether the safety mission is being fulfilled. This skepticism is completely appropriate and is, in fact, essential to a proper transition towards risk and performance-based approaches. Our task in the Office of Nuclear Regulatory Research is to increase the PRA knowledge base within the agency and develop appropriate guidance and methods needed to support the transitioning process.

With regard to operating plants, the majority of the licensees have grown to appreciate the benefits of PRAs in their day-to-day operation of their nuclear facilities. Their motivation focuses on safety, economics, and investments. The individual plant examination programs (IPEs) provided not only safety insights to plant design and performance, but also provided valuable information on plant maintenance and operation. Expanded regulatory application of PRAs is not inconsistent with these objectives.

The NRC established its regulatory requirements to ensure that a licensed facility is designed, constructed, and operated without undue risk to the health and safety of the public. These requirements are largely based on deterministic engineering criteria, involving the use of multiple barriers and application of a defense-in-depth philosophy. PRA methods offer the potential to improve both the efficiency and effectiveness of these regulatory requirements. PRA information and insights have been applied successfully in numerous regulatory activities

and have proved to be a valuable complement to deterministic engineering approaches. This application of PRA represents an extension and enhancement of traditional regulation rather than a separate and different approach.

This paper summarizes past and recent uses of PRA, ongoing PRA related activities, and discusses a transition strategy for expanded usage of PRA in the regulatory decision making process. Expanded use of PRA can help to focus attention on the operational and regulatory issues that are risk significant. Identifying risk significant issues is the first step of the transitioning process. The next step is to identify a process that can take regulations, whether new or revisions of existing regulations, and transform them into performance based or programmatic requirements. The proposed transitioning strategy to risk-based regulation over the next two to ten years includes:

(1) identifying application areas,

(2) developing a regulatory framework,

(3) identifying PRA information needs,

(4) developing guidelines for regulatory applications.

Our goal is to ensure that our regulations are in concert with risk importance and are subjected to periodic reevaluations as we acquire more data and related information and develop better models.

PAST AND RECENT USES OF PRA

PRA methods have been applied successfully in numerous regulatory activities, proving to be a valuable adjunct to deterministic engineering approaches. Two basic policies for reactor regulation established by the NRC (on the basis of PRA methods) were the backfit rule and the safety goals. An example of a major past PRA application is the Systematic Evaluation Program (SEP), in which risk importance was used to assess the significance of deviations from current licensing criteria for some of the oldest operating reactors. PRA methods also were used effectively during the anticipated transient without scram (ATWS) and station blackout rulemakings, and to support the generic issue prioritization and resolution process. Additional benefits have been found in the use of risk-based inspection guides to focus inspector efforts and make more efficient use of inspection resources. The issuance of NUREG-1150, in which the staff took advantage of the technological developments of the 1980s to assess the risk associated with five selected plants, represented a significant turning point in the use of risk-based concepts in the regulatory process. The methods developed for and results obtained from these studies provided a valuable foundation and further enhanced the application of quantitative risk techniques in regulatory decision-making.

More recently, the NRC has relied extensively on PRA techniques to assess the safety importance of operating reactor events and is using them as an integral part of the design certification review process for advanced reactor designs. In addition, the Individual Plant Examination (IPE) program and the Individual Plant Examination - External Events (IPEEE)

program will result in all commercial reactor licensees performing PRAs to identify any vulnerabilities needing attention. The IPE and IPEEE performed on all operating plants are providing a rich source of information on the risk profile of the various plants. One challenge for the future will be to derive as much information and insights as possible from these studies, while recognizing the limitations that come from the use of disparate methods and data. A long term goal is to have all such decisions (such as shutting down a plant, ruling on Tech Spec changes, exemptions from LCOs, new rules, generic issue resolution, etc.) receive an independent assessment of the risk implications and that such assessments be formally included in the deliberation processes.

In summary, PRAs have proved valuable in providing insights into plant design and operation, the relative importance to safety of plant specific characteristics, regulatory issues, and alternative regulatory actions.

The practical problems associated with further progress to risk-based approaches to regulation are significant. In many cases, the methods used in risk analysis are robust and reasonably mature. Research is still needed in some areas, however. Perhaps the most important lie in the areas of common cause failure modeling and operational data use. Common cause failure modeling includes both human reliability and organizational factors modeling. While reasonable methods exist to evaluate the likelihood that an operator will fail to follow procedures under specified circumstances, our ability to analyze the capability of the operating crew to diagnose correctly is still weak. The significance of this is compounded by the fact that mis-diagnosis will likely lead to human actions which were not modeled or anticipated by the PRA analyst. Also, the current ability to determine the effect of organizational influences on operator performance quantitatively is in its infancy, at best.

Improved operational data would permit the estimation of actual train and system unavailabilities which could be used for Maintenance Rule monitoring and maintenance effectiveness evaluations and for numerous risk-based and performance-based regulatory applications including quality assurance and evaluation of low-power/shutdown risk issues. Also, such a common database would provide NRC and industry a consistent source from which safety system performance could be evaluated for both generic and plant-specific issues. Further explorations in these areas are needed.

ONGOING PRA RELATED ACTIVITIES

Today, the NRC is applying PRA techniques, complemented with other quantitative and qualitative techniques, in its licensing decision making processes. Insights from PRAs have led to improved technical specifications, better focused inspection programs, granting of temporary exemptions, non-prescriptive regulations, and other important agency activities, such as the review of advanced reactor concepts. Additional ongoing PRA related activities are discussed below.

IPE/IPEEE REVIEWS

The purposes of the IPE program are to have each commercial nuclear power plant licensee (1) develop an overall appreciation of severe accident behavior, (2) understand the most likely severe accident sequences that could occur at the plant, (3) gain a more quantitative understanding of the overall frequencies of core damage and radioactive releases, and (4) if appropriate, reduce the overall frequencies of core damage and radioactive material releases by modifying hardware and procedures that would help prevent or mitigate severe accidents. This program principally focuses on licensee use of IPE/PRA information. However, the information contained in the IPEs is also of potential benefit to the NRC staff in its regulatory programs.

The review of the IPEs does not imply that the licensee's PRA is acceptable as a basis for licensing actions (such as modifications to technical specifications). The review focuses on the adequacy of the process in ensuring that the program has accomplished its intended objectives. The staff's review, thus far, shows that the IPE program has accomplished its goals. The IPEs were performed by utility personnel 100% or with the support of contractors and substantial utility involvement. All licensees chose to perform a level 1 (and most a level 2) PRA in order to gain an understanding of the most important sequences as well as a more quantitative understanding of risk. The licensee's used their IPE to derive insights regarding plant performance under severe accident conditions and to identify potential plant improvements for reducing the probability of these sequences; in general licensees did (or committed to) implement most of their identified improvements. The challenge ahead relates to identifying how IPEs will be used in regulations and in developing guidance to staff and industry on the submittal review process.

COMMISSION POLICY STATEMENT

In an effort to enhance the use of PRAs within the NRC, the staff is presently drafting a policy on uses of probabilistic assessment methods in nuclear regulatory activities. In part, this policy was stimulated by the NRC's Advisory Committee on Reactor Safeguards' (ACRS) insistence that PRA methods are not consistently applied throughout the agency and that the Commission is not deriving full benefit from the large agency and industry investment in the developed risk assessment methods. The Commission has indicated its support to apply PRAs as one means to ensure consistent, stable, efficient, and predictable regulatory regimes both for the reactor and nuclear materials licensees.

The policy statement integrates the Commission's Principles of Good Regulations, the Commission's policy on Safety Goals, and other regulatory activities pursued within the NRC. The draft policy statement is addressed in a publicly released Commission paper, SECY-94-218. This policy was discussed in an open Commission meeting in August of this year. The Commissioners' comments strongly supported use of PRAs and their intent to address the broad use of PRAs within the agency.

PRA IMPLEMENTATION PLAN

In a companion Commission paper, SECY-94-219, the staff outlined its proposed agency-wide implementation plan for applying PRAs on a daily basis. The implementation plan encompasses the need to improve our capabilities to model certain human performance activities, especially errors of commission and organizational or management issues. In the areas of industrial and medical uses of nuclear materials, for instance, the primary contributor to overexposure is human error. The plan acknowledges and addresses the need for staff data collection and analysis in the nuclear reactor and material licensee activities. Given the dissimilarities in the nature and consequences of the use of nuclear materials in reactors, industrial situations, and medical applications, the PRA Implementation Plan acknowledges that a single approach to risk management is not appropriate. Therefore, the staff will share methods and insights between the disciplines to ensure that the best use is made of available techniques to foster consistency in NRC decision-making. The updated NRC guidelines for conducting Regulatory Analysis will be an important step forward in fostering this agency-wide consistency. To this end, the PRA implementation plan addresses continued development of PRA methods and regulatory decision-making tools and the need to enhance the collection of equipment and human reliability data for all of the agency's risk assessment applications, including those associated with the use, transportation, and storage of nuclear materials.

The NRC will also continue its current activities as outlined in the PRA Implementation Plan including the development of consistent PRA models and methods and will expand the data base on human performance reliability. In addition, the NRC will continue its current activities associated with industry initiatives, including Quality Assurance, Containment Leakage, Motor Operated Valves, and development of a means to establish an equipment reliability and availability database to support the maintenance rule and performance-based regulation.

The staff will continue to work with the Nuclear Energy Institute to identify areas of mutual interest for the use of PRA methods and insights and plans to continue its interactions with the Institute of Nuclear Power Operations (INPO) to improve availability of plant-specific failure data.

RISK-BASED REGULATION

Risk-Based regulation is the use of PRA models and insights to focus licensee and regulatory attention on design and operational issues commensurate with their impact on risk. Risk-Based regulation utilizes risk importance, which is based on PRA technology, to determine effectiveness of regulatory requirements. The term "risk-based regulation" can be interpreted in a variety of ways. Here it encompasses the use of probabilistic analysis as a tool (1) to assist in defining the appropriate parameters for risk-based regulation, and (2) to optimize deterministic requirements which may presently exist. The ultimate in performance-based approaches might be the direct incorporation of probabilistic requirements or quantitative risk criteria into the regulations. However, the state-of-the-art is such that these approaches must be taken with extreme care because of the limitations imposed by lack of plant-specific data

and weaknesses in certain portions of the analytical techniques, particularly those associated with various aspects of human reliability analysis. Our objective is to obtain improved safety and reduced burdens on the NRC regulated community by directing resources to areas that are most safety significant.

TRANSITION STRATEGY

The proposed transition strategy will be an evolutionary process consisting of the following four phases: (1) Identification of application areas, (2) Development of a regulatory framework, (3) Specification of PRA information Needs, and (4) Development of guidelines for regulatory applications. The transitioning process will involve the NRC staff, industry, and the public. The staff will develop the transitioning strategy and solicit comment from appropriate NRC staff and the nuclear industry. The strategy will then be refined and updated as appropriate. NRC has supported research focused on developing a proposed strategy and framework for risk-based regulations and we will now describe our progress and current plans.

APPLICATION AREAS

Regulatory categories have been identified where efficiency and effectiveness can potentially be enhanced by using PRA methods. These categories are also areas where PRA information and insights can be used to transition from prescriptive requirements to more performance and risk based requirements. The regulatory categories identified include: (1) inspections, (2) operator licensing, (3) event investigation, (4) event assessment, (5) generic issues, (6) licensing actions, (7) regulatory effectiveness, (8) industry initiatives, (9) advanced reactor reviews, (10) severe accident closure, and (11) senior management meetings. Each category requires the identification of appropriate PRA information, development of guidelines, demonstrations of potential applications.

REGULATORY FRAMEWORK

In developing a proposed framework, the fundamental objective is to incorporate more explicit risk related criteria into regulations and activities which are directed at controlling risk contributors so that requirements and actions are consistent with the risk importance of the contributors. The most severe requirements and highest resource commitments should be directed at the highest risk contributors. Less severe requirements and lesser amounts of resources should be directed at less important contributors. This can be accomplished by "grading" the risk importance of contributors to risk and then identifying appropriate graded regulatory responses. This proposed process of transitioning to risk-based regulation consist of three basic steps: (1) identify PRA risk contributor, (2) grade risk-importance, and (3) grade regulatory response. Implementation of the process will have the effect of transforming present requirements and practices to more explicit risk-based requirements in a stepwise, evolutionary manner for each application. The risk-based requirements can then be transformed to programmatic or performance based requirements for implementation. When appropriate, present requirements may need to be modified because of their lack of consistency with their associated risk importance.

The above described framework will provide some discipline to the transitioning process and also provides a means to ensure consistency across applications. PRA Information Needs

Core PRA information required to perform risk-based applications include both absolute and relative importance measures and core damage frequency information. The basic importance measures are the risk contributor importance, risk increase importance, and the risk decrease importance measure. For some applications joint importance measures may also be desirable. The importance measures should be provided at the basic component, system, and human error level. Different importance measures are required for different applications. For example, risk-graded importance contributions are appropriate for inspection, operator licensing, and licensing actions, while risk graded increase contributions are more appropriate for event investigation, generic issues, and regulatory effectiveness.

There is also additional methods development needs. One of the more evasive is common cause failure models for equipment, human reliability and organizational factors modeling. There are currently ongoing programs in each of these areas to improve the state-of-the-art. Each activity will require associated data collection activities to support their application in the regulatory decision-making process.

In some applications the scope of the PRA may need to be expanded to ensure coverage of certain risk contributors identified in the regulation. The expanded scope would require methods development to include the risk significance of the contributor in the PRA results.

GUIDELINES FOR REGULATORY APPLICATIONS

The guidelines for regulatory applications should outline the major steps and provide enough detail to permit detailed application specific guidelines to be developed. Decision criteria and the rationale for such criteria should also be included. The criteria must be such that the impact of using the PRA information can be judged. This implies that consideration be given to uncertainty and the criteria translated into a deterministic standard.

The first step of the process is the identification of regulatory application areas. Example areas that have been previously identified include graded quality assurance, technical specifications, and risk-based inspections. Relevant regulations and guidelines would be identified to identify potential risk contributors. If the scope of the PRA includes these risk contributors, appropriate importance measures are extracted or developed from the PRA information base. For example, for the allowed outage time area, the risk effect of a downtime change needs to be extracted from the PRA. For Quality Assurance Requirements, quality assurance activities affecting failure rates need to be identified. Since a PRA does not necessarily include all the contributors which may be of interest for a given application, only those contributors covered by the PRA will be able to be formally evaluated for their risk importance. Risk contributors which are not covered in the PRA will need to be addressed by other means. For a given risk contributor, the interface with the particular regulatory area needs also to be identified.

Criteria for determining and grading the risk importance of the particular PRA contributors needs to be determined. The next step in the process would require a graded regulatory response to be associated with the graded risk importance of the contributor.

A major focus of risk-based applications is to define requirements or actions which are consistent with the risk importance of the contributors addressed by the requirements or actions. To provide the framework for defining risk consistent requirements, current requirements and their stringencies need to be compared to the risk importance of the contributors covered by the requirements. These comparisons, or correspondences, can be used to identify inequities in the requirement stringency versus risk importance. These inequities can then be addressed to make the requirements more risk consistent.

To develop the regulatory requirements versus risk importance correspondence for given regulatory areas, the requirement stringency must be identified and a measure of the requirement stringency defined. More than one measure of the stringency may be appropriate for given regulations. Examples of the requirement stringency measures include surveillance test frequency, associated restrictions or tolerances, resource requirements, and penalties. The final step in the process is to order the requirements according to their risk importance and denote the associated stringencies. For ease of presentations and for further utilizations, the risk importance and/or requirement stringencies can be grouped into categories. This correspondence of risk importance versus requirement stringency will provide the framework for risk-based applications and risk-based improvements involving the regulations and regulatory area.

The final step requires the identification of factors that must be considered in conducting pilot applications as well as a general structure for conducting the pilot. The structure must be detailed enough and provide enough guidance for more detailed applications to be developed for each regulatory category. Consideration should be given to size and duration of any pilot applications to assure with reasonable confidence that the proposed application can enhance the effectiveness of regulatory programs without negatively impacting safety. Checks and assurances should be instituted to monitor performance of risk-based modifications.

One or more pilot programs need to be conducted to obtain hands-on experience in attempting to implement risk-based applications. Specific objectives of conducting pilot programs on risk-based applications include: (1) to develop and demonstrate the process and steps that are involved in carrying out an application, (2) to develop specific procedures for identifying the risk contributors for a given application and for risk grading their importance, (3) to evaluate the resources that are required to implement the risk-graded application, both from a regulatory perspective and an applicant perspective, and (4) to evaluate the impacts of the risk-graded application on plant performance, from both a safety perspective and from an operational perspective. Tasks involved in performing a pilot program have been identified and require procedures for checking and monitoring the performance impacts, regulatory impacts, and plant impacts of the modification.

CONCLUSIONS

The initiatives outlined above are part of an ongoing effort to improve the efficiency and effectiveness of NRC's regulations and enforcement activities. These efforts have been motivated by a desire to eliminate or modify regulations where burdens are not commensurate with their safety significance, and thus free up resources and improve the focus of the body of regulations. Programs that can result in a better allocation of resources for competing risks are worthy of expending staff resources and are consistent with the mission of the agency.

As the nuclear industry matured through the heydays of the 70s, through the troubles in the 80s, and through the improvements in the 90s, so has the NRC. As we integrate the lessons learned, we continue to tailor our programs in the area of risk reduction by focusing on the risk important contributors and optimize operations by focusing our resources on risk important features or activities. We have matured in our understanding and implementation of the Commission's Safety Goals Policy Statement and are proceeding to establish a regulatory regime with a strong foundation for stable and predictable regulatory programs.

Experiences in implementing PRAs have thus far been encouraging. Its continued application in the regulatory and research activities appears fully justified, appropriate, and important as evidenced by staff and Commission support for a clear policy statement. PRA techniques are extensions and enhancements of the traditional regulatory processes. The deterministic approach to regulations, which most regulators are familiar and comfortable with, is fraught with implied elements of probabilities, thus the concepts of safety factors, redundancy, diversity, and the list continues. PRAs complement and enhance the traditional engineering and operational approaches by considering risk in a coherent and complete fashion, thereby providing a method to quantify and, as necessary, adjust the overall level of safety and completeness (or lack there of) of our regulations.

CORE DAMAGE FREQUENCY OBSERVATIONS AND INSIGHTS OF LWRs BASED ON THE IPEs*

S. E. Dingman[1], M. T. Drouin[2], A. L. Camp[1], A. Kolaczkowski[3], J. Darby[4], J. L. LaChance[3], J. Yakle[3]

[1] Sandia National Laboratories
[2] U.S. Nuclear Regulatory Commission
[3] Science Applications International, Corp.
[4] Science and Engineering Associates

Seventy-eight plants are expected to submit Individual Plant Examinations (IPEs) for severe accident vulnerabilities to the U.S. Nuclear Regulatory Commission (NRC). The majority of the plants have elected to perform full Level 1 probabilistic risk assessments (PRAs) to meet the intent of the IPEs. Because of this, it is possible to compare the results from the IPE submittals to determine general observations and "lessons learned" from the IPEs. The IPE Insights Program is performing this evaluation, and preliminary results are presented in this paper. The core damage frequency and core damage sequences are identified and compared for pressurized water reactors and boiling water reactors. Examination of the results indicates that variations among plant results are due to a combination of actual plant design/operational features and analysis approaches. The findings are consistent with previous NRC studies, such as WASH-1400 and NUREG-1150.

BACKGROUND AND OBJECTIVES

On August 8, 1985, the Nuclear Regulatory Commission (NRC) issued a Policy Statement on Severe Accidents regarding Future Designs and Existing Plants (50 FR 32138) that introduced the Commission's plan to address severe accident issues for existing commercial nuclear power plants. In this Policy Statement, the Commission addressed its plan to formulate an approach for a systematic safety examination of existing plants to study particular accident vulnerabilities and desirable cost-effective changes so as to ensure that there is no undue risk to public health and safety. To implement this plan, NRC issued Generic Letter 88-20, in November 1988, requesting all licensees to perform an Individual Plant Examination (IPE) to identify any plant-specific vulnerabilities to severe accidents and to report the results to the Commission. The purpose and scope of the IPE effort includes examination of internal events, including those initiated by internal flooding, occurring at full power. In concert with the objectives of the above NRC Policy Statement on Severe Accidents, a memorandum from the Executive Director of Operations to the Office of Nuclear Regulatory Research in NRC on May 12, 1993, recommended that NRC should publish a World-Class document highlighting the significant safety insights resulting from this program and showing how the safety of reactors has been improved by the IPE initiative.

Seventy-eight IPEs are expected to be submitted to the NRC staff in response to the Generic Letter. The NRC staff is reviewing the IPEs to determine if the licensee met the intent of the Generic Letter. A staff evaluation report (SER) documenting the staff's response is prepared at the completion of each review.

The Generic Letter did not require the licensees to perform a full Level 1 probabilistic risk assessment (PRA). However, the majority of the licensees have elected to do so. Because of this, it is possible to compare results from the IPE submittals to determine general observations and "lessons learned" from the IPE initiative. The IPE Insights Program was initiated to document such safety insights. The emphasis of the program is to search for any potential generic significance arising from plant features, e.g., system

* This work was supported by the U.S. Nuclear Regulatory Commission and was performed at Sandia National Laboratories, which is operated for the U.S. Department of Energy under Contract Number DE-AC04-94AL85000.

design, plant operation, for different classes of plants. The program is also quantitatively assessing the impact of the proposed plant changes and modifications (identified by the licensees from their IPE program) on core damage frequency (CDF) and containment performance. The IPE Insights Program is thus documenting the significant safety insights relative to the CDF and containment performance results. This paper is limited to the CDF findings from the IPEs.

As a summary, Figure 1 shows the key points in the evolution of the IPE Insights Program. The figure also shows the interrelationships between this program and other NRC efforts.

The objective of the IPE Insights program is to document the significant safety insights relative to CDF for the different reactor and containment types and plant designs as indicated in the IPEs. The major insights to be gained include:

- What is the nuclear power industry's own judgment of the CDF risk from operating nuclear power plants?
  - How does the risk compare among and within various plant groups?
  - How does the risk compare against previous risk estimates and the safety goals?

- What is driving the CDF risk?
  - What are the important (significant and nonsignificant) designs, operational features, etc. that increase or decrease risk?
  - How important is the role of the plant operators in determining risk?
  - Are some of the findings (differences and similarities) artifacts of the methodology, assumptions, etc?

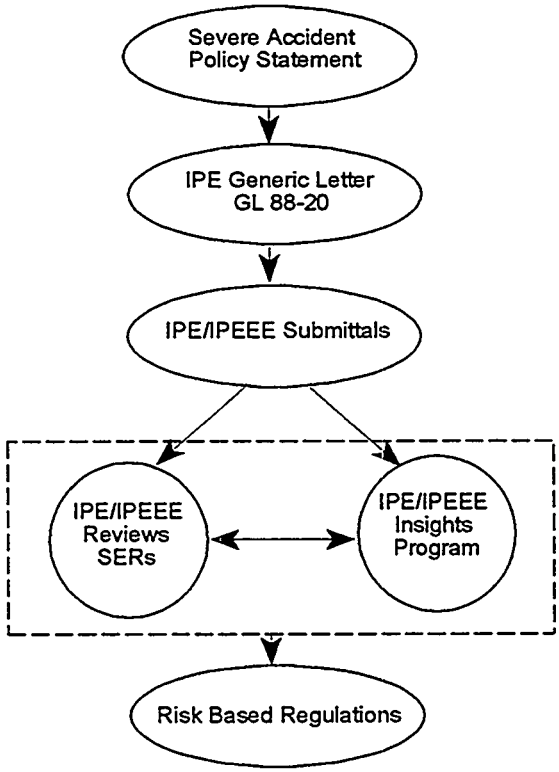


Figure 1. Role of IPEs in NRC Severe Accident Policy

- What is the impact of plant improvements resulting from the IPEs?
  - Has the IPE process had an impact on the safety of plants?
  - How much variation is there among the plant IPE results resulting from implementation of plant improvements?
  - Are there any "generic" improvements that have significantly affected the plant CDFs, or are the plant improvements plant specific?

- How do the IPE models compare?
  - Is there any consistency or standardization?
  - What are the potential viable applications?

ANALYSIS OVERVIEW

To accomplish the program objectives, the IPE/IPEEE Insights Program is composed of four key tasks, as shown in Figure 2:

1. Develop insights related to core damage frequency and its drivers;
2. Develop insights related to containment performance;
3. Examine the impact of plant improvements that were noted in the IPEs; and
4. Address and compare the modeling approaches used in the IPEs, and how those approaches can affect the potential viable applications of the IPEs.

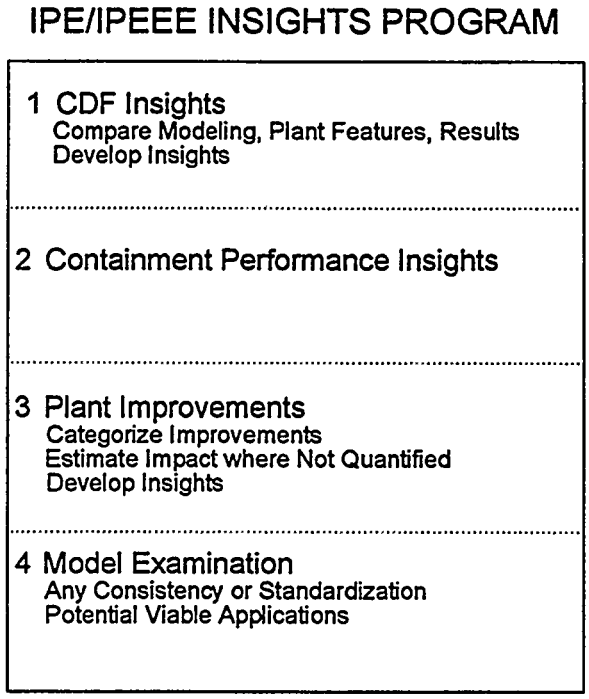


Figure 2. Tasks in IPE/IPEEE Insights Program

This paper presents the approaches being used in and preliminary results from the IPE Insights Program for the first of the four tasks. The approach used to perform the task is summarized in the next section of this paper, followed by a summary of the IPE CDF results, CDF drivers, and preliminary CDF-related insights. The IPE treatment of human actions is discussed in another paper at this conference .

This program is developing insights related to the core damage frequency **as reported in the IPE submittals**. The correctness of the IPE modeling is not addressed here because it is being considered in the NRC staff reviews that are documented in SERs. The insights are limited to internal initiators and internal flooding events at full power. Other modes of operation, such as shutdown, are not considered in the IPE initiative. Some licensees have reported additional external events results, but they are not reviewed in the scope of this work. However, the IPE/IPEEE Insights Program will examine external events implications at a later time.

The IPEs reflect plant conditions at a "snapshot" in time. The licensees have all indicated that they are planning to make improvements to either plant systems/configurations or operating conditions. These are the plant improvements being examined for task 3. In some cases, the IPEs have taken credit for these changes, while in other cases they have not. This variability introduces nonuniformity when comparing the reported plant results, and the IPEs do not provide adequate information to fully account for these differences (i.e., to "normalize" the results). The insights regarding CDF (for task 1) do not attempt to "normalize" the results to account for this concern.

TECHNICAL APPROACH

The approach used to derive safety insights from the IPE submittals regarding core damage frequency results is summarized in this section. A three-step process was used. First, the results from the IPEs were identified and categorized. Second, support information that was believed to be important for explaining commonalities and differences in results among the IPEs was identified. This included information on plant characteristics, the methods and data used in the IPEs, and the assumptions that were made in the analysis. Third, the information obtained in the first and second steps was evaluated and assessed so that global perspectives on the IPE results could be gained.

Developing these findings involved a considerable effort in comparing plant results, design information, and analysis information. To facilitate this, NRC's IPE database, which was developed to store information from the licensee's IPEs, was used. This information includes plant design, CDF and containment performance information. It was also necessary to gather supplementary information from the IPEs so that commonalities and differences in IPE results could be explained. The desired information was not always contained in the submittals, which limited the insights that could be drawn.

The plants were categorized in various ways in order to gain insights from the IPEs regarding commonalities and differences within and across logical groupings of plants. The first grouping is a breakdown of the plants in terms of whether a plant is a Boiling Water Reactor (BWR) or a Pressurized Water Reactor (PWR). The BWRs are further grouped by major model and containment type: BWRs 1, 2, or 3 with isolation condensers and Mark I containments as a group; BWRs 3 and 4 with Reactor Core Isolation Cooling (RCIC) and Mark I containments as a group (a few of the BWRs 3 and 4 with RCIC have Mark II containments, and are included in this group); BWR 5s with Mark II containments; and finally, BWR 6s with Mark III containments. For the PWRs, the first grouping is by vendor (i.e., Westinghouse,

---

* J. A. Forester, "Human Event Observations in the Individual Plant Examinations."

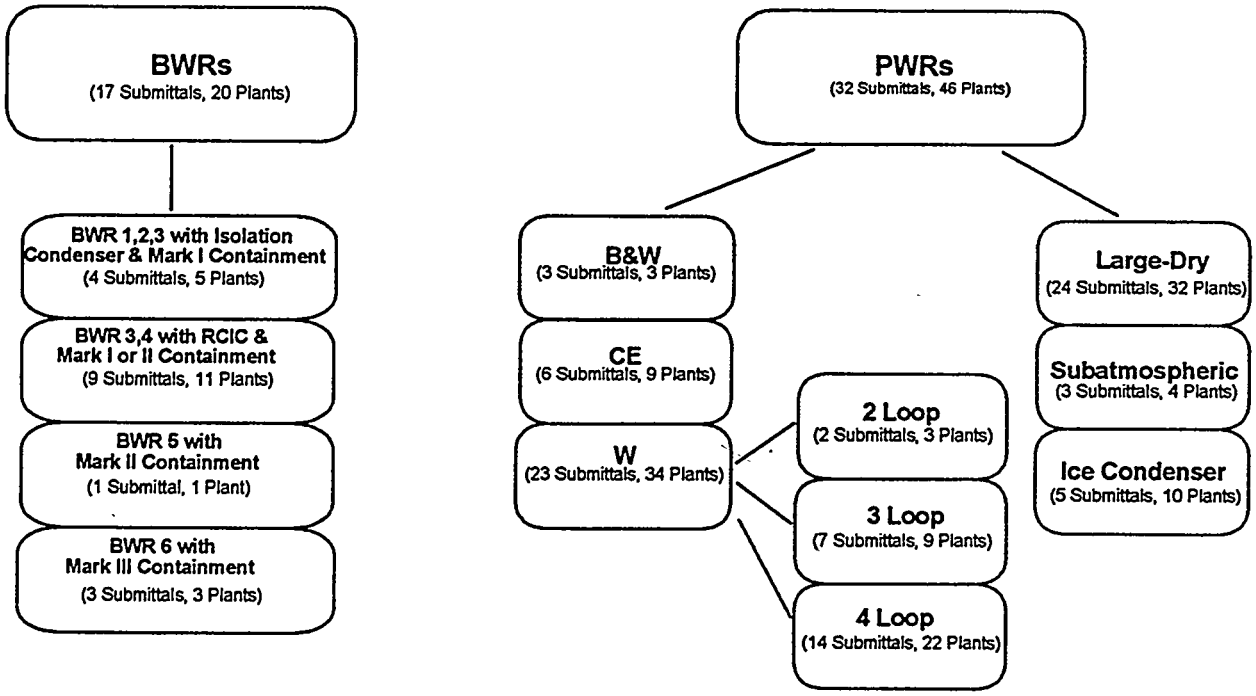


Figure 3. Plant groupings

Combustion Engineering, or Babcock and Wilcox). The Westinghouse plants are further broken down into groups based on the number of coolant loops the plant has (i.e., 2, 3, or 4 loops). Additionally, a separate grouping of all PWRs is made by containment type (i.e., Large Dry, Ice Condenser, or Subatmospheric type containment). These various plant groupings are summarized in Figure 3.

Step 1: Identification and Categorization of IPE CDF Results

For the first step, identifying and categorizing the IPE CDF results, a tiered approach was followed. The results were first examined at a high level, followed by a systematic progression to more detailed levels. The CDF results were examined first, followed by sequence level results, and then the dominant contributors to those sequences.

Tier 1 - Plant Core Damage Frequency

For a Level 1 PRA, the outcome that provides an overall comparable insight into the safety of a nuclear power plant is the plant CDF. As a result, Tier 1 is a comparison of the CDF (either mean or point estimate, whichever was provided in the submittal) across the plants and subgroups of plants.

The first level of insights comes from a comparison of the CDF for each of the plants to be considered in this program. The result of this comparison was summarized by plotting the CDF mean, median, and the individual estimates for the entire population of plants reviewed in this program. This comparison provides insights into the spread and weighting of the CDF values representing all the reviewed IPE submittals. Next, the collective set of CDF values within each of the groups identified above was summarized by

plotting the CDF mean and the individual estimates for all plants identified as belonging within each group (e.g., all BWRs, all BWR 5s, etc.). The results were then compared to determine the variations that exist among and within the plant groups.

Tier 2 - Accident Sequences

The general insights gained from comparing the CDFs for the various plants and groups of plants were further enhanced by examining the individual accident sequences driving the overall CDF for each plant. It must be recognized that there can be a variety of accident sequences that can potentially dominate the CDF and these sequences can be plant specific. Also, the way an accident sequence is defined can vary from IPE to IPE. Typical approaches for defining accident sequences include the following:

- functional [in terms of failed functions resulting in core damage, such as reactor coolant system (RCS) inventory control or heat removal], or
- systemic (in terms of failed systems that lead to core damage), or
- a combination of these two.

Hence, for this program, a standard set of sequence definitions needed to be derived. Once the sequence definitions were derived, all of the IPE-identified dominant accident sequences could be classified into these "standard" sequences for proper comparison. It would be desirable to have sequence descriptions that included summary descriptors such as the type of initiator, timing of core damage, etc. However, this information was not reported in many of the IPE submittals, while other submittals contained such a detailed level of sequence reporting that a very large number of sequences were needed to represent the bulk of the CDF. Because of these limitations, the comparisons among IPEs were based on a higher level sequence description. These summary sequences are listed in Table 1.

The sequence results were compared for the plant groups defined in Figure 3. For each plant group and for each sequence group identified, both the sequence CDF and the percent contribution to the total CDF were reported. The information was summarized by plotting the mean and the individual estimates for all plants within a particular group. The results from this stage of the program allowed insights to be gained regarding how the dominant accident sequence types and their relative contributions vary (or are similar) within and across plant groups.

Table 1. Summary Sequences

SBO - Station Blackout
ATWS - Anticipated Transient Without Scram
DHR - Transients with Loss of Containment Heat Removal (BWRs only)
T - Other Transients
LOCA - Loss-of-Coolant Accidents
FLD - Internal Flood Initiators
R - Vessel Rupture
V - Interfacing Systems LOCA
SGTR - Steam Generator Tube Rupture (PWRs only)

Tier 3 - Dominant Contributors

After the dominant accident sequences were examined for each of the plant groups, the dominant contributors to the most significant sequence types were examined to enhance the insights gained thus far. As with the sequences, variability among the IPEs on how dominant contributors are identified had to be addressed. For example, some submittals only identify dominant contributors to the total CDF, while other submittals identify dominant contributors for each of the accident sequences. In addition, some submittals report contributors at the system level while other submittals report contributors at the component level.

The dominant contributors were identified for the most significant summary accident sequences. When sufficient detail was provided, the form of the identification was specific (i.e., the system in which the failure occurred was identified; the failure was identified as a component failure or a human error; and the failure mode was identified).

For the most significant summary sequences and for each plant group, a listing of each of the dominant contributors that were identified was provided. This listing identified which dominant contributors were contributing to which accident sequences and also which plant groups. This allowed the determination of the relative level of commonality among the contributors within each plant group that make the plants vulnerable to this type of sequence.

Step 2: Identification and Categorization of IPE Methods, Data, Assumptions

The second step in the process of deriving safety insights consisted of identifying and categorizing the methods, data, and assumptions used in the various IPEs. This information was collected so that it could be used to determine possible reasons for similarities and differences of IPE results (which were identified through step one).

The necessary information included both actual plant characteristics and the representation of the plant in the IPE analyses. This information provided some of the issues and potential factors (differences in design, methodology and assumptions) necessary for drawing generic insights from the IPE results, and determining the impact of actual plant characteristics versus analyses characteristics. This information was not available for all cases, which limited the ability to fully explain differences in results.

Similarly, to determine the impact of analysis assumptions on the results, information was needed regarding methods used and assumptions made in areas that could significantly impact the results. Examples include the method used in performing the Human Reliability Analysis (HRA) and assumptions regarding continued operation following battery depletion.

Step 3: Examination for Generic Implication

In the first two steps of this process, an attempt was made to simply summarize, categorize, and compare the IPE results. The third step was to attempt to identify the plant commonalities and differences that cause the results to be as they are.

This examination was focused on selected sequences and issues, rather than on a comprehensive evaluation of all possibilities. To identify which sequences and issues to address, the results from the CDF, accident sequences, and dominant contributors were first reviewed, and based on this review, "differences of interest" were identified. This predominantly involved differences in dominant sequence frequencies among various plant groups as well as the spread in frequencies within individual plant groups. If a large variation in sequence frequencies was noted among or within plant groups, the reasons for the variation were explored. In addition, the sequences with the greatest contribution to CDF for the

particular plant groups were investigated to attempt to determine the factors that most heavily influenced the results.

Reasons for the "differences of interest" were explored by correlating the results with the factors that should have the greatest impact on the results. These factors were identified by examining the dominant contributors to the sequences. The sequence frequencies were then plotted against the factors of interest, and these plots were examined to determine whether any single factor had a large impact on the results. In some cases, outliers were also examined to determine if there were specific factors that caused them to vary from the other plants in the group. Some preliminary results are given in the next section of this paper.

SUMMARY OF IPE RESULTS AND PRELIMINARY INSIGHTS

Figure 4 shows the CDF for the 49 IPEs (representing 66 plants because of multiunit sites) that have been examined to date for this program. Individual plant results are shown by the diamonds in the plot, with the results grouped for the 66 light water reactor (LWR) plants, the 46 PWR plants and the 20 BWR plants. The highest and lowest CDFs reported are approximately 3E-4 and 2E-6, representing a factor of about 150 between the highest and lowest values. The BWRs generally have lower CDFs than the PWRs, with the mean CDF for the PWRs being about a factor of four higher than the mean CDF for the BWRs. However, the spread in the results is large enough that many of the individual PWR CDFs are lower than individual BWR CDFs.

The CDFs were also examined for the various plant groups described above. The differences in mean CDFs among plant group were less than the variations in CDF among the individual plant groups.

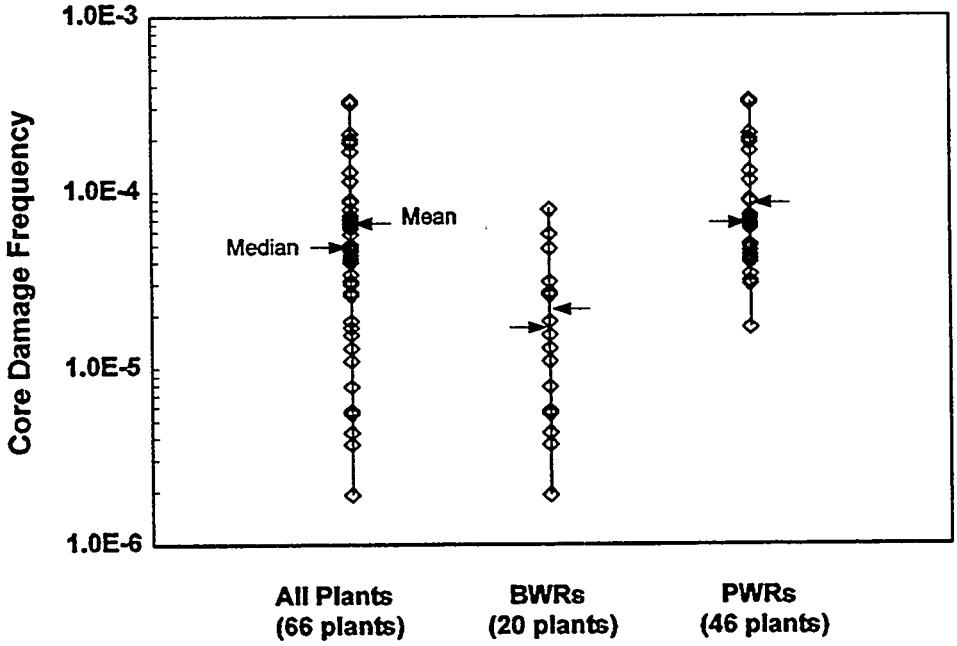


Figure 4 Comparison of BWR and PWR CDF Results for Internal Events

The results for the summary sequences are shown in Figures 5 and 6 for the PWRs and BWRs, respectively. Each figure contains a plot of the individual plant sequence CDFs and a plot of the percent contribution of the sequences to the plant CDFs. The sequence contributions were obtained from summary information in the IPEs. In most cases, the IPE results were reported in a manner that allowed us to determine contributions for the summary sequences, but in some cases, it was not possible to determine the contribution for a particular summary sequence. We included such plants in the comparisons, but only for the information we were able to obtain from the submittal. As a result, the number of plants represented in the various summary sequences is not uniform.

The dominant sequences for PWRs are SBO, ATWS, T, LOCA and FLD. The steam generator tube rupture, bypass and vessel rupture contributions are much smaller. As shown in Figure 5, no single sequence appears as overwhelmingly dominant for the bulk of PWRs, indicating that the IPEs have not identified any generic problem that would dominate the risk for PWRs. The spread in plant results, both in terms of frequency and fractional contribution, is fairly large within all of the sequences, and is larger than the variation in means among the summary sequences. The spread in the CDF is about two orders of magnitude for SBO, T, and LOCA, with means in the range 2E-5 to 3E-5. The ATWS and flood sequences have a much larger spread, varying from a negligible contribution to 4E-5 and 7E-5, respectively. The means for the ATWS and flood sequences are about an order of magnitude lower than the means of the other three summary sequences. The plants are spread fairly uniformly throughout the range for each sequence except that the ATWS and flood sequences each have a high outlier plant.

The fractional contribution to total plant CDF also varies considerably within most of the sequences. For station blackout, the contribution varies from about 5 to 60%; for transients, the contribution varies from 5 to 85%; for LOCAS, the contribution varies from 10 to 55%; and for floods, the contribution varies from negligible to 30%. The variation for ATWS in terms of fractional contribution is much less. Excluding one outlier plant with a contribution of 20%, the remaining plants have ATWS contributions of less than 10%.

Figure 6 shows the ranges of CDFs for each accident class, and the percentage contributions to the overall plant CDF by accident class for the twenty BWRs. Across all the BWRs cited in this paper, SBO, T, and DHR accident sequences are typically the dominant contributors to the CDF. Over the whole group, these three classes of accident sequences combine to represent about 82% of the total CDF, with ATWS contributing about another 10% to the CDF. The mean CDFs for SBO, T and DHR sequences are in the range of 4E-6 to 9E-6, and the mean ATWS CDF is 1E-6. The other classes of accident sequences (i.e., LOCA, FLD, R, and V) generally tend to contribute very little to the CDF (8% all together).

The spread in the BWR sequence results is much larger than for the PWRs. Typically, the high and low CDFs for a particular sequence vary by about three orders of magnitude. In terms of percent contribution, the three dominant sequences (SBO, T, DHR) vary from a negligible contribution to about 80 - 90%. The variation in sequence contribution to CDF within the other sequences is much less, with ATWS varying from negligible to about 40%, and the remaining sequences generally falling below 20%.

The sequence results were also examined for the various plant groups described above. Generally, the differences among plant groups in mean sequence CDFs and fractional contribution to plant CDF were less than the variations observed within the individual plant groups.

The IPE Insights Program is currently investigating the reasons for the observed differences in plant CDF and sequence CDF results. Preliminary results indicate that the variations are due to multiple influences. In general, the differences in results are due to the combined effect of plant design/operational characteristics and differences in IPE modeling and assumptions. To date, no single factor has been found whose variation can explain the observed difference in sequence CDFs.

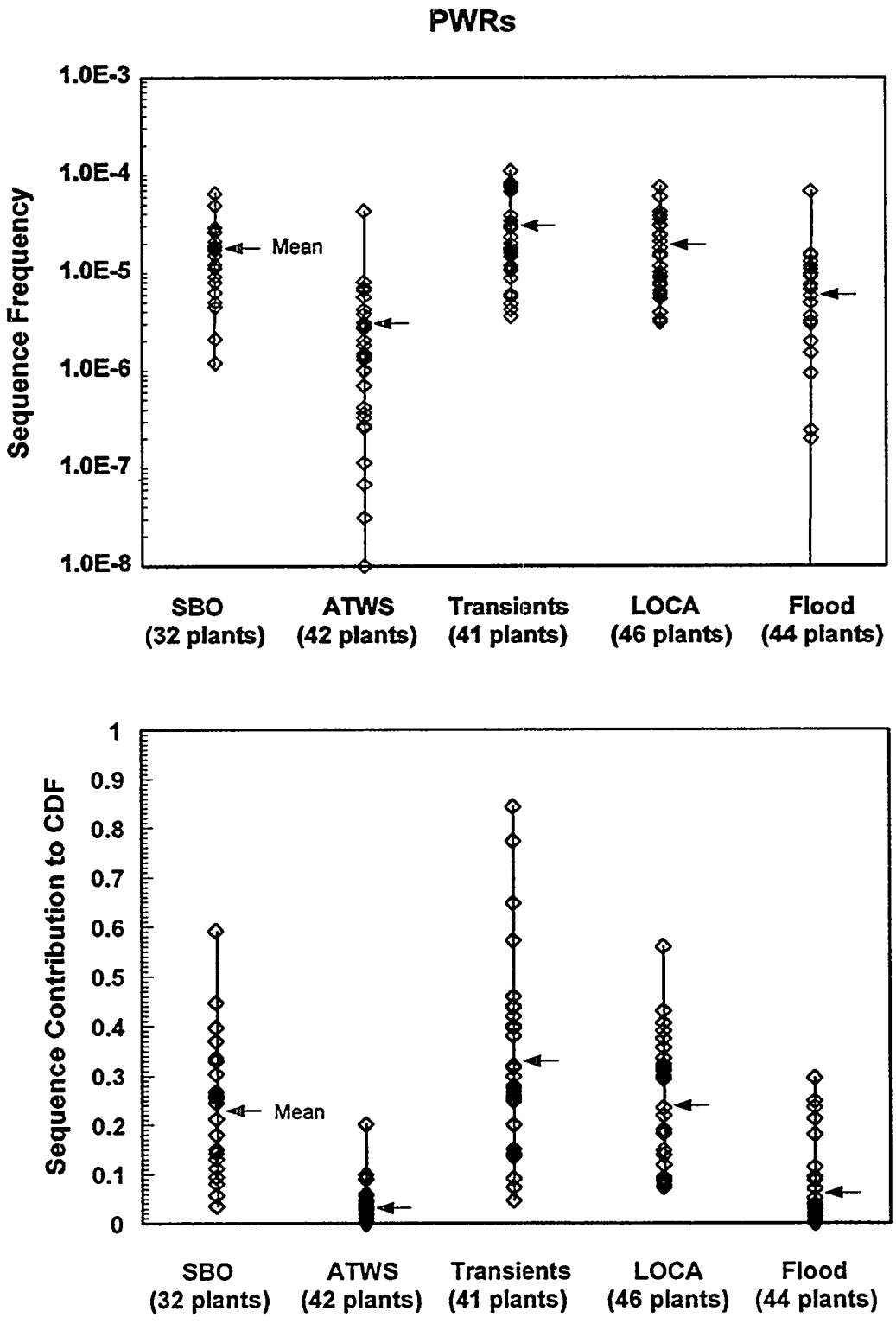


Figure 5 PWR Accident Sequence Frequencies and Contribution to Plant CDF

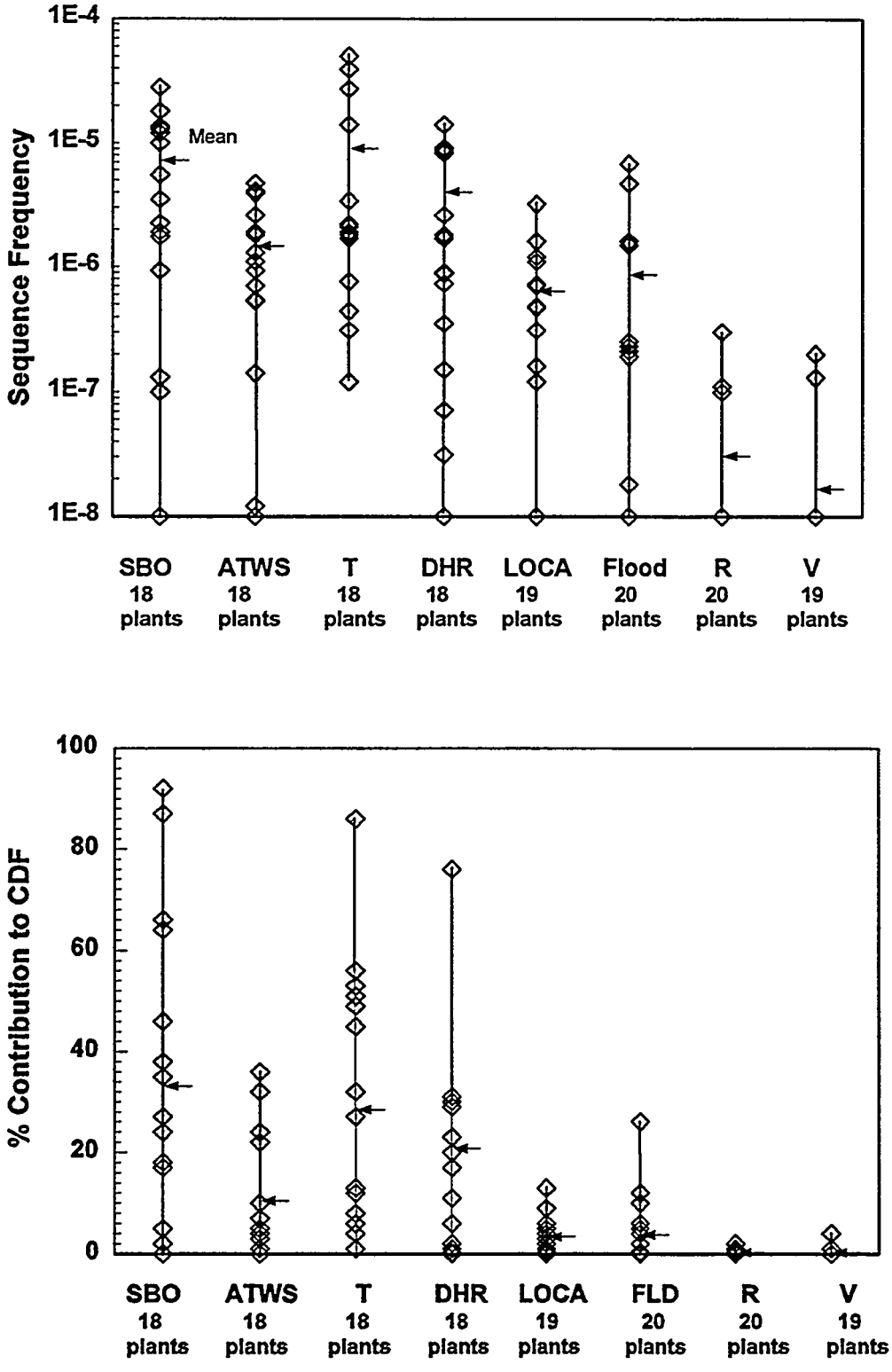


Figure 6 BWR Accident Sequence Frequencies and Contribution to Plant CDF

Figures 7 and 8 show examples of the influence of a variable on the sequence CDF. Figure 7 shows a scatter plot of the SBO CDF for PWRs plotted against the battery life, and Figure 8 shows the ATWS CDF for BWRs plotted against the probability that the operator fails to manually initiate standby liquid control (SLC). Neither factor can account for the observed variation in sequence CDFs. This tendency is typical for all comparisons that have been made in the IPE Insights Program. In general, the variation in results is caused by a combination of factors.

SUMMARY

The IPE Insights Program has been established to gain safety perspectives from the IPE results. To date, the plant CDF, sequence CDFs and dominant contributors have been identified (to the extent possible from the IPE submittals) and categorized. On average, the PWR CDFs are larger than the BWR CDFs, but the individual plant results vary considerably. Examination of the results indicates that variations among plant results are due to a combination of actual plant design/operational features and analysis approaches.

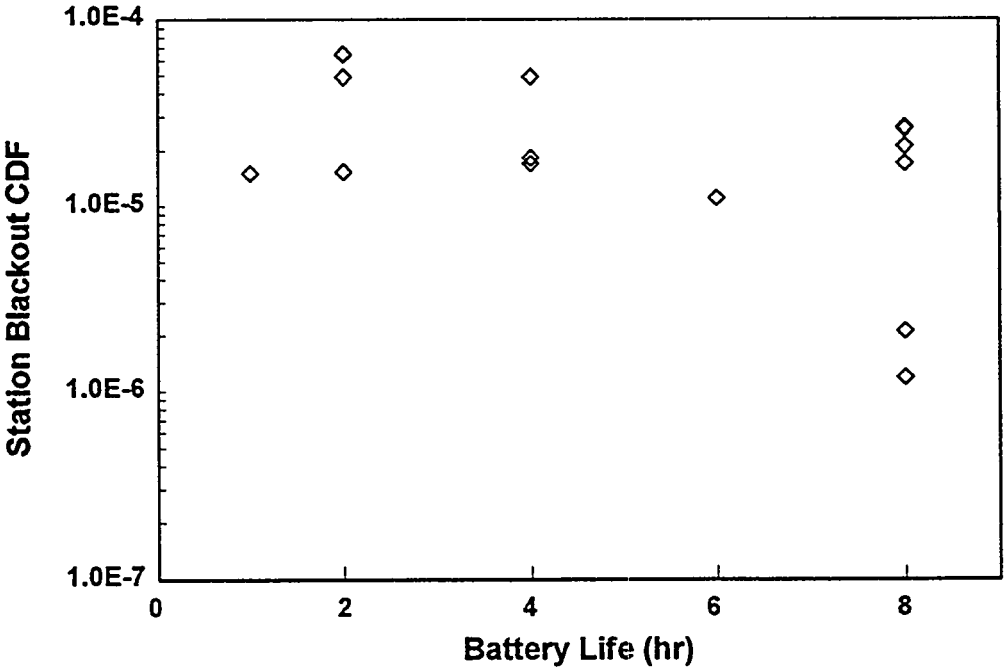


Figure 7 Dependence of PWR SBO CDF on Battery Life

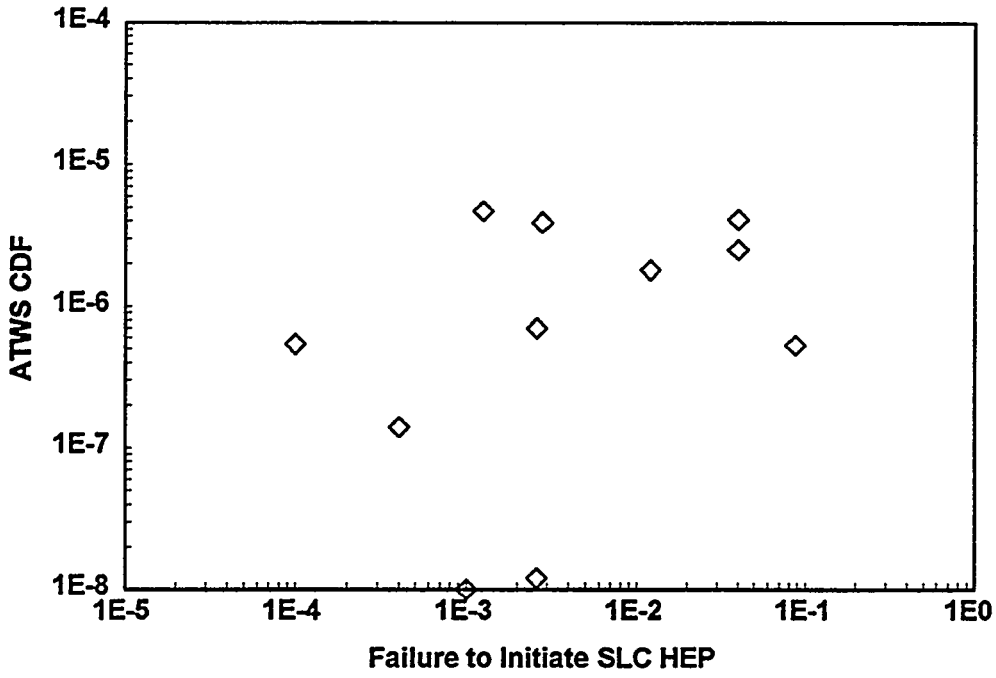


Figure 8 Comparison of BWR ATWS CDF to SLC HEP

Perspectives on Containment Performance Improvement Based on the IPEs[1]

J. R. Lehner, C. C. Lin and W. T. Pratt, Brookhaven National Laboratory
T. S. Su and M. Drouin, Nuclear Regulatory Commission

ABSTRACT

Generic Letter 88-20, "Individual Plant Examination (IPE) for Severe Accident Vulnerabilities - 10CFR 50.54(f)," was issued by the NRC on November 23, 1988. In addition to assessing the core damage frequency from severe accidents, licensees were requested to report the results of their analyses regarding containment performance. Supplements to the Generic Letter forwarded technical insights obtained by the NRC staff through its Containment Performance Improvement (CPI) program. At this time, most of the IPEs have been submitted by the licensees. In a follow-on effort to support regulatory activities, the NRC staff with assistance from Brookhaven National Laboratory, has initiated a program involving a global examination of the containment performance results documented in the IPEs. The objective is to identify insights of potential generic safety significance relative to plant design, operation and maintenance, as well as to assess response to the previously forwarded CPI insights. The containment performance results of the IPEs are being categorized for commonalities and differences for different reactor and containment types. Preliminary results show that not only differences in plant design but also the methods, data, boundary conditions, and assumptions used in the different IPEs have a major impact on the containment performance results obtained. This paper presents preliminary results regarding the differences in containment performance observed in the IPEs and discusses some of the underlying reasons for these differences.

1. Introduction

Generic Letter 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities - 10CFR 50.54(f)," was issued by the NRC on November 23, 1988. U.S. licensees were requested to conduct an Individual Plant Examination (IPE) in order to identify potential severe accident vulnerabilities at their plant and to implement cost-effective plant improvements to reduce or eliminate these vulnerabilities. Subsequently, 4 supplements to GL 88-20 were issued and Supplement 1 and

[1] Work performed under the auspices of the U.S. Nuclear Regulatory Commission

Supplement 3 forwarded technical insights obtained by the NRC staff through its Containment Performance Improvement (CPI) program. These insights were considered important enough by the staff to bring to the attention of the licensees for use, as they deemed appropriate, in the IPEs which they were preparing. Coupled to their level 1 results, licensees were requested to report the results of their analyses regarding containment performance. This included results related to:

1) the general methodology used,

2) plant data and plant features,

3) plant damage states,

4) models and methods used in the accident progression analysis,

5) containment failure characterization,

6) containment event trees and their end states, and

7) radionuclide release characterization.

At this time, most of the IPEs have been submitted by the licensees. In a follow-on effort to support regulatory activities, the NRC staff with assistance from Brookhaven National Laboratory (BNL), has initiated a program involving a global examination of the containment performance results documented in the IPEs. The objective is to identify insights of potential generic safety significance relative to plant design, operation and maintenance, as well as to assess response to the previously forwarded CPI insights. The containment performance results of the IPEs are being categorized for commonalities and differences for different reactor and containment types. Preliminary results are discussed below.

It should also be noted that under a related program BNL has developed an IPE Database[1] which captures important information regarding core damage frequency and containment performance from each IPE submittal.

2. Approach

The objective of a systematic review of the IPE submittals is to examine and compare the reported containment performance results for generic implications (e.g., safety significance and non-significance). The idea is to catalogue variability among types of plants as well as plant to plant variability in containment performance, and to identify the reasons for the variability. Obvious initial categories for comparison purposes are the six containment types found in domestic nuclear plants, i.e. BWR Mark I, Mark II, and Mark III containments and PWR large dry, subatmospheric, and ice-condenser containments. Subcategories or other groupings of interest are expected to arise as the examination and comparison develops.

To accomplish this goal of obtaining reliable global insights several steps are necessary:

a) The containment performance results of the IPEs must be identified and categorized for commonalities and differences relative to reactor and containment types and various plant designs.

b) The methods, data, boundary conditions and assumptions used to obtain these results must be identified and categorized as well, so that one can determine the extent to which these items contribute to the differences and commonalities of classes of plants.

c) Using the results of (a) and (b) above, one can obtain global or generic implications about the containment performance of plants while allowing for the distortions resulting from IPE-to-IPE variability.

The drawing of inferences and insights regarding containment performance is likely to be best accomplished by using steps (a), (b) and (c) in an iterative manner.

An added complication in accomplishing these steps is the fact that the level 2 analyses contained in the IPE submittals have considerably variability. For example, no uniform definition of plant damage states is used. Instead, such definitions are left up to the individual submittal. Besides PDS definitions, the definitions of release classes and source terms are unique to individual IPEs and it is in general unlikely that entire plant damage states or release classes are similarly defined in the IPE submittals being compared. Initially, common parameters need to be found that can reasonably be used to compare containment performance characteristics such as:

- Dominant plant damage states
- Dominant containment failure modes
- Conditional probability of various containment failures
- Source term releases

To obtain global insights on containment performance a two-pronged technical approach is being applied which uses information already contained in the level 2 part of the IPE Database[1] on the one hand, and obtains additional information from direct further review of the level 2 analyses of the IPE submittals. These two sources of information are being used in a complementary way. Broadly speaking, the IPE Database can be used to quickly pinpoint differences in containment performance and the areas where those differences occur; while a detailed review of the submittals, especially in those areas pointed to by the Database information, can highlight the reasons for those differences, i.e. due to assumptions made, phenomena considered, plant features, etc. Important analysis features are being determined for each submittal, including:

a) how was the accident progression analysis performed (i.e. large or simple containment event trees, etc.)

b) how were containment phenomena handled (i.e. how was direct containment heating, liner melt-through, etc. considered)

c) what was assumed for containment strength

d) how were source terms obtained (MAAP[2] runs, etc.)

e) how were decontamination factors treated

f) any plant unique containment features

As indicated by the list of features to be considered, given above, this study looks at how each submittal handled the various phenomena, deemed possible during the course of a severe accident, which could challenge the containment. The audit considers whether these phenomena were addressed by established methods, such as those of NUREG-1150[3] for instance, or if novel procedures were used. Methods employed for obtaining source terms are also scrutinized to see if actual MAAP[2], MELCOR[4], or other calculations were made, and under what assumptions, or if source terms were obtained through analogy and comparison with previously existing results from other analyses.

Below some preliminary results are presented using the approach outlined above.

3. Preliminary Results

Two sets of preliminary results are presented. The first is an overall, or global, comparison of early failure frequency among all currently used U.S. containment types. The second set of results shows comparisons of some containment performance parameters among plants with similar containment types.

3.1 Global Comparisons

The first set of preliminary insights on containment performance involve containment early failure and bypass frequency (CEFF). Containment early failure or bypass are two types of failures that could result in a large release of radioactive material to the environment. The timing of containment failure is very important in terms of radiological consequences. If the containment remains intact for a longer time, the operator will have time for protective actions to prevent radioactive material from being released to the environment (as part of accident management strategies). Therefore, the containment early failure or bypass frequency is a key measure for containment performance.

At this preliminary stage, the information about the containment early failure or bypass frequencies was extracted from the summary section of each IPE submittal without elaborate analysis for its assumptions or boundary conditions; that is, without independently confirming the licensees' calculations or re-baselining them using a common methodology or containment failure definition. (These frequencies do not include the frequencies associated with "small" failure or release as they do not tend to dominate risk.) The term "large" and "small" are defined by the licensees and vary from plant to plant. Therefore, as noted under the "Approach" discussion, the information is subject to interpretation of the licensees own definition of certain key parameters. These parameters include plant damage states, timing of containment failure, and magnitude (i.e., "small" and "large") of source terms. This lack of uniformity in defining these key parameters has made meaningful comparisons between plants in terms of containment performance difficult.

In addition, it should be pointed out that the CEFF is not the conditional containment early failure probability (CCEF), but the product of the core damage frequency (CDF) and the CCEF. However, due to the lack of consistency of the information in the IPEs, the CEFF was used for the present preliminary results. Normalization of these various parameters is being pursued as part of this ongoing program. For now, the following information should be considered as quite preliminary and only as an illustration of the potential utilization of the IPE database and the IPE submittals.

The CEFFs for 62 IPEs are shown in Figure 1. The results are presented in terms of the mean and the median as well as the 95th and 5th statistical measures of the CEFFs reported in the IPEs. As indicated, the mean CEFF for the 62 plants is 4.5E-6 per reactor year (ry) with a mean CEFF of 3.8E-6 per ry for 20 BWRs and 4.9E-6 per ry for 42 PWRs. These mean CEFFs are below the 1E-5 per ry release frequency which can serve as a conservative surrogate for the prompt fatality quantitative health objective (QHO)[5]. It is noted that the CEFF for the 62 plants results in a broad range, which varies from a high value of 2.2E-5 per ry to a low value of 3E-8 per ry. Further categorization should help in the understanding of the reasons for this variation.

In Figure 2, the individual CEFFs for the different BWR containment types are shown. These range from a high value of 2.2E-5 per ry to a low value of 3.8E-8 per ry with a mean value of 3.8E-6. The difference between the high and low CEFFs is three orders of magnitude and at least an order magnitude for each containment type. The mean CEFF for each containment type falls below 1E-5 with Mark I BWRs having the largest contribution.

In examining each BWR containment type, there appears to be "outliers" for each type. One Mark I BWR appears to have a CEFF two orders of magnitude lower than the "group" of CEFFs and three plants with CEFFs almost an order of magnitude higher. One Mark II BWR appears to have a CEFF two orders of magnitude lower. For the Mark III BWRs, one plant appears to have a CEFF an order of magnitude lower. This difference could be more of a result of the lower CDF than design features related to containment performance. The causes for the differences are being explored.

The individual CEFFs for the different PWR vendor types (i.e., Westinghouse, B&W, and CE) and containment types are shown in Figure 3. As indicated, the CEFFs range from a high value of 1.8E-5 per ry to a low value of 4E-8 per ry with a mean value of 4.9E-6. In examining the PWR groups, the mean CEFF for each falls below 1E-5. The sub-atmospheric plants have the largest mean with a value of 8.6E-6.

In examining the PWR groups and individual CEFFs, there appears to be plants at the low range outside of the "group." For CE and B&W plants, an order of magnitude difference is seen while two orders of magnitude is seen for the Westinghouse and large dry PWRs.

The overall results in regard to CEFFs indicate that CEFFs for BWRs and PWRs are not vastly different (less than a factor of 1.5 difference can be seen between the mean values, Figure 1). Although, the level 1 IPE results show that the mean CDF for the BWRs is almost a factor of 4 lower than the mean CDF for the PWRs, the CCEFs tend to be higher for BWRs due to their smaller containments. The CEFF reflect the combination of both CDF and CCEF.

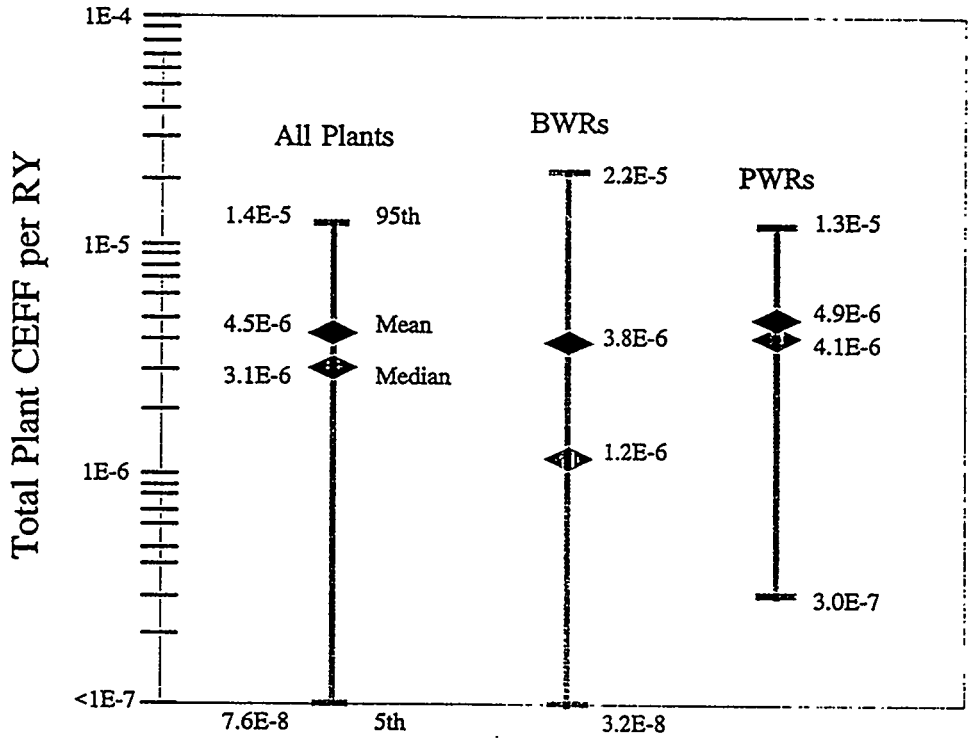


Figure 1. Preliminary CEFF estimates of BWRs and PWRs

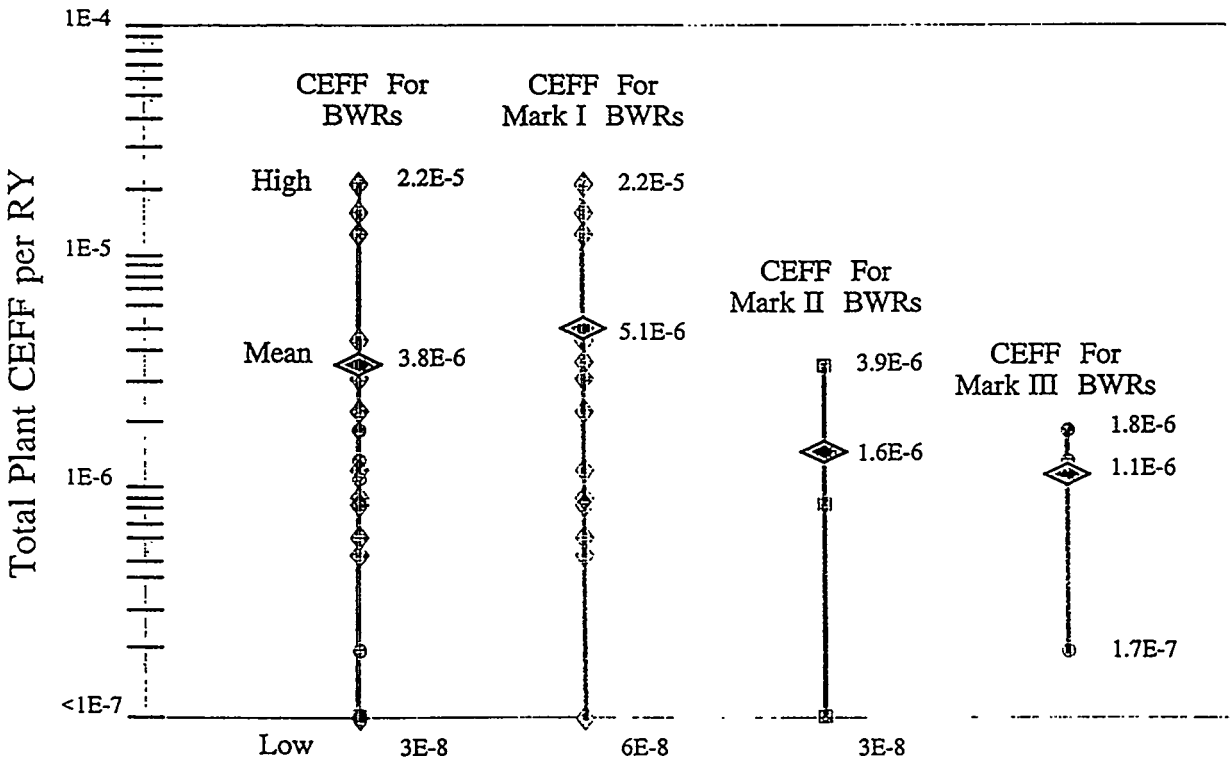


Figure 2. Individual CEFFs for BWRs by containment type.

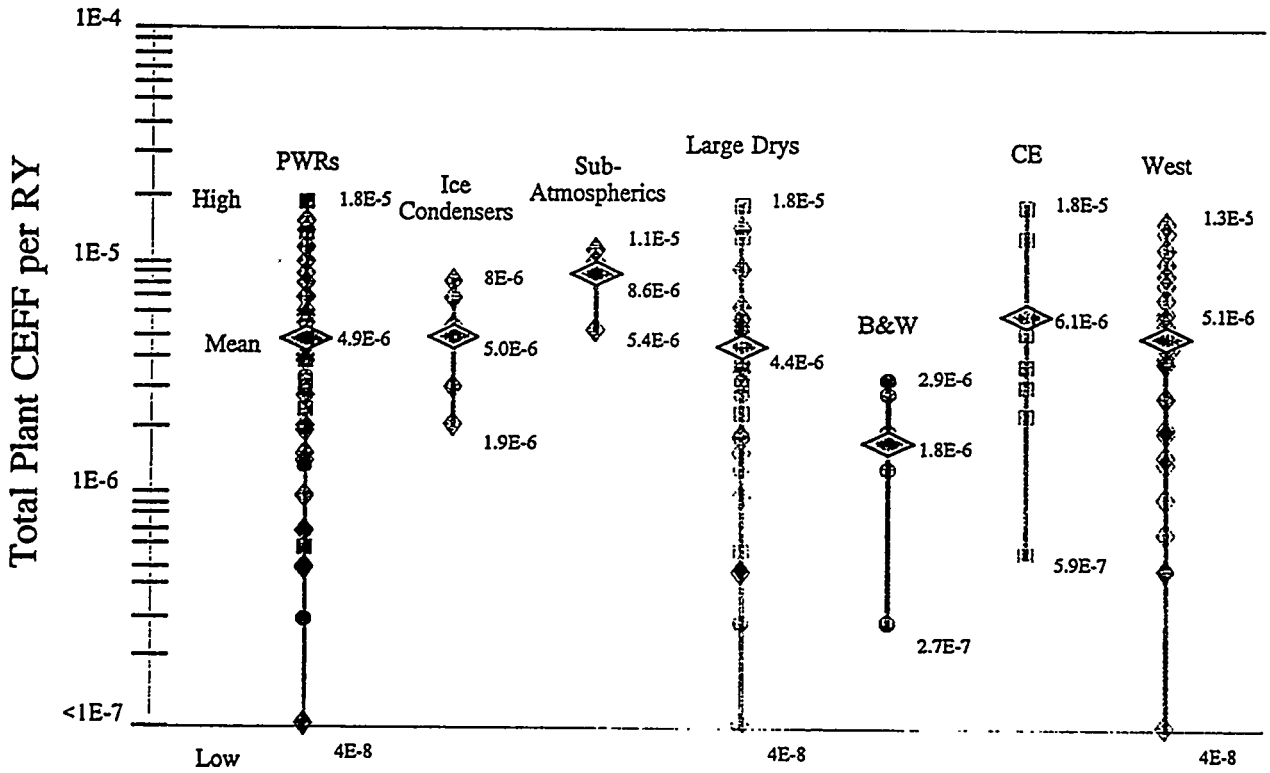


Figure 3. Individual CEFFs for PWRs by NSSS vendor and containment type

3.2 Comparison Among Similar Containment Types

The second set of preliminary insights involves comparing early failure and bypass frequencies among plants with similar containments. Both containment early failure frequency (CEFF) and the corresponding conditional containment early failure (CCEF) are presented. Besides the total CEFF and CCEF, the CEFF and CCEF for releases with the iodine and/or cesium fission product group greater than 10% of core inventory are also compared.

Comparisons are made among (1) six BWR plants with Mark I containments, (2) five PWR Westinghouse 4 loop plants with large dry containments, and (3) three plants with ice condenser containments (also Westinghouse 4 loop). (Some of the plants discussed here are not among the 62 plants for which results were shown above. Results shown include "small" early releases, not included above).

Table 1 shows six BWR Mark I plants, A through F, arranged according to CEFF. The CEFF for releases with fission product groups 2 and 3, i.e. iodine and cesium groups respectively, greater than 10% of core inventory is also shown. This latter CEFF will be referred to for convenience as the "substantial release" CEFF. The range of frequencies varies by more than two and one half orders of magnitude for both the total CEFF and the substantial release CEFF. Figure 4 shows these results graphically with total CEFF on the left and substantial release CEFF on the right. As can

be seen the relative order of the plants is the same for both frequency measures.

Table 2 shows what happens when the frequencies are normalized to conditional early containment failure probabilities CCEF. While plant A and F are still the highest and lowest respectively, the order of plants B, C, D and E has changed. As a matter of fact the CCEF for the these middle four plants is very similar, while plant A now appears unusually high and plant F unusually low. This is graphically illustrated in Figure 5. One reason, although not the only one, for the plant A and F results is that the IPE for plant A treated drywell liner melt through in its base case analysis and ascribed a large amount of early failures to this postulated phenomenon, while in plant B's IPE liner melt through was not considered in the base case analysis.

It is interesting to note, both from Table 2 and Figure 5, that, when the CCEF for substantial releases is considered, all the plants, with the exception of plant F, fall into the same range. Therefore plant A's IPE assumptions relative to those of the other plants' regarding source terms must in some way compensate for the larger CCEF of plant A. Plant F's results seem unusually low judged by any of the measures discussed.

The next comparison involves five PWR Westinghouse 4 loop plants, a through e, whose CEFFs are shown in Table 3 and Figure 6. Again the relative order for total CEFF and substantial release CEFF is the same. The range in both cases is about two orders of magnitude. Normalized (i.e. conditional) values are shown in Table 4 and Figure 7. The order of the plants for total CCEF is changed from that of CEFF, but when the CCEF for substantial release is considered the order reverts back to what it was for CEFF. The results for substantial release CCEF are very similar for all plants except for plant e, which appears to be unusually low. For large dry containments the CCEF, as used here, is dominated by bypass scenarios, with other early failure modes being relatively unlikely. Therefore the results shown here for these five plants are an indication of the importance bypass scenarios, both interfacing LOCA and steam generator tube rupture, played in the IPE modelling.

The final comparison is made for three PWR plants, x, y and z, using ice condenser containments. Since all plants with ice condensers are Westinghouse 4 loop plants, a comparison of containment performance results with the five Westinghouse 4 loop plants with large dry containments, considered above, may also be of interest. Table 5 and Figure 8 show the CEFF values for the three ice condenser plants. Since these plants are very similar in design one has some reason to expect very similar results. While the total CEFF are very close, plant z appears to have an unusually low substantial release CEFF. Table 6 and Figure 9 show the conditional, i.e. CCEF, values. Here the results are quite striking: plants x and y are very similar in both their total CCEF and substantial release CCEF while plant z has a considerably higher total CCEF but a considerably lower substantial release CCEF. It is hard to imagine that actual plant features would account for these various differences and it is expected that the reason for the variation will be found in the modeling differences used in the IPE of plant z versus the IPEs of plants x and y.

PLANT	CEFF	CEFF with Releases for FPG2 or FPG3>0.1
A	2.8 E-5	6.2 E-6
B	7.8 E-6	5.5 E-6
C	5.2 E-6	1.2 E-6
D	4.8 E-6	1.1 E-6
E	7.5 E-7	3.3 E-7
F	6.0 E-8	1.1 E-8

CEFF - Containment Early Failure Frequency
FPG2 - Iodine Fission Product Group
FPG3 - Cesium Fission Product Group
0.1 - Fraction of Core Inventory

Table 1

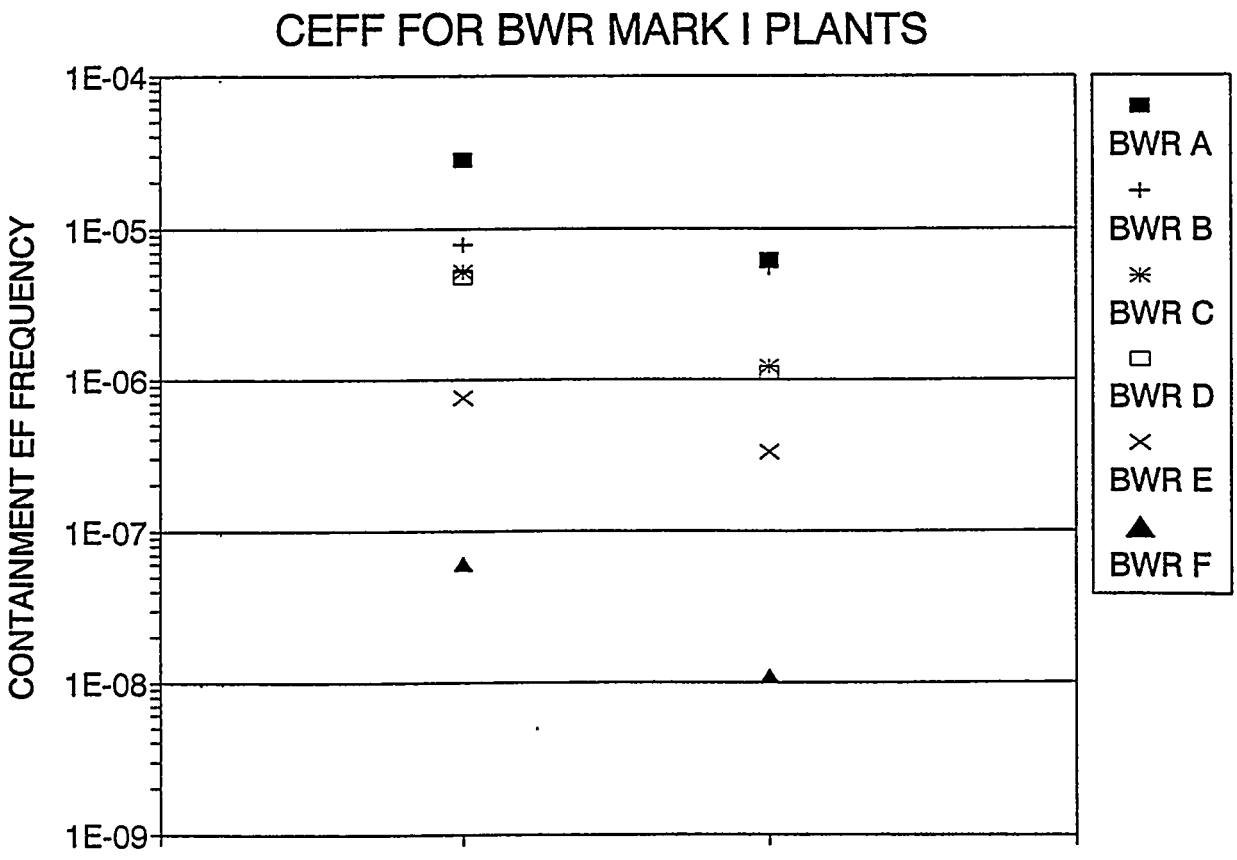


Figure 4

PLANT	CEFF	CCEF	CCEF with Releases for FPG2 or FPG3>0.1
A	2.8 E-5	.607	0.134
B	7.8 E-6	.134	0.095
C	5.2 E-6	.233	0.054
D	4.8 E-6	.203	0.047
E	7.5 E-7	.237	0.104
F	6.0 E-8	.050	0.009

CCEF - Conditional Containment Early Failure
FPG2 - Iodine Fission Product Group
FPG3 - Cesium Fission Product Group
0.1 - Fraction of Core Inventory

Table 2

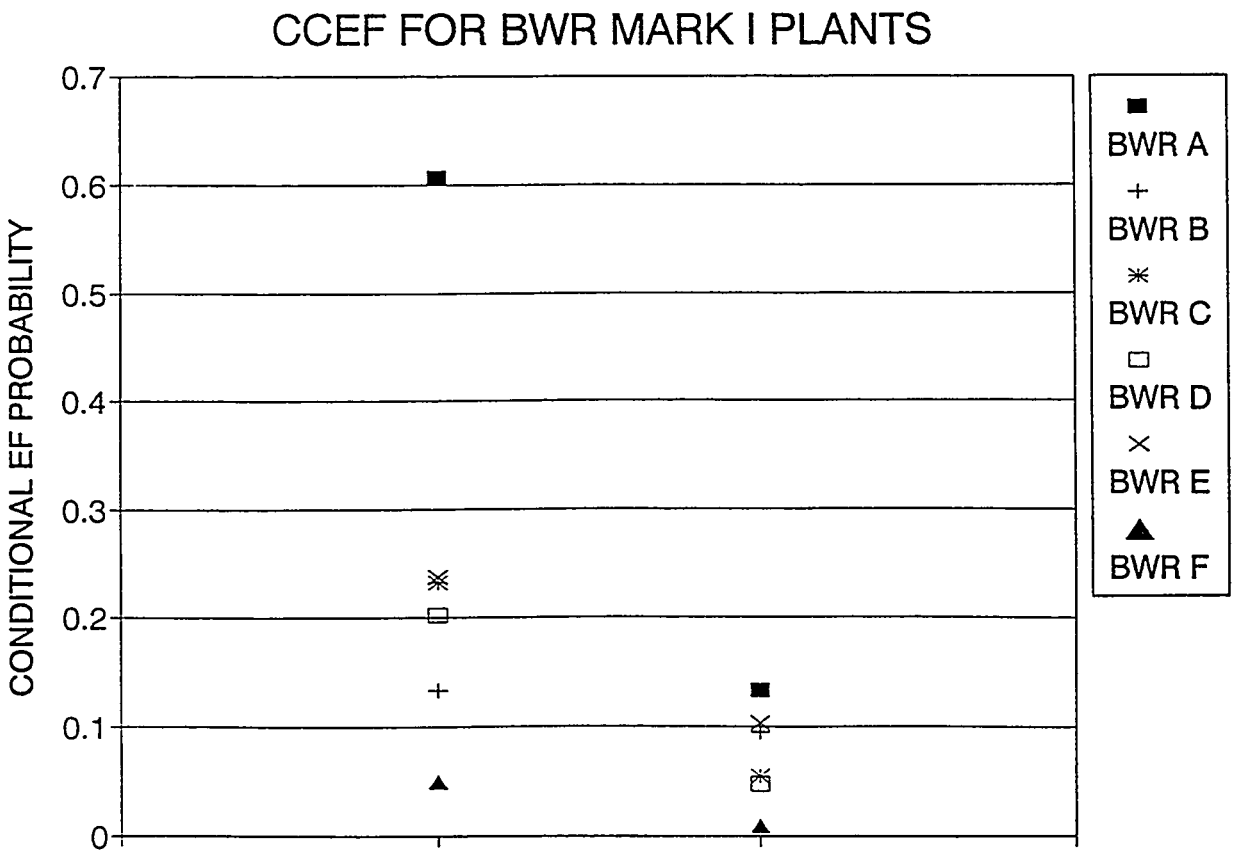


Figure 5

PLANT	CEFF	CEFF with Releases for FPG2 or FPG3>0.1
a	1.3 E-5	9.0 E-6
b	1.2 E-5	3.7 E-6
c	2.4 E-6	7.7 E-7
d	2.0 E-6	4.4 E-7
e	1.6 E-7	6.1 E-8

CEFF - Containment Early Failure Frequency
FPG2 - Iodine Fission Product Group
FPG3 - Cesium Fission Product Group
0.1 - Fraction of Core Inventory

Table 3

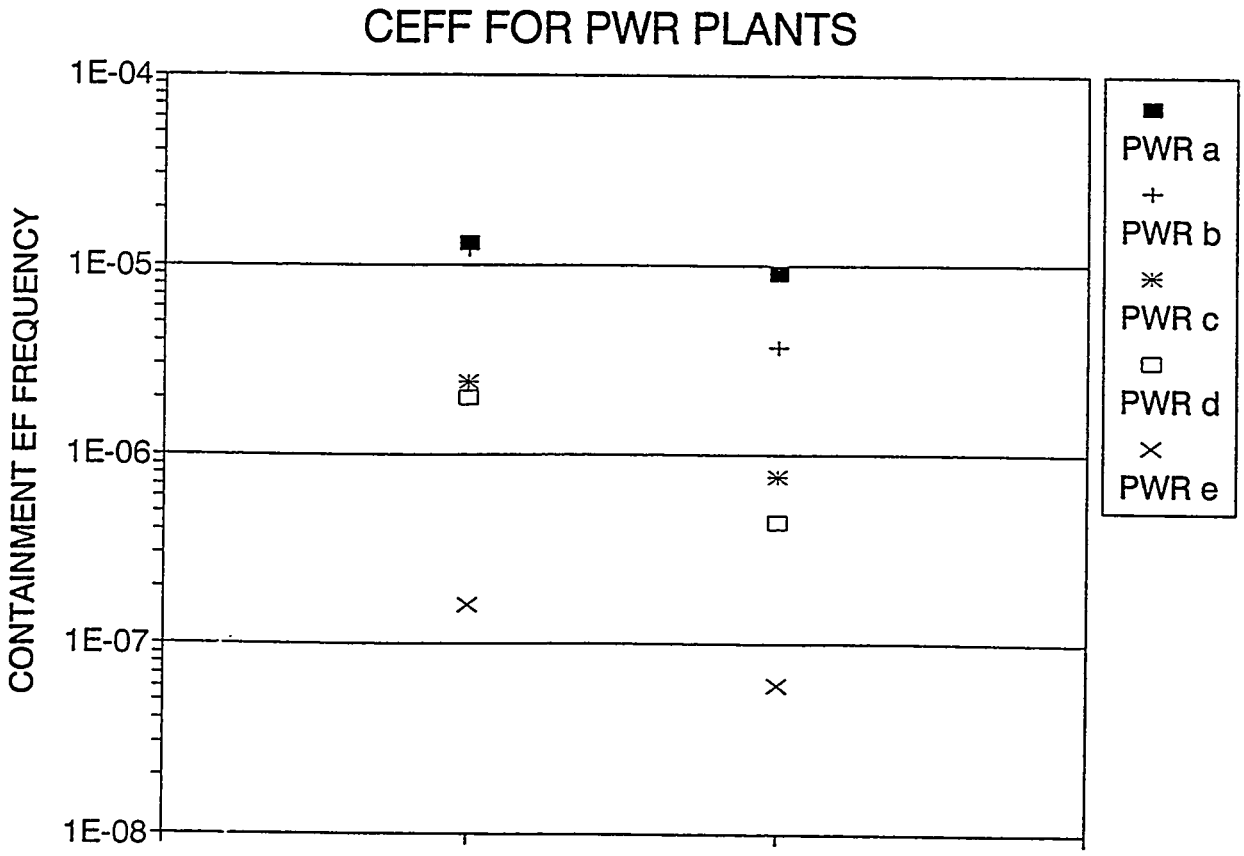


Figure 6

PLANT	CEFF	CCEF	CCEF with Releases for FPG2 or FPG3>0.1
a	1.3 E-5	.067	.050
b	1.2 E-5	.134	.042
c	2.4 E-6	.055	.018
d	2.0 E-6	.064	.014
e	1.6 E-7	.004	.001

CCEF - Conditional Containment Early Failure
FPG2 - Iodine Fission Product Group
FPG3 - Cesium Fission Product Group
0.1 - Fraction of Core Inventory

Table 4

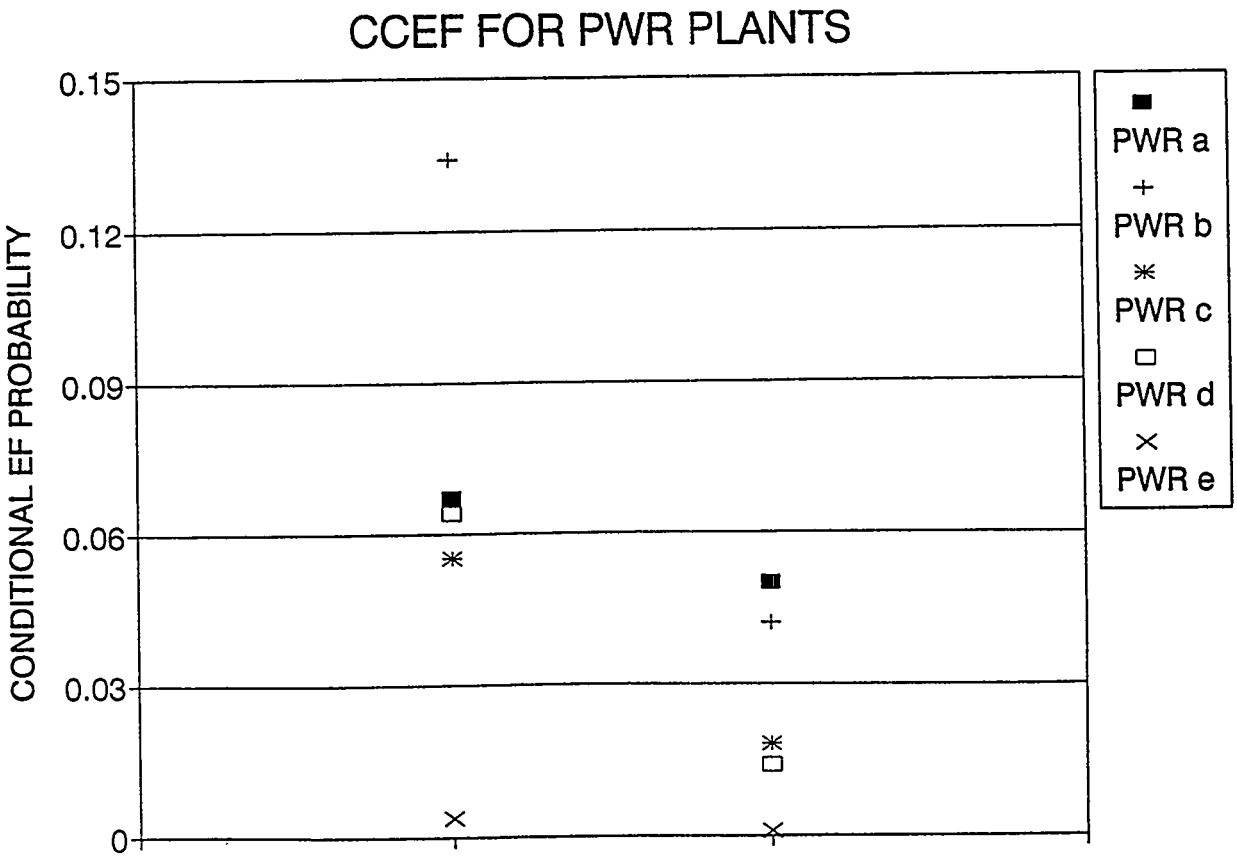


Figure 7

PLANT	CEFF	CEFF with Releases for FPG2 or FPG3>0.1
x	2.1 E-5	1.5 E-5
y	1.1 E-5	8.0 E-6
z	7.1 E-6	1.1 E-6

CEFF - Conditional Early Failure Frequency
FPG2 - Iodine Fission Product Group
FPG3 - Cesium Fission Product Group
0.1 - Fraction of Core Inventory

Table 5

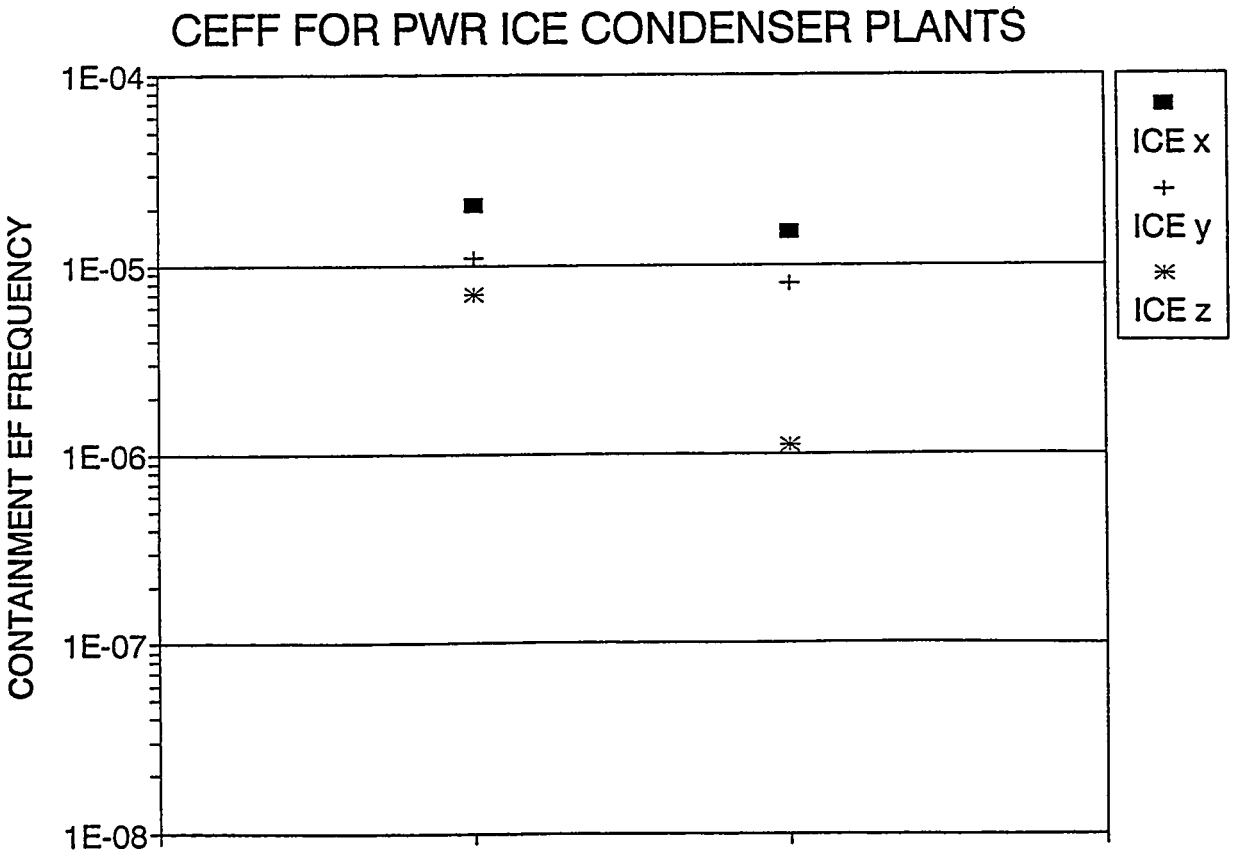


Figure 8

PLANT	CEFF	CCEF	CCEF with Releases for FPG2 or FPG3>0.1
x	2.1 E-5	0.064	.045
y	1.1 E-5	0.063	.047
z	7.1 E-6	0.120	.018

CCEF - Conditional Containment Early Failure
FPG2 - Iodine Fission Product Group
FPG3 - Cesium Fission Product Group
0.1 - Fraction of Core Inventory

Table 6

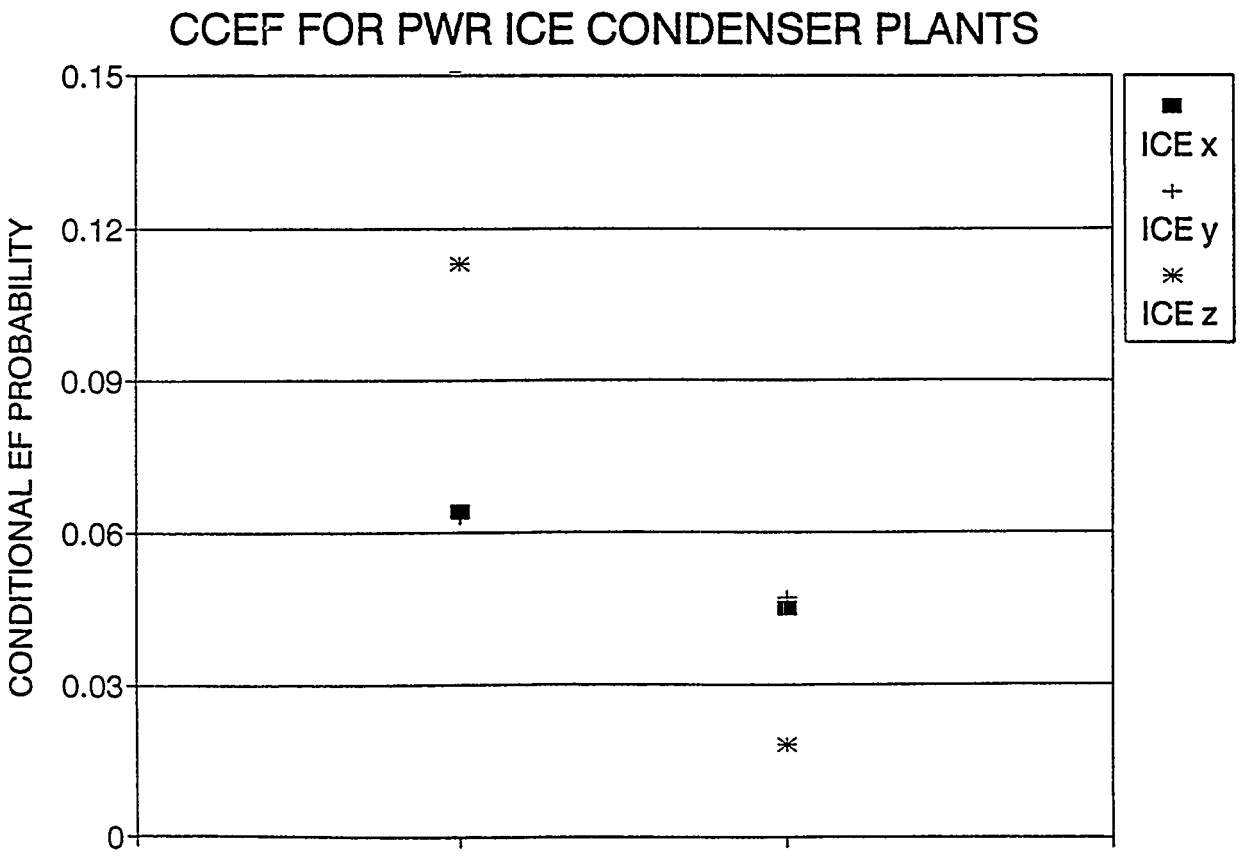


Figure 9

4. Conclusions

The differences seen in the preliminary results presented above may be due to plant and containment design features, or due to analytical assumptions, or due to the plant-specific analytical definitions.

As stated repeatedly, the results presented are preliminary, and exploration of the reasons for the differences in containment performance is continuing under the current program.

While some failure modes are common to all plants of a certain containment type (e.g., liner melt through for Mark I containments) their contributions change among plants even with similar containment design. The relative contribution of liner melt through to containment early failure is dependent on the assumptions used in the analysis and, of course, specific design features. (For example, more recent research information indicates that liner melt through results in a relatively lower contribution to early containment failure when water is available in the drywell (NUREG/CR-5423[6]), while NUREG-1150[3] assumed a high probability of liner melt through for both a wet and dry cavity. Different plant characteristics also have a major impact on CEFF. Such characteristics as reactor thermal power, containment free volume, sump volume, drywell floor area, pedestal radius, distance form pedestal wall to liner and height of main vent lines above drywell floor can determine whether liner melt through is an issue.

6. References

1. Lehner J.R. et al., "IPE Data Base Structure and Insights," NUREG/CP-0133, Proceedings of the USNRC 21st WRSIM, March 1994.

2. MAAP 3.0B Users Manual, Vol.1 and Vol.2, Fauske and Associates, Inc., March 1990.

3. U.S. Nuclear Regulatory Commission, Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, NUREG-1150, December 1990.

4. Summers, R.M. et al., MELCOR 1.8.0: A Computer Code for Nuclear Reactor Severe Accident Source Term and Risk Assessment Analyses, NUREG/CR-5531, January 1991.

5. Taylor, J. M., "Status of IPE and IPEEE Insights Programs," SECY-94-134, USNRC, May 20, 1994.

6. Theofanous, T.G. et al., The Probability of Liner Failure in a Mark I Containment, NUREG/CR-5423, August 1991.

Risk Contribution from Low Power, Shutdown, and Other Operational Modes Beyond Full Power*

D. W. Whitehead[1]
T. D. Brown[2]
T-L Chu[3]
W. T. Pratt[3]

[1]Risk Assessment and Systems Modeling Department 6412
Sandia National Laboratories
Albuquerque, New Mexico 87185-0747

[2]Accident Analysis and Consequence Assessment Department 6413
Sandia National Laboratories
Albuquerque, New Mexico 87185-0748

[3]Department of Advanced Technology
Brookhaven National Laboratory
Upton, New York 11973

During 1989 the Nuclear Regulatory Commission (NRC) initiated an extensive program to carefully examine the potential risks during low power and shutdown operations. Two plants, Surry (a pressurized water reactor) and Grand Gulf (a boiling water reactor), were selected for study by Brookhaven National Laboratory and Sandia National Laboratories, respectively.

The program objectives included assessing the risks of severe accidents initiated during plant operational states other than full power and comparing estimated core damage frequencies, important accident sequences, and other qualitative and quantitative results with full power accidents as assessed in NUREG-1150. The scope included a Level 3 probabilistic risk assessment (PRA) for traditional internal events and a Level 1 PRA on fire, flooding, and seismically induced core damage sequences.

A phased approach was used in Level 1. In Phase 1 the concept of plant operational states (POSs) was developed to provide a better representation of the plant as it transitions from power to nonpower operation. This included a coarse screening analysis of all POSs to identify vulnerable plant configurations, to characterize (on a high, medium, or low basis) potential frequencies of core damage accidents, and to provide a foundation for a detailed Phase 2 analysis.

In Phase 2, selected POSs from both Grand Gulf and Surry were chosen for detailed analysis. For Grand Gulf, POS 5 (approximately cold shutdown as defined by Grand Gulf Technical Specifications) during a refueling outage was selected. For Surry, three POSs representing the time the plant spends in midloop operation were chosen for analysis. These included POS 6 and POS 10 of a refueling outage and POS 6 of a drained maintenance outage.

Level 1 and Level 2/3 results from both the Surry and Grand Gulf analyses are presented.

*This work was supported by the United States Nuclear Regulatory Commission and was performed at Brookhaven National Laboratory and Sandia National Laboratories, which are operated for the U.S. Department of Energy under Contract Numbers DE-AC02-76CH00016 and DE-AC04-94AL85000, respectively.

1. Introduction

During 1989 the Nuclear Regulatory Commission (NRC) initiated an extensive program to carefully examine the potential risks during low power and shutdown operations. Two plants, Surry (a pressurized water reactor) and Grand Gulf (a boiling water reactor), were selected as the plants to be studied by Brookhaven National Laboratory and Sandia National Laboratories, respectively.

The program objectives included assessing the risks of severe accidents initiated during plant operational states other than full power operation and comparing the estimated core damage frequencies, risks, important accident sequences, and other qualitative and quantitative results with those accidents initiated during full power operation as assessed in NUREG-1150.

A phased approach was used in the Level 1 program. In Phase 1 the concept of plant operational states (POSs) was developed to allow the analysts to obtain a better representation of the plant as it transitions from power to nonpower operation. This phase consisted of a coarse screening analysis for all POSs to identify potential vulnerable plant configurations, to characterize (on a high, medium, or low basis) the potential frequencies of core damage accidents, and to provide a foundation for a detailed Phase 2 analysis.

In Phase 2, selected POSs from both Grand Gulf and Surry were chosen for detailed analysis. For Grand Gulf, POS 5 (approximately cold shutdown as defined by Grand Gulf Technical Specifications) during a refueling outage was selected. For Surry, three POSs representing the time the plant spends in midloop operation were chosen for analysis. These included POS 6 and POS 10 of a refueling outage and POS 6 of a drained maintenance outage.

During the preliminary quantification of the accident sequences in Phase 2, it was found that the decay heat at which the accident-initiating event occurs is an important parameter that determines both the success criteria for the mitigating functions and the time available for operator actions. In order to better account for the decay heat, a "time window" approach was developed. In this approach, time windows after shutdown were defined based on the success criteria established for the methods used to mitigate the accident. Section 2 documents the results from the work performed during the Phase 2 analysis of the Grand Gulf plant, and Section 3 documents the results from the Surry Phase 2 analysis.

2. Grand Gulf Results and Conclusions

The results and conclusions presented below come directly from NUREG/CR-6143, Vols. 2 - 6.[1-6]

2.1 Level 1 Results

2.1.1 Quantitative Results for Traditional Internal Events

Individual Sequences

The total core damage frequency (CDF) presented here results from combining the mean CDFs from all 38 sequence cut sets for the 28 sequences that survived through the time window analysis. For POS 5 during a refueling outage at Grand Gulf, the sum of the mean CDFs from the surviving sequences is 2.1E-6 per calendar year for internally initiated events (excluding internal fires and floods).

IE Class	Mean CDF	% Contribution To CDF
LOCA/diversion	1.3E-06	62
LOSP/blackout	7.0E-07	33
Other	9.9E-08	5
Total	2.1E-06	100

Figure 1 shows the contributions of the various initiating events to core damage frequency. Two classes of initiating events dominate the results from this study. As can be seen above, loss-of-coolant accident (LOCA)/diversion and loss of offsite power (LOSP)/blackout constitute approximately 95% of the total core damage frequency.

Within these two classes of sequences, two types of accidents are dominant. They are:

- Blackout - Initiated by a loss of offsite power, a subsequent loss of all onsite ac power either by loss of the diesel generators (DGs) directly or indirectly--by the loss of some DG support system, and the failure to restore either offsite or onsite ac power before core damage occurs; and

- Flooding Containment - Initiated by an event requiring the injection of water into the vessel, out the SRVs to the suppression pool, and finally out the open lower containment personnel lock. owing to the failure of the operators to either close the lower personnel lock or to control the injection of the water into the vessel. The resulting flood is assumed to cause failure of the equipment necessary to prevent core damage.

From a CDF vs. time window aspect, time window 2 is the most important; Figure 2 indicates that it contributes 58 percent of the total core damage frequency. Another way to present the core damage frequency information is to plot the fractional contribution of each initiator group by time window. This results in Figure 3. From this figure it can be seen that for:

Time Window 1

The core damage frequency is split between the LOCA/diversion and the LOSP/blackout groups (42 and 58 percent respectively).

Time Window 2

The core damage frequency is split among the three groups (41 percent - LOCA/diversion, 50 percent - LOCA/blackout, and 9 percent - Other)

Time Window 3

All core damage frequency results from the LOCA/diversion group.

One final way to present the core damage frequency information is to plot the percent contribution to the total core damage frequency and the percent of time spent in each time window vs. the three time windows on the same graph. From Figure 4 it can be seen that even though the plant spends only 21 percent of the time in time window 2, this window contributes 58 percent to the total core damage frequency. Figure 4 also indicates that time window 3 contributes 35 percent of the total core damage frequency, yet 76 percent of the time is spent in this window. Thus, from Figures 3 and 4 we see that time window 2 is the most important time regime for POS 5 during a refueling outage.

Total Plant Model

The CDF results from the uncertainty analysis of the total plant model for traditional internal events (i.e., an uncertainty analysis of all of the sequence cut sets at the same time) using 1000 samples are as follows:

Mean Value	2.0E-006
5th Percentile Value	4.1E-007
Median Value	1.3E-006
95th Percentile Value	5.4E-006

Comparing the results of this study with those obtained in the NUREG/CR-4550 study of Grand Gulf and the Grand Gulf individual plant examination (IPE), we find that the mean CDF from the total plant model obtained in this study (2.0E-6) is 50 percent of the NUREG/CR-4550 value of 4.0E-6 and almost an order of magnitude less than IPE results of 1.7E-5. In addition, the results from this study indicate that, unlike the NUREG/CR-4550 results, sequences other than those initiated by LOSP (e.g., LOCAs) contribute significantly to the core damage frequency.

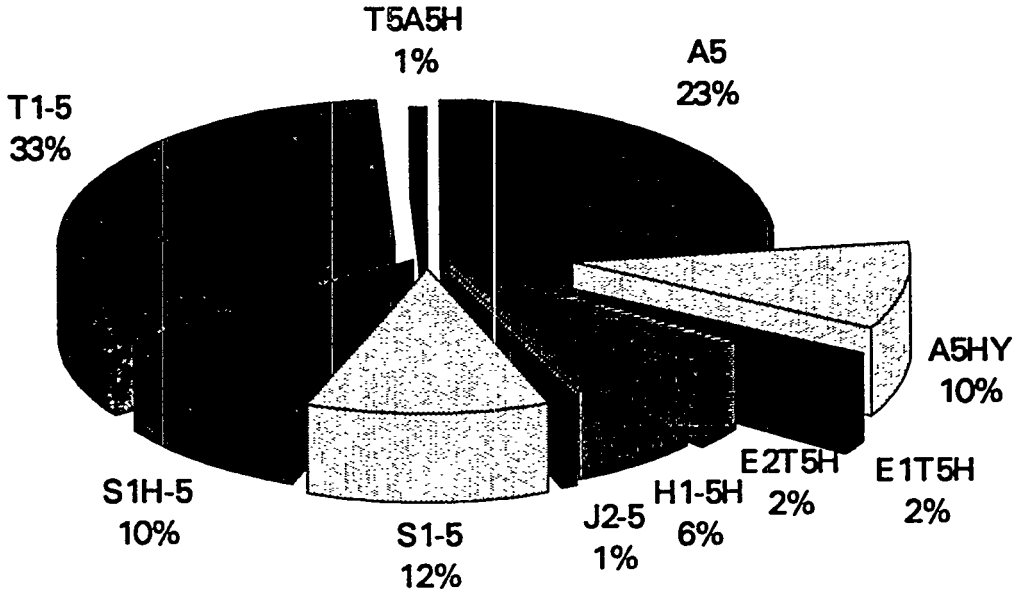


Figure 1 Contribution to CDF by Initiating Event

A5 - Large LOCA during nonhydro conditions
A5HY - Large LOCA during hydro conditions
E1T5H - Isolation of shutdown cooling common suction line
E2T5H - Loss of shutdown cooling common suction line
H1-5H - Diversion to the suppression pool via the residual heat removal system
J2-5 - LOCA in the residual heat removal system
S1-5 - Intermediate LOCA during nonhydro conditions
S1H-5 - Intermediate LOCA during hydro conditions
T1-5 - Loss of offsite power
T5A5H - Loss of standby service water system

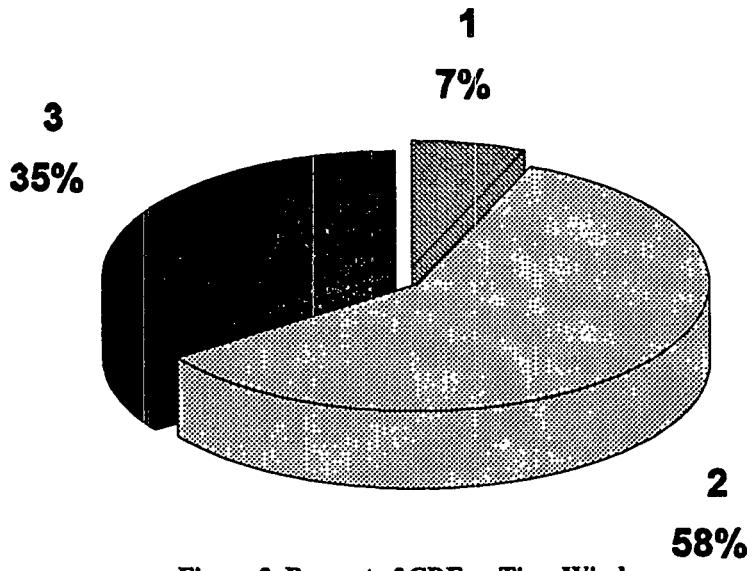


Figure 2 Percent of CDF vs Time Window

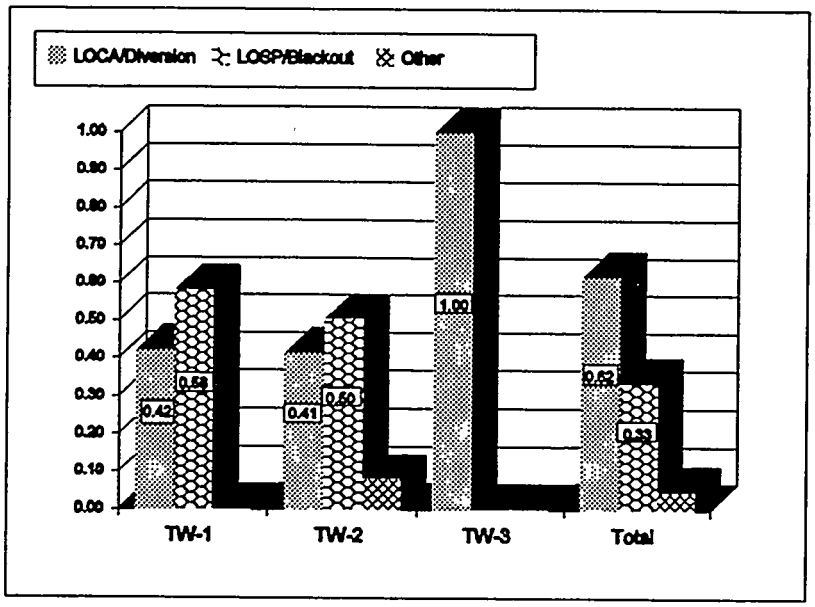


Figure 3 Fractional Contribution to CDF by IE Group vs Time Window

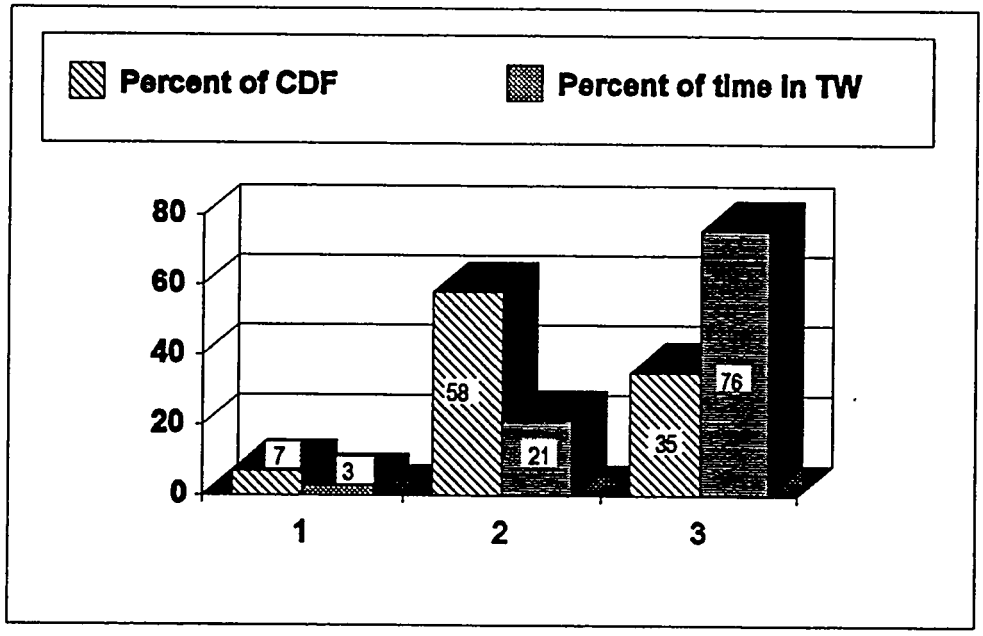


Figure 4 Percent of CDF and Percent of Time in Time Window vs. Time Window

2.1.2 Quantitative Results from Internal Fire Events

A detailed screening analysis was performed which showed that most plant areas had a negligible contribution to the frequency of fire-induced core damage. A detailed fire propagation analysis was performed for four fire zones. There were no plant areas which were found to have a contribution to core damage frequency greater than the truncation limit of 1E-8; thus, no fire sequences survived.

2.1.3 Quantitative Results for Internal Flooding Events

A single sequence survived through the time window analysis. This sequence is initiated by a break in a fire water system pipe. The resulting flood from this initiator disables Divisions 1, 2, and 3 Class 1E ac and dc power. Given the severity of this postulated accident sequence, no operator recovery was postulated. The mean core damage frequency for this sequence is 2.3E-8 per year. The 5th and 95th percentiles are 8.2E-11 and 8.6E-6 per year, respectively.

2.1.4 Quantitative Results from Seismic Events

The CDF results of the seismic analyses for earthquake-initiated accidents during POS 5 for a refueling outage are as follows:

For the LLNL (1993) Hazard Curves		**For the EPRI Hazard Curves**	
5th percentile	2.1E-11	5th percentile	2.5E-12
Median	2.4E-9	Median	2.0E-10
Mean	7.1E-8	Mean	2.5E-9
95th percentile	2.2E-7	95th percentile	1.1E-8

2.1.5 Qualitative Results

Insights from Traditional Internal Events

Systems Insights

Characteristics of the plant design are a major factor affecting the likelihood of core damage while in cold shutdown. For Grand Gulf, the following plant characteristics are most important:

1. Shutdown cooling system components are not rated for full pressure, but automatic isolation occurs on either high pressure or on low level;

2. Use of the residual heat removal system for shutdown cooling requires recirculation, either forced or natural, to prevent pressurization transients;

3. Owing to density and pump head effects, recirculation is sensitive to actual level in the core region. The water level in the core region is related to but not equal to measured level in the downcomer;

4. At decay heat levels of concern, flooding-induced dryout of the core at atmospheric pressure will not occur, and the core can be cooled by steaming with a maximum of 250 gpm makeup;

5. To steam at low pressure, opening one safety relief valve in relief mode is sufficient to maintain pressure low enough that the low head pumps in the emergency cooling system can provide sufficient makeup;

6. Opening one safety relief valve in relief requires operator action, dc power, and air;

7. In using the emergency core cooling system in a water solid mode, opening of two safety relief valves in the relief mode prevents overpressurizing the shutdown cooling system components, both in the residual heat removal system and in the alternate decay heat removal system (ADHRS), regardless of the pump(s) used;

8. In using the emergency core cooling system in a water solid mode, opening one safety relief valve in the relief mode prevents overpressurizing the components in the residual heat removal system used in shutdown cooling, but components in the auxiliary decay heat removal system may be overpressurized;

9. Isolation of the shutdown cooling system allows the core to be cooled at full pressure by steaming on one safety relief valve at its safety setpoint, and no operator action or support systems are required to operate the valve in the safety mode;

10. Use of emergency core cooling systems in a water solid mode does not require suppression pool makeup, in the short term, to compensate for vessel fill;

11. Water can be injected into the vessel at low pressure from both service water and diesel-driven firewater pumps.

Operations Insights

In POS 5 (i.e., cold shutdown), the requirements of the technical specifications for the operability of systems and components are much less stringent than for power operation. The actual availability of systems depends on plant-specific practices, and on the reason for transitioning the plant to cold shutdown -- in this case, a refueling outage.

For Grand Gulf, the following practices have an important impact on the ability to cool the core in POS 5:

1. At least two safety relief valves are maintained operable for both relief and safety operation;

2. Automatic isolation of the low-pressure shutdown cooling system is not bypassed, but is maintained on both high pressure and low level;

3. Some subsystems of the emergency core cooling system are available most of the time.

Insights from Internal Fire Events

The fire-induced core damage frequency is lower than other fire risk assessments at power owing to a number of factors. First, this plant operational state represents only 3 percent of the time at shutdown, and shutdown fire frequencies are similar to those at power. This immediately reduces core damage frequency. Second, even if active electromechanical safety-related equipment is damaged by fire, an initiating event may not necessarily occur. For instance, for the loss of the turbine building cooling water (TBCW) initiator to result from fire-related damage, multiple operational pumps must fail. These pumps and their associated cabling have sufficient separation to make it highly unlikely that a single fire could lead to failure of all pumps. Many initiating events at shutdown were screened because of physical separation criteria. Even for the unscreened initiating events, very few fire zones were found to be applicable because of physical separation criteria. Also, relative to other plants, Grand Gulf utilizes more automatic fire protection systems in critical safety-related areas, which in turn reduces the probability of damage from a fire. Therefore, after taking into account the physical separation of safety-related functions, automatic fire protection systems, lower frequencies of fire-initiated events, and manual fire suppression, most initiating events at shutdown and many fire zones were eliminated from further analysis.

A detailed fire propagation analysis was performed for the remaining initiators and respective fire zones. It was found that only in very limited areas could fire damage result in both the initiating event and other fire-related failures that were necessary for core damage. Even in these situations, other random failures (nonfire-related) were also necessary before core damage occurred. Therefore, when taking into account the reduction in fire frequency caused by the limited area of influence and other random failures which were required before core damage, all remaining fire scenarios were found to be less than the truncation limit.

In all areas, additional random failures of equipment (damage not related to the fire itself) had to occur in order to obtain core damage. Adequate separation of equipment (and/or) cabling between redundant functions and the presence of automatic fire suppression systems reduced core damage frequency for those areas.

Insights from Internal Flooding Events

The overall conclusion of this work is that internal floods do not pose a significant core damage threat to the Grand Gulf Nuclear Station for POS 5 during a refueling outage. The core damage frequency of 2.3 E-8 per year resulting from internal flood events is approximately two orders of magnitude lower than the core damage frequency of 2.0E-6 per year for traditional internal events. Thus, internal flooding would make only a minor contribution to the total core damage frequency during POS 5. This is principally because of the low frequency of fluid boundary component breaks that could result in a flood and a separation of systems that would be available to mitigate the effects of such an accident.

The two conservative assumptions affecting flow rates and flood volumes included in these analyses (i.e., fully guillotined catastrophic breaks and full hour undetected breaks) did not significantly affect the results of this study. For completeness, it should be noted that the assumed undetected break time for the single surviving sequence was 15 minutes. This time, while a departure from the 1-hour assumption, was sufficient to cause a loss of all Class 1E ac and dc power, and probably represents a more realistic estimate of the undetected break time for POS 5 during a refueling outage.

Insights from Seismic Events

The mean core damage frequency of 7.1E-8 per year (maximum) is also low relative to the 2.0E-6 per year frequency for traditional internal initiators. Two reasons for this are:

1. Grand Gulf's seismic capacity in responding to earthquakes during shutdown is excellent, well above its design basis.

2. The Grand Gulf site is one of the least seismically active locations in the United States.

2.2 Level 2/3 Results

2.2.1 Core Damage Frequency

For discussion purposes, the core damage scenarios identified in the Level 1 analysis were combined into the following three PDS groups (12 PDSs were actually evaluated in the accident progression analysis): (LOCAs, station blackouts (SBOs), and Other transients. The total core damage frequency and the fractional contributions to the core damage frequency for these three groups are provided in Table 1. The LOCA PDS group is the dominant contributor to the core damage frequency, followed by the SBO PDS group and the Other transients PDS group.

2.2.2 Accident Progression

A simplified representation of the accident progression event tree (APET) that addresses the major aspects of the accident is shown in Figure 5. (The actual APET included 59 top events or questions.) Figure 5 combines the results from all the accidents and is conditional on the occurrence of core damage; the values displayed are mean conditional probabilities. From the simplified tree presented in Figure 5, it can be seen that in the most likely accidents in POS 5 the containment is open, the suppression pool is bypassed, and the vessel fails. For the cases where the vessel fails, there is a significant probability that the core debris will either be quenched in a flooded cavity or the interactions between the core debris and the concrete structures beneath the vessel, the core-concrete interaction (CCI), will occur in a flooded cavity. For the cases where the vessel fails, there is a significant probability that the core debris will either be quenched in a flooded cavity or the interactions between the core debris and the concrete structures beneath the vessel, the CCI, will occur in a flooded cavity. For the former, the releases associated with CCI are prevented. In the latter case, the radioactive releases are scrubbed by the water in the flooded cavity, which helps reduce the source term to the environment. If the containment is closed prior to core damage, it is predicted to either fail or to be vented after core damage because containment heat removal is not available in these accidents. Venting the containment late in the accident is the most likely scenario. For the accidents identified in POS 5, the containment sprays were never available after the onset of core damage.

2.2.3 Aggregate Risk

Table 2 presents the offsite risk results for the following six measures: early fatalities, total latent cancer fatalities, population dose within 50 miles of the site, population dose within 1000 miles of the site, individual early fatality risk within 1 mile of the site, and individual latent cancer risk within 10 miles of the site.

Many factors can affect the magnitude and severity of the release and in turn affect risk. Factors associated with POS 5 accidents that tend to increase risk include the following:

- In many of the accidents the containment equipment hatch was open during the entire accident. An open equipment hatch provides a path for radionuclides to escape from the containment to the auxiliary building and then out into the environment.

- Two plant features that can be used to attenuate the release of radioactive aerosols are the suppression pool and the containment sprays. In both the LOCA and the SBO PDSs, the radioactive material released from the damaged fuel bypassed the suppression pool. The containment sprays were not available in any of the POS 5 accidents.

- In many of the accidents, core cooling was not restored early in the accident, thus precluding any possibility of arresting the core damage process before vessel failure. When the vessel fails, the core debris in the vessel is released into the reactor cavity, allowing for possible CCIs. Significant amounts of radioactive material can be released during this ex-vessel phase of the accident.

Table 1 Core Damage Frequency for POS 5 and Fractional Contributions to the Core Damage Frequency for the LOCA, SBO, and Other Transients Plant Damage State Groups

Plant Damage State Groups	Descriptive Statistics[a]				
	Percentiles			Mean	Standard Deviation
	5th	50th	95th		
	Total Core Damage Frequency (per calendar year)				
Total	4.1E-07	1.4E-06	5.6E-06	2.1E-06	2.7E-06
	Fractional Contribution to Core Damage Frequency				
LOCA	0.10	0.50	0.93	0.51	0.27
SBO	0.03	0.24	0.80	0.33	0.26
Other	0.01	0.09	0.58	0.17	0.18

[a]Statistics based on a Latin hypercube sampling (LHS) sample size of 200 observations.

Table 2 Distributions for Aggregated Risk for POS 5
(all values are per calendar year; population doses are in person-rem)

Consequence Measures	Descriptive Statistics[a]				
	Percentiles			Mean	Standard Deviation
	5th	50th	95th		
Early Fatality Risk	3.7E-11	2.8E-09	3.9E-08	1.4E-08	5.4E-08
Total Latent Cancer Risk	4.3E-04	1.9E-03	1.2E-02	3.8E-03	7.7E-03
Population Dose within 50 miles of the plant	1.3E-01	5.3E-01	3.1E+00	9.9E-01	1.9E+00
Population Dose within 1000 miles of the plant	9.9E-01	4.4E+00	2.8E+01	8.7E+00	1.8E+01
Individual Early Fatality Risk-- 0 to 1 mile	4.2E-13	2.7E-11	3.0E-10	9.6E-11	3.4E-10
Individual Latent Cancer Risk-- 0 to 10 miles	2.5E-10	9.4E-10	4.9E-09	1.6E-09	2.4E-09

[a]Statistics are based on a LHS sample of 200 observations.

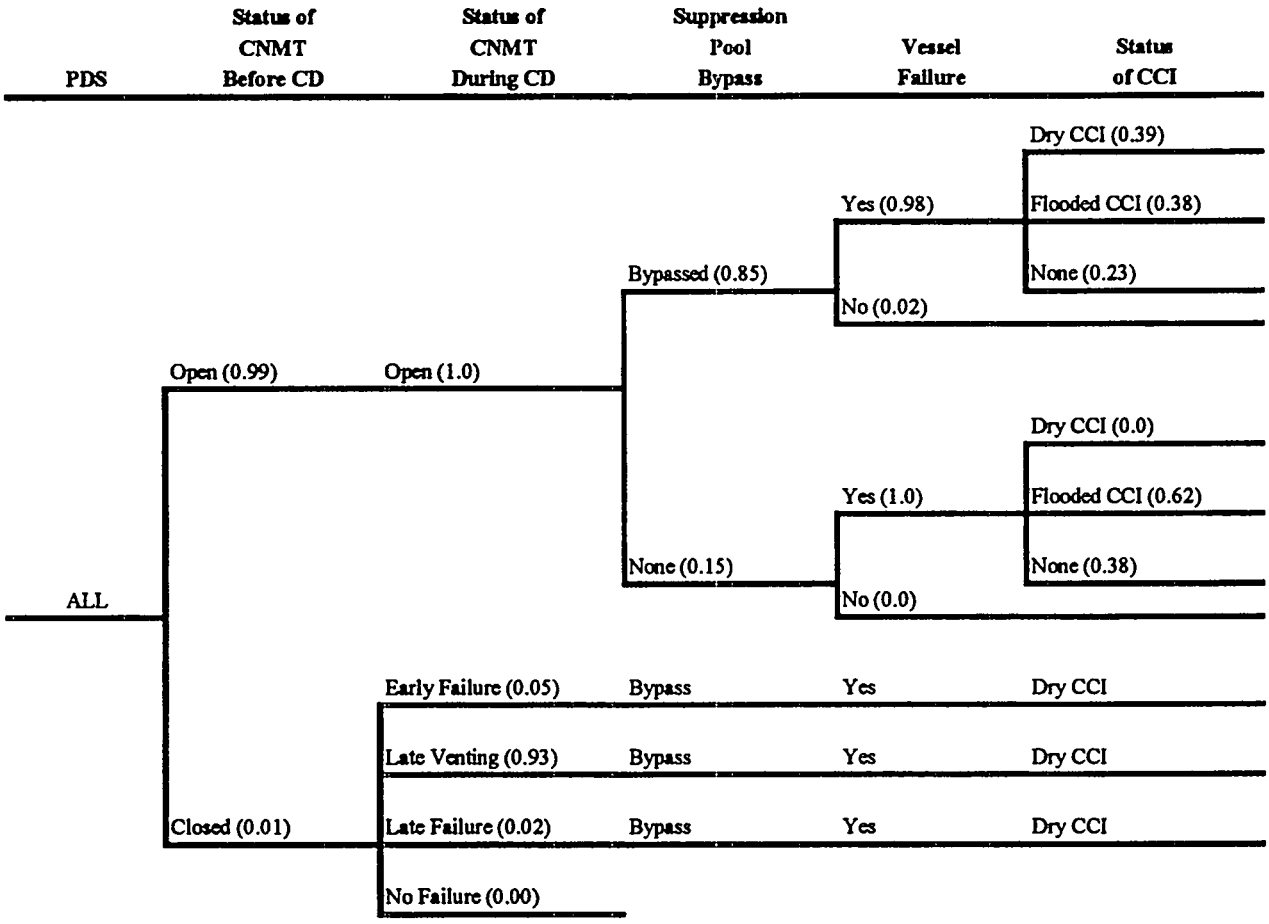


Figure 5 Simplified Representation of POS 5 Accident Progressions

A number of factors associated with these POS 5 accidents also tend to decrease risk. These factors are listed below:

- Although in many of the accidents the containment equipment hatch is open, the suppression pool is bypassed, and the containment sprays are unavailable, the releases pass through the auxiliary building before escaping into the environment. Because of its large volume and surface area, the auxiliary building provides a location for the radionuclides to be attenuated by deposition and thereby reduce the source term to the environment.

- The accidents delineated for these shutdown conditions progress slowly, and therefore a considerable amount of time is generally available for the public to respond to the accident and evacuate before exposure to the release. This is primarily important for measures of the early health effects, which are more strongly affected by the time available for evacuation.

- Radioactive decay has reduced the radioactive potential of these shutdown accidents relative to the inventory that is present immediately after the reactor is shut down. This factor is primarily important for early health effects, which are more strongly affected by the shorter lived radionuclides. This effect is much less noticeable for latent health effects, which are more strongly affected by the longer lived isotopes.

- The population around the Grand Gulf plant is relatively low. Although many factors influence the magnitude of the consequences, in general, for a given release, a smaller population correlates with a smaller number of fatalities. Of the four Mark III plants in the United States, Grand Gulf has the fewest number of people living within 50 miles of the plant, according to the 1990 census data. The Mark III plant with the greatest number of people living within 50 miles of the site has a population that is more than an order of magnitude greater than the Grand Gulf 50-mile population.

To place the risks from POS 5 into context, they were compared with the risks from full power operation as estimated in the NUREG-1150 Grand Gulf plant analysis.[7] In Figure 6, the early fatality and total latent cancer fatality risks from full power operation and POS 5 are presented. This comparison shows that the risks from POS 5 are not insignificant compared with the risks from full power operation. In fact, although the mean risk values from the two studies are similar (i.e., not differing by more that a factor of 5), the mean risk values from POS 5 are actually greater than the full power risk values.

Table 3 provides the fractional contributions to the early fatality risk and the total latent cancer risk for the following three PDS groups: LOCAs, SBOs, and Other transients. The fractional contributions to the population dose risk measures (not shown in Table 3 for brevity) are similar to the fractional contributions to the total latent cancer risk measure. From Table 3 it can be seen that, on average, the SBO PDS group is the dominant contributor to the total early fatality risk. Because a large amount of overlap exists among the three distributions, as is evident from the descriptive statistics provided in Table 3, on any given observation (an observation is one particular trial in the many trials made in a Monte Carlo type analysis) the contribution from the three groups can vary. That is, for one observation the SBO group may be dominant, whereas for another observation the LOCA group may be the dominant group. On average, however, the SBO is the dominant contributor. The SBO PDS group's large contribution to early fatality risk can be attributed to its relatively high contribution to the core damage frequency coupled with the fact that the containment equipment hatch is open, the suppression pool is bypassed, and the auxiliary building fails early in these accidents.

Table 3 Fractional Contributions to Aggregate Risk for the LOCA, SBO, and Other Transients Plant Damage State Groups

Plant Damage State Groups	Descriptive Statistics[a]				
	Percentiles			Mean	Standard Deviation
	5th	50th	95th		
	Fractional Contribution to Early Fatality Risk				
LOCA	0.001	0.04	0.72	0.16	0.24
SBO	0.080	0.87	1.00	0.73	0.30
Other	0.001	0.04	0.61	0.12	0.18
	Fractional Contribution to Total Latent Cancer Fatality Risk				
LOCA	0.04	0.38	0.90	0.42	0.27
SBO	0.04	0.41	0.90	0.45	0.28
Other	0.01	0.06	0.55	0.13	0.17

[a]Statistics are based on a LHS sample of 200 observations.

Combined, these factors cause the SBOs to have relatively high risk values. The LOCA PDS group, however, is not a dominant contributor to early fatality risk even though it is a dominant contributor to the core damage frequency. This situation occurs primarily because the dominant contributors to the LOCA core damage frequency are LOCA accidents that are initiated while the plant is in time window 3 (i.e., PDS3-1). Numerous factors can reduce the number of early fatalities that occur when the accident is initiated in time window 3 relative to the other time windows. These factors include the following conditions: (1) Radioactive decay has reduced the inventory of short-lived radionuclides that are important to early health effects. (2) Because of the lower decay heat, the accidents progress more slowly, allowing more time for the population to evacuate. (3) The release is spread out over a longer time which helps reduce the concentration of radionuclides in the environment. For these reasons time window 3 is a negligible contributor to early fatality risk.

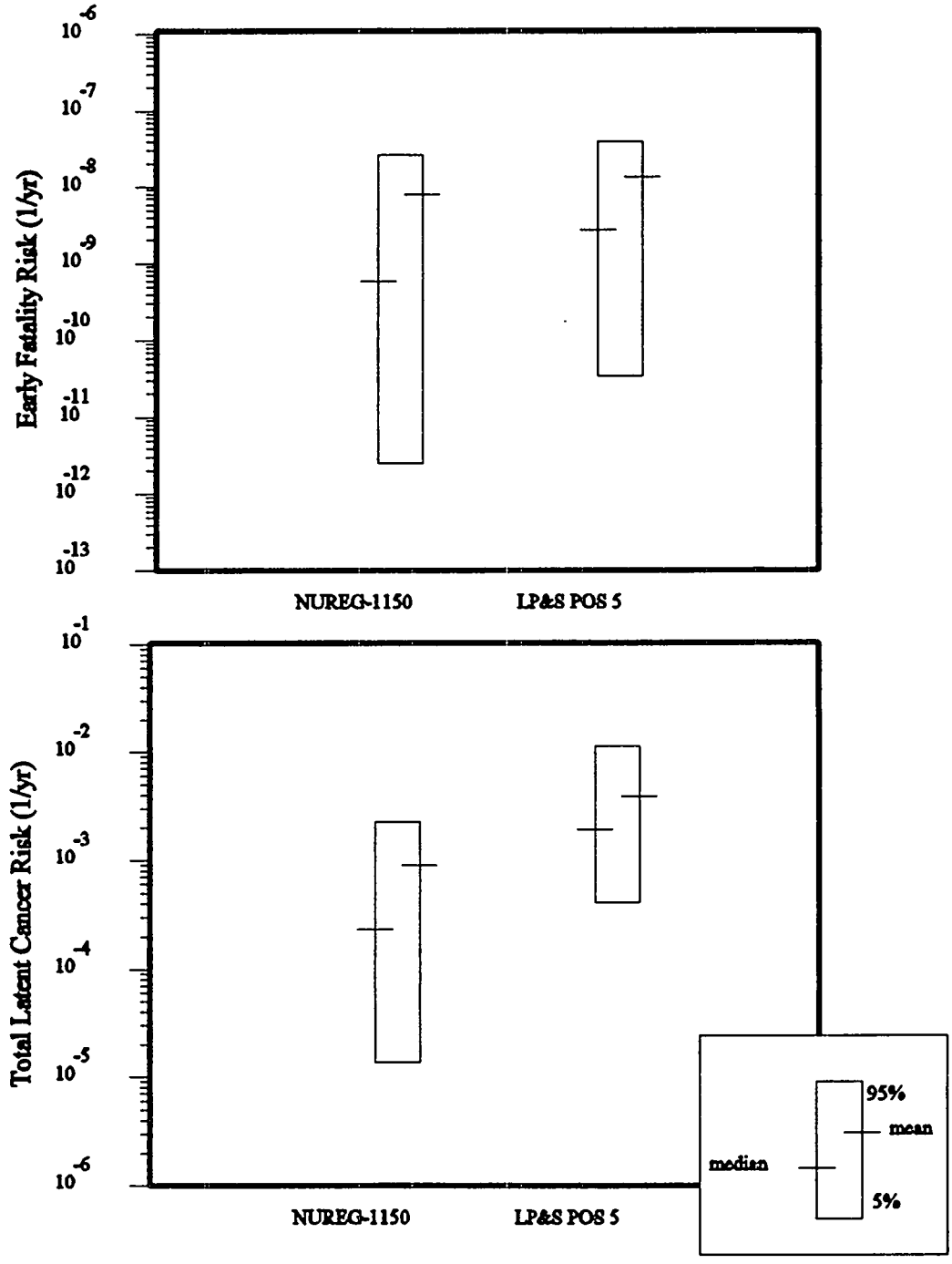


Figure 6
Comparison of POS 5 Risk with Full Power Risk

For latent cancer health effects, the LOCA and SBO PDS groups are, on average, the dominant contributors to risk. Because the radionuclides that are important to the latent health effects tend to have long half lives, these risk measures are not particularly sensitive to the time of accident occurrence relative to shutdown . Latent cancers primarily depend on the total amount of radioactive material released, not on the time it was released (i.e., early in the accident versus late in the accident). Because latent cancers are not strongly dependent on the timing characteristics of the accident (i.e., start of release or release duration), the latent cancer risk will depend on the likelihood of the accident and on the total amount of radioactive material released. In all of the core damage accidents delineated in this study, the containment is either open at the start of the accident or fails during the accident, and in most of the accidents the core damage process is not arrested in the vessel. Thus, although the timing of the accident may vary, when the uncertainty in the source term is considered, all the accidents will result in roughly similar releases of radioactive material to the environment. Thus, as can be seen in Tables 1 and 3, the mean fractional contribution to latent cancer risks tends to be roughly similar to the mean fractional contribution to the core damage frequency for each of the PDS groups. The fractional contributions from the LOCA and Other transient groups tend to be less than their fractional contributions to the core damage frequency because for these PDSs, portions of the release are scrubbed by either the suppression pool or the pool formed by flooding the containment. The fractional contribution from the SBO PDS group tends to be greater than the fractional contribution to the core damage frequency because for these accidents the containment is open at the start of the accident, the auxiliary building fails early in the accident, the vessel always fails, CCI always occurs, and none of the releases are scrubbed by water. Therefore the releases associated with the SBO tend to be large relative to the other accidents analyzed in this study.

2.2.4 Qualitative Issues and Cautions

The results presented here for the Level 2/3 analysis are for a single POS (namely POS 5) and, as such, only assess the risk associated with this POS. While the Phase 1 screening study and other qualitative insights suggest that POS 5 is the risk-dominant mode of shutdown, no detailed study has been performed on the other POSs to confirm this belief.

Only accidents initiated from traditional internal events were analyzed in this study. Hence, the risk calculated for POS 5 is not complete in the sense that it does not include accidents initiated by internal fires and floods; it also does not include accidents initiated by seismic events.

It is important to realize that reducing the risk in one POS, for example by changing when equipment is available and unavailable, can shift the risk to another POS. Since this study only addresses the risk associated with one POS, the effect of this change on overall risk (i.e., risk across all the POSs) cannot currently be quantitatively assessed.

Since only a single plant was analyzed, these results cannot be considered generic and applicable to a population of plants. The plant and system models used in this study are based on the Grand Gulf plant as it operates in a selected mode of operation. Thus, while some insights may be applicable to other plants, in general, the results from this study should not be arbitrarily applied to other plants or conditions. The model used to develop the progression of the accidents after the onset of core damage is, in part, based on the Grand Gulf Emergency Operating Procedures and other procedures and practices at the plant. Changes in these procedures and practices can certainly affect the progression of the accident and the ultimate risk of the POS. Similarly, since the offsite consequences are sensitive to the site characteristics and surrounding region (e.g., weather, population, land use), for a given release of radioactive material, the consequences can be expected to vary from one site to the next.

2.3 General Conclusions

2.3.1 Level 1 Conclusions

The conclusions drawn from the Level 1 study can be grouped into three categories. They are (1) methodological, (2) plant specific, and (3) generic.

Methodological

This study was successful in developing a methodology to estimate the risk (i.e., the core damage frequency) associated with the operation of a BWR during low power and shutdown conditions. The methodology developed and the lessons learned from its application provide the NRC with new tools that could be used in subsequent analyses.

The mean CDF for each of the internal and external analyses presented in this report includes the fraction of time the plant is in POS 5 during a refueling outage. If one wanted to present the results as a conditional CDF (i.e., conditional on the plant being in POS 5), then the results should be divided by the value assigned to the POS 5 event. Thus, for example, for the total plant model for the traditional internal events analysis, the conditional CDF is (2E-6)/0.031 = 6.5E-5 per year in POS 5. However, use of the conditional CDF on a per year basis is *not* recommended since plant conditions (e.g., system unavailabilities and decay heat loads) would change dramatically during a year. However, it does show that the instantaneous CDF is higher in POS 5 than at full power.

Plant Specific

There are three major aspects of the specific Grand Gulf plant model used in this analysis that significantly affected the results. These are:

1. Grand Gulf's continued requirement for automatic isolation of low-pressure components in the shutdown cooling system, given an increase in pressure and/or a decrease in water level in POS 5.

2. Grand Gulf's requirement that at least two safety relief valves be available in POS 5 allows the operators to use portions of their inadequate decay heat removal procedure, which would otherwise be inaccessible.

3. Grand Gulf's additional system for removing decay heat (i.e., the alternate decay heat removal system) affects the estimated core damage frequency during two of the three POS 5 time windows.

Generic

The results from this study appear to indicate that the core damage frequency associated with operating in POS 5 during a refueling outage is less than that from operating at full power. While this should be true for Grand Gulf, generalizations to other BWRs should be performed with care.

Two factors that should be considered during any generalization are:

1. Does the other BWR have a motor-driven high-pressure pump? The availability of such a pump provides a mechanism for injecting water at high pressure, if necessary, and also provides an alternative means of injecting water at low pressure should the low-pressure pumps fail.

2. Does the other BWR have procedures in place to deal with the loss of the normal decay heat removal system? If the procedures do exist, does the utility require that the systems and components necessary for the procedure be available?

2.3.2 Level 2/3 Conclusions

The following conclusions can be drawn from this study:

- With many plant features unavailable to mitigate a release, the potential exists for a large release of radioactive material should core damage occur. For the most likely accidents, the containment is open, the suppression pool is bypassed, and the containment sprays are not available.

- In the event that the containment is closed prior to the onset of core damage, it is always predicted to fail since containment heat removal was not available in the accidents analyzed.

- The risks from POS 5 are not insignificant compared with the risks from full power operation. Hence the full-power risk distributions by themselves do not completely characterize the risks associated with the operation of this plant.

To accurately characterize the plant results from this study, it may be necessary to include other modes of operation in addition to the full-power mode. This can have important implications for assessments that rely on the total risk from a plant, such as when comparisons are made with the safety goals.

- Although only a simplified scoping study of the onsite consequences was performed, the possible consequences of an accident during shutdown could be significant, particularly since in many of the accidents the containment remains open, allowing an early release of radioactive material.

3. Surry Results and Conclusions

The results and conclusions presented below come directly from NUREG/CR-6144, Vols. 2 - 6.[8-13]

3.1 Level 1 Results

3.1.1 Results from Traditional Internal Events

Table 4 summarizes the results of the event tree quantification, showing the core damage frequency as a function of the initiating events and POSs. The core damage frequency is the frequency that core damage occurs while the reactor is at midloop, and includes the fraction of a year that the reactor is at midloop. POS 6 of a drained maintenance outage (D6), and POS 6 of a refueling outage (R6) are the most dominant POSs. Their characteristics are high decay-heat level and a relatively short time available for operator action. In contrast, POS 10 of a refueling outage (R10) has a very low decay heat, and its core damage frequency is approximately one order of magnitude lower.

Table 5 compares the results of this study with those of NUREG-1150[14] and the individual plant examination[15] performed by the utility for Surry. The results are displayed in two ways. The core damage frequency, shown in the first row, is the frequency with which core damage occurs when the plant is at midloop (the core damage frequencies in the parentheses are the contributions from overdraining events), and the conditional core damage frequency, shown in the third row, is the core damage frequency (minus the contribution of overdraining events) divided by the fraction of time the plant is at midloop. The former accounts for the fact that the plant is at midloop only a small fraction of the time, while the latter is the conditional frequency at which core damage occurs given the plant is at midloop. The core damage frequency of midloop operations is approximately one eighth of that of power operation as estimated in NUREG-1150, while the plant is in midloop operation approximately 7 percent of a year. The numbers in the parentheses of the third row of the table are the conditional probability of core damage from overdraining events, given that the plant enters midloop operation in the POS.

The core damage frequencies shown in the first row of Table 5 are additive. That is, the sum of the core damage frequencies of the 3 POSs is the total core damage frequency of midloop operation. This total, 5.06 E-06 per year, can be added to the core damage frequency of power operation, e.g., 4.01 E-05 per year for NUREG-1150. Therefore, the sum of 4.51 E-05 per year is the frequency per year that core damage occurs while the plant is at full power or mid-loop operation.

The conditional core damage frequency shown in the third row of Table 5 is a measure of how susceptible a plant configuration is with respect to core damage. For example, the fact that the conditional core-damage frequency of midloop operation, 7.62 E-05 per year, is higher than that of full power operation, 4.01 E-05 per year, shows that midloop operation is more susceptible to core damage than full power operation, although the plant is at midloop only a small fraction of the time.

Table 6 lists the conditional core damage frequency as a function of the time windows and POSs. The conditional core damage frequency is the rate at which core damage occurs given that the plant is in the time window of the POS. It is obtained by dividing the core damage frequency by the fraction of time the plant is in the time window of the POS. The conditional core damage frequency/probability is a measure that can be used to compare the vulnerability of the time windows and POSs with respect to core damage. It can be seen from Table 6 that for each POS the conditional core damage frequency decreases with the time window. This is due to the relaxed success criteria and more time available for operator actions. The conditional core damage frequency/probability for R6 or R10 is higher than that of D6 mainly because the RCS loops have a high probability of being isolated in a refueling outage; that makes reflux cooling impossible. For example, in window 1, the probability that the loops are isolated in a refueling outage is 0.3, and the

Table 4 Summary of Results--Core Damage Frequency by Initiating Event and Plant Operational States

	Initiating Event	Core Damage Frequency (per year)			
1.	Loss of residual heat removal (RHR)	R6	R10	D6	Total
	RHR2A-Over Draining	1.8E-7	5.3E-8	2.6E-7	4.9E-7
	RHR2B-Failure to Maintain Level	2.1E-8	2.0E-8	2.9E-8	7.0E-8
	RHR3-Nonrecoverable Loss of RHR	1.5E-7	8.4E-9	3.0E-7	4.6E-7
	RHR4-Nonrecoverable Loss of Operating Train of RHR	7.6E-9	1.2E-9	2.3E-8	3.2E-8
	RHR5-Recoverable Loss of RHR	4.0E-8	4.1E-9	9.3E-8	1.4E-7
2.	LOOP-Loss of Offsite Power				
	L1-Both 1H and 1J Energized	3.3E-7	7.0E-8	7.6E-7	1.2E-6
	L2-1H and 2H energized, not 1J	1.0E-7	1.3E-8	1.7E-7	2.9E-7
	L3-1H energized, not 1J, unit 2 blackout	4.2E-8	1.3E-8	9.9E-8	1.5E-7
	B1-Unit 1 Blackout	4.8E-8	1.1E-8	1.7E-7	2.3E-7
	B2-2 Unit Blackout	3.8E-8	4.2E-8	1.1E-7	1.9E-7
3.	4 kV-Loss of 4 kV Bus	1.4E-7	1.9E-8	2.4E-7	4.0E-7
4.	VITAL-Loss of Vital Bus	2.8E-8	5.1E-9	7.3E-8	1.1E-7
5.	AIR-Loss of Outside Instrument Air	7.9E-10	-	3.2-9	4.0E-9
6.	CCW-Loss of CCW	6.3E-8	1.1E-10	2.1E-7	2.7E-7
7.	SWGR-Loss of Emergency Switchgear Room Cooling	3.6E-8	1.2E-8	7.4E-8	1.2E-7
8.	ESFAS-Inadvertent Safety Feature Actuation	2.7E-7	2.7E-8	6.8E-7	9.8E-7
9.	Dilute-Boron Dilution (CDF)	-	-	-	6.8E-8
TOTAL		1.5E-6	3.0E-7	3.3E-6	5.1E-6[a]

[a]Not including boron dilution.

Table 5 Comparison of Total Core-Damage Frequency with NUREG-1150 and IPE

Study	Results				
PWR Low Power and Shutdown Study (Midloop POSs, Internal Event Only)		R6	R10	D6	TOTAL
	CDF[a] per year	1.49E-6 (1.82E-7)[b]	3.06E-7 (5.47E-8)[b]	3.25E-6 (2.67E-7)[b]	5.06E-6 (5.04E-7)[b]
	Fraction of a year the plant is in midloop	1.63E-2	1.52E-2	3.49E-2	6.64E-2
	Conditional CDF per year[c] (CDP)	8.09E-5 (3.03E-7)	1.65E-5 (1.82E-7)	8.55E-5 (2.23E-7)	7.62E-5 (2.40E-7)
NUREG-1150 (Internal Event Only)	4.01E-5				
IPE (Internal Event Only)	7.40E-5				

[a]CDF reflects the fraction of time the plant is at midloop.
[b]Contribution of overdraining events.
[c]Frequency of core damage given that the plant is at midloop.
CDP = probability of core damage resulting from overdraining to the POS

Table 6 Conditional Core Damage Frequency As a Function of the Time Windows and POSs (per year)

	R6	R10	D6	Total
Window 1 (13 hr-75 hr)	9.96E-4	-	3.37E-4	3.77E-4
Window 2 (75 hr-240 hr)	7.55E-5	-	5.90E-5	7.25E-5
Window 3 (240 hr-768 hr)	5.49E-5	6.54E-5	5.18E-5	5.60E-5
Window 4 (> 768 hr)	1.87E-5	1.57E-5	1.05E-5	1.80E-5
TOTAL	8.09E-5	1.65E-5	8.55E-5	7.62E-5

probability that reflux cooling fails in a drained maintenance outage is 0.1 (modeled as a recovery action). The difference between R6 and R10 in windows 3 and 4 is due to the difference in maintenance unavailabilities.

The total and subtotals in Table 6 represent the averaged conditional core damage frequency. For example, the averaged conditional core damage frequency for R6 is 8.09E-05 per year, while that for D6 is 8.55E-05 per year. This means that the plant is better off if it is in R6, given it is at midloop. This does not contradict the comparison made earlier for a given time window of the POSs, because given that plant is in D6, it is more likely to be in the earlier time windows that have higher conditional core damage frequency. The averaged conditional core damage frequency over the POSs, shown in the rightmost column of Table 6, does show a trend of decreasing with decay heat. The reversed trend for the averaged conditional core damage probability for windows 3 and 4 is caused by the same error introduced by truncation that made the trend reversed for the conditional core damage probability of R10 in windows 3 and 4.

Table 7 lists the key uncertainty characteristics of the core-damage frequencies for midloop operation and power operation, and shows that the core damage for midloop operation has a wider spread than that of power operation. Note also that the mean total CDF in Table 7 is slightly different for the total CDF in Tables 4 and 5. This is because the numbers in Tables 4 and 5 are point estimates whereas the information in Table 7 reflects an uncertainty analysis.

3.1.2 Results from Internal Fire Analysis

Table 8 summarizes the point estimate results of the fire analysis. Note that the CDF is the frequency at which core damage occurs when the plant is at midloop. It accounts for the fact that the plant is at midloop only a small fraction of the time. The quantification indicates that certain scenarios in the H and J compartments of the emergency switchgear room, one scenario in the cable vault and tunnel, and one containment scenario dominate the CDF. The most dominant scenarios occur in the cable vault and tunnel (owing to the proximity of many emergency cables from both divisions in a closed, constrained space) and in the J room of the ESGR, where many emergency cables from both the H and the J divisions come together in close proximity (before entering the control room). In the containment, the relatively high CDF is due to a relatively high scenario frequency combined with nonseparation of RHR trains over significant distances. Other scenarios are also important, owing to moderate damage from the fire combined with a relatively high scenario frequency.

POSs D6 and R6 are much more important than R10 (as R10 occurs in later time windows). D6 is more important than R6 owing to constraints imposed by a drained maintenance outage and its tendency to occur in earlier time windows.

The earlier time windows are more important than the later ones, with window 4 being relatively unimportant. Windows 1 and 2 are of the highest importance, with window 2 being significantly more important than window 1. While the decay heat is higher and the success criteria are more stringent in window 1, this window doesn't last as long and the outages tend to occur in the later time windows. The most risk significant fire initiator occurs in the cable vault tunnel area, in window 2 and POS D6, followed by a few scenarios in the J room of the ESGR, in the same window and POS.

Table 7 summarizes the result of the uncertainty analysis for core damage accidents initiated by fires. The results were obtained by performing uncertainty analysis using 500 Latin hypercube sampling (LHS) samples. Also shown in the table are the uncertainty analysis results of the internal event analysis as well as the mean value of the internal fire analysis of NUREG-1150.

Table 7 Result of the Level 1 Uncertainty Analysis and Comparison with Full Power Operation (per year)

	Study		Mean	5th Percentile	50th Percentile	95th Percentile	Error Factor
Internal Events	Full Power Operation - NUREG 1150 (per year)		4.01E-5	6.75E-6	2.31E-5	1.31E-4	4.41
	Full Power Operation - IPE		7.40E-5[a]	-	-	-	-
	Midloop Operation (per year while at midloop)		4.86E-6	4.76E-7	2.14E-6	1.54E-5	5.69
Internal Fires	Full Power Operation - NUREG 1150 (per year)		1.13E-5	-	-	-	-
	Full Power Operation - IPE		[b]	-	-	-	-
	Midloop Operation (per year while at midloop)		2.2E-5	1.4E-6	9.1E-6	7.6E-5	7.2
Internal Flood	Full Power Operation - NUREG 1150 (per year)		[c]	-	-	-	-
	Full Power Operation - IPE		5.0E05[b]	-	-	-	-
	Midloop Operation (per year while at midloop)		4.8E-6	2.2E-7	1.7E-6	1.8E-5	9.0
Seismic Events	Full Power Operation - NUREG 1150 (per year)	LLNL	1.2E-4	-	-	-	33
		EPRI	4.01E-5	-	-	-	4.41
	Full Power Operation - IPE		[b]	-	-	-	-
	Midloop Operation (per year while at midloop)[d]	LLNL	3.5E-7	1.3E-9	4.0E-8	1.4E-6	32
		EPRI	8.6E-7	2.5E-10	9.7E-9	3.7E-7	37

[a]Point estimate.
[b]Not available.
[c]Below truncation of 1.0E-8 per year.
[d]Refueling outage only (no drained maintenance).

Table 8 Summary of Point Estimate Core Damage Frequencies for Fire Events (per year)

Fire Area	R6	D6	R10	Total
Emergency Switchgear Room	4.1E-6	8.2E-6	2.1E-7	1.3E-5
Containment	7.0E-8	5.5E-7	5.0E-9	6.3E-7
Cable Vault and Tunnel	1.3E-6	2.7E-6	7.4E-8	4.0E-6
Normal Switchgear Room	1.5E-8	3.5E-8	1.4E-9	5.1E-8
Main Control Room	7.0E-8	5.3E-7	4.4E-9	6.0E-7
Total	5.5E-6	1.2E-5	2.9E-7	1.8E-5

No prevalence of fires at shutdown base was noticed in the data, compared with power operation fires (after the construction events are taken out). It is true that there is greater potential for fires in certain categories (e.g., transient fires, fires caused by welding igniting cables, or other equipment fires). It is also true that the possibility of some types of fires is reduced (e.g. deenergized equipment, oil dripping on hot piping). A fire at shutdown is liable to be detected much sooner and extinguished in its early phases because of increased floor traffic. [Credit is taken for this by disallowing events that were discovered in the smoking stage (without flames) or early enough so that deenergizing equipment extinguished the fire.] Increased vigilance by licensees may play a part in this also. At Surry, a fire watch is in place during welding operations; fire doors are kept closed.

Human error events are not prominent contributors individually in terms of the Fussell-Vesely importance range (a few percent). Part of the reason is that there are many human error probabilities (HEPs), each applicable in a small fraction of sequences; another reason is in the values assigned to the HEPs; the third is that in many important scenarios hardware failures dominate because of heavy damage by fire.

Table 7 provides a comparison of the fire-induced core damage frequency during midloop operation with that of power operation. Although the plant spends much less time in midloop, the core damage frequency is comparable to that of power operation. The main reason is that the routing of the cables of the equipment needed to support RHR operation or mitigate an accident during midloop operation is such that a single fire at a few critical locations can damage almost all the equipment needed, while during power operation there are fewer critical locations.

3.1.3 Results from Internal Flood Analysis

The main results of the flooding analysis are presented in Table 9, which lists the point estimate core damage frequencies of the operating states analyzed. It was found that the most dominant contributors to core damage from internal floods are accident scenarios initiated in the turbine building leading to the draining of the intake canal. This could result in a flood of the plant emergency switchgear rooms (ESGR), leading to a two-unit loss of all emergency power (F1 and F2 scenarios). The scenarios account for approximately 85 percent of the total CDF caused by internal floods. This result is mainly due to the specific features of the Surry circulating water system and may not be applicable to other plants. The second most dominating flood scenario involves flooding of the safeguard/auxiliary building in combination with the unavailability of the refueling water storage tank (RWST). The contribution of these scenarios (F4 and F5) is approximately 13 percent of the total internal CDF. Again, these specific findings may not be generalized to other plants because of the plant-specific nature of the actual evolvement of these accident scenarios.

The main results of the uncertainty analysis are shown in Table 7 and indicate the uncertainty bounds of the core damage frequency caused by internal floods. The important measures of the uncertainty distribution are the 5th percentile, mean, and 95th percentile values at 2.2E-07, 4.8E-06 and 1.8E-05/yr, respectively.

Table 9 Summary of Point Estimate Core Damage Frequencies for Flood Events (/yr)

Scenario	Core Damage Frequency with Recovery			
	POS 6 Refueling	POS 6 Drained	POS 10 Refueling	Total
Turbine Building (F1)	1.9E-6	9.3E-8	1.5E-6	3.5E-6
Turbine Building (F2)	4.5E-7	2.2E-8	3.6E-7	8.3E-7
Auxiliary Building (F3)	4.7E-8	4.3E-8	1.2E-8	1.0E-7
Auxiliary Building (F4)	1.6E-7	5.7E-8	6.7E-8	2.8E-7
Safeguard Area (F5)	2.0E-7	8.9E-8	9.4E-8	3.8E-7
Spray in Containment (F6)	-	-	-	-
Mechanical Equipment Room No. #3 (F7)	1.0E-8	1.5E-8	7.8E-9	3.3E-8
Total-Flood	2.8E-6	3.2E-7	2.0E-6	5.1E-6

The internal flood CDF is dominated by turbine building flood events. These events are primarily initiated by failure of either valves or expansion joints in the main inlet lines of the circulating water system. These failures may lead to pipe ruptures upstream of the condenser water box and inlet valves. At Surry the circulating water system is gravity fed from a very large capacity intake canal and it may not be isolated quickly enough. This is in contrast to other common design arrangements in which dedicated pumps provide the required cooling water for the system. In these designs, stopping the pumps would effectively isolate the system, limiting potential water outflow.

The potential draining of the intake canal inventory in the turbine building is dominant because of a plant-specific spatial interdependence. For both units the ESGR are located in the service building on the same elevation as the turbine building basement. These areas are separated by a fire door with 2-foot- high flood dikes in front of them. A large-scale flood could overflow the dikes and enter into the two-unit ESGR, leading to the potential loss of emergency power in both units, including the loss of residual heat removal (RHR) stub busses. The normal offsite power supply to the plant would not be affected since the normal switch gear room is located at a higher elevation in the service building.

Another important contributor to the internal flood CDF is flood events originating in or entering into the auxiliary building. These flood scenarios, mainly supply pipe ruptures from the RWST, result in the loss of all component cooling water (CCW) and consequently the RHR function at the plant. This, coupled with the unavailability of the RWST inventory to be injected into the reactor core, leads to core damage. Again, the plant-specific spatial arrangement of piping and equipment is the main reason for the development of the accident scenario and its risk significance.

3.1.4 Results from Seismic Analysis

Table 7 shows the base case results. The base case consists of the Surry plant (systems and fragilities) at the Surry site with Electric Power Research Institute (EPRI)[16] and Lawrence Livermore National Laboratory (LLNL)[17] seismic hazard curves. In this table, the mean, median, 5th percentile, and 95th percentile frequencies of the two plant operating states are shown. It is seen from the table that mean annual frequency of the two plant operating states is less than 10^{-6} per year using either the LLNL or the EPRI seismic hazard curves. Therefore, we conclude that the seismic contribution to mean annual core damage frequency during both POS 6 and POS 10 is very small at Surry Unit 1.

The comparison of CDF results is also shown in Table 7. From examining the table, several important observations emerge:

- During shutdown conditions, the total annual mean CDF arising from earthquakes is small compared with the CDF arising from internal initiators: a factor of about 15 smaller for the LLNL seismic hazard curves and a factor of about 60 smaller using the EPRI hazard curves.

- The seismic mean CDF during shutdown is small compared with the mean CDF at full power from seismic initiators from NUREG-1150: a factor of about 350 times smaller for the LLNL hazard curves and about 300 times smaller for the EPRI hazard curves.

- The error factor (EF) in this seismic study is significantly greater than the EF in the CDF from internal initiators during shutdown This is primarily caused by the large uncertainty in the seismic hazard curves but another contribution arises from the uncertainty in the seismic fragilities.

A number of important insights emerge from this Surry analysis, including:

Core-damage frequency

The core damage frequency for earthquake-initiated accidents during refueling outages in POS 6 and POS 10 is found to be low in absolute terms, below 10^{-6}/year. The reasons for this are (1) Surry's capacity to respond to earthquakes during shutdown is excellent, well above its design basis and similar to its ability to respond to earthquakes during full power conditions; (2) the Surry site is one of the least seismically active locations in the United States; (3) the Surry plant is only in POS 6 and POS 10 (combined) for an average (mean) of 6.6 percent of the time. The core damage frequencies are also low relative to the frequencies during POS 6 and POS 10 for internal initiators. This can be seen in Table 7.

The results are plant-specific

We believe that the results for Surry are highly plant-specific, in the sense that the seismic capacities, the specific sequences that are found to be most important, and the seismicity of the site are all difficult to generalize to other reactors elsewhere.

Shutdown seismic sequences are similar to full-power seismic sequences

Nevertheless, it is important to observe that all of the sequence types, components, and human errors that emerge in the key sequences in this analysis are similar or identical to sequences, components, and human errors that appear in typical full-power seismic PRAs. That is, nothing that has arisen as important in this study appears to be unique to earthquakes occurring during shutdown conditions. Whether this observation can be generalized to other reactors at other sites is not known to us.

Sensitivities

Sensitivity studies reveal that if the Surry reactor were moved to the Zion site in Illinois (a typical Midwestern site) or the Pilgrim site in Massachusetts (one of the most seismically active sites among all of the reactor sites in the eastern United States), the mean annual CDF from this study would increase by factors of about 1.8 and 10, respectively.

Uncertainties

While there are significant uncertainties in the numerical values of core-damage frequencies found in this study (see Table 7), the above conclusions are relatively robust --- they do not depend on the detailed numerical values found.

3.2 Level 2/3 Results

Table 10 presents statistical measures of the distributions for seven consequence measures for accidents during mid-loop operation obtained from this study. Similar statistical measures for full power operation obtained from the NUREG-1150 study of Surry are also included in the table. Table 10 indicates that the mean risk of offsite early health effects is over two orders of magnitude lower for accidents during mid-loop operation than for full power. This is due to the natural decay of the radionuclide inventory (because the accidents occur a long time after shutdown) particularly the short-lived isotopes of iodine and tellurium, which are primarily associated with early health effects. The distributions obtained for population dose (50 miles and 1000 miles) for mid-loop and full power operation are very similar. However the distributions for latent cancer fatalities differ by a factor of about three. The mid-loop study used the latest version of the MACCS code, which incorporates the BEIR V update to the latent cancer versus dose relationship, whereas NUREG-1150 used an older version of MACCS. The latest BEIR V update gives approximately a factor of three higher latent cancers for the same value of population dose.

In addition, scoping estimates of onsite doses were performed which indicate that the parking lot dose rates for accidents involving unisolated containment were high. This would limit the ability to take corrective actions, which cannot be performed from the control room, for this class of accidents.

The main finding of the study is that during mid-loop operation the risk of consequence measures related to long-term health effects, latent cancer fatalities and population dose, are high, comparable to those at full power, despite the much lower level of the decay heat and the radionuclide inventory. The reason for this is that containment is likely to be unisolated for a significant fraction of the accidents initiated during mid-loop operation so the releases to the environment are potentially large and the radionuclide species which mostly contribute to long-term health effects (such as cesium) have long half-lives. Accident sequences involving failure to correctly diagnose the situation or take proper actions are the largest contributors to the risk. Another finding of the study is that the risk of early fatalities is low despite the unisolated containment due to the decay of the short-lived radionuclide species such as iodine and tellurium which contribute to early fatality risk. The calculated risk estimates have a range of uncertainty extending over approximately two orders of magnitude from the 5th to the 95th percentile of the distribution.

Table 10 Comparison of Distributions of Risk for Mid-Loop and Full-Power Operation (All Values per Reactor Year; Population Doses in P-Sv per Year)

	Sample 5th Percentile		Sample Median		Sample Mean		Sample 95th Percentile		Standard Deviation	
	Mid-Loop	Full-Power	Mid-Loop	Full-Power	Mid-Loop	Full-Power	Mid-Loop	Full-Power	Mid-Loop	Full-Power
Early Fatalities	1.26E-10	7.60E-10	3.57E-09	7.00E-08	4.90E-08	2.00E-06	1.59E-07	5.40E-06	1.69E-07	N.A.
Latent Fatalities within 50 mi	1.55E-04	N.A.	8.34E-04	N.A.	2.46E-03	N.A.	8.78E-03	N.A.	3.68E-03	N.A.
Latent Fatalities within 1000 mi	7.97E-04	3.10E-04	5.35E-03	2.20E-03	1.57E-02	5.20E-03	5.50E-02	1.90E-02	2.52E-02	N.A.
Population Dose within 50 mi	3.77E-03	5.90E-03	1.98E-02	2.70E-02	5.79E-02	5.80E-02	1.89E-01	2.50E-01	8.77E-02	N.A.
Population Dose within 1000 mi	1.87E-02	1.90E-02	1.25E-01	1.30E-01	3.66E-01	3.10E-01	1.29E+00	1.20E+00	5.90E-01	N.A.
Individual Early Fatalities Risk within 1 mi*	6.00E-12	1.40E-11	1.27E-10	8.70E-10	1.74E-09	1.60E-08	6.94E-09	4.90E-08	5.52E-09	N.A.
Individual Latent Fatalities Risk within 10 mi*	1.20E-10	1.60E-10	7.48E-10	4.90E-10	2.09E-09	1.70E-09	7.10E-09	8.10E-09	3.01E-09	N.A.

N.A. – Not Available

*NRC quantitative health objectives:

- Individual early fatality risk within one mile to be less than 5×10^{-7} per reactor year.
- Individual latent cancer fatality risk within 10 miles to be less than 2×10^{-6} per reactor year.

Containment Status

The major factor driving the risk is the status of containment during mid-loop operation. It was judged that there is a high probability that the containment is either unisolated or that it would not have full pressure retaining capability during mid-loop operation. This is particularly the case if the operators fail to diagnose the accident as it was judged unlikely that they would take action to isolate containment or could succeed in doing so within the available time frame. This factor played a significant role in influencing the risk estimates of mid-loop operation. During the course of the study, Surry plant personnel made available new procedures for containment closure during mid-loop operation. However, it was difficult to assess the adequacy of these procedures in ensuring the pressure retaining capability of the containment within the time frame encompassed by this study. This feature contributed significantly to the uncertainty in containment status and the estimate of risk.

Availability of Containment Sprays

There is no requirement at Surry for the containment sprays to be available during shutdown. Plant records show that the spray systems could be inoperable because of maintenance. Spray availability was modeled as an uncertainty parameter in the risk analysis. Since the sprays perform an important safety function in mitigating the effects of releases, spray unavailability contributed both to the risk and its uncertainty.

Possibility of Core Damage Arrest

The inclusion of the possibility of arresting the core degradation process before vessel failure is an important feature of this analysis as it was for the full power study. Termination of the accident in-vessel can significantly reduce some of the fission product releases and thus the risk. The potential for core recovery depends on the nature of the accident progression and is different for the various PDS Groups. Overall, the conditional probability of core damage arrest ranged from 0.23 (5th percentile) to 0.44 (95th percentile) with a mean of 0.35.

Comparison with Full Power Study

The mean core damage frequency for accidents during mid-loop operation is about an order of magnitude lower than the mean frequency of accidents caused by internal events at full power. However, the risk distributions obtained for comparable long term health consequences are very similar in the two studies. What this finding implies is that the lower decay heat and lower radionuclide inventory of the mid-loop operating state, compared with full power, is offset by the lack of mitigative features. Finally, the mean risk of early health effects is over two orders of magnitude lower for accidents during mid-loop operation than for accidents during full power operation. This is due to the natural decay of those radionuclide species which have the greatest impact on early fatality risk because accidents during mid-loop operation occur a long time after shutdown.

Comparison With the Safety Goals

Comparison of the results of this study against the NRC safety goals is done only for the two quantitative health objectives identified in the Commission's policy statement of August 1986. These objectives deal with individual early fatality and latent cancer fatality risks within 1 mile and 10 miles of the site, respectively. The numerical value of these objectives are given in Table S.1. The 95th percentile of the distribution for individual latent cancer fatality risk falls more than an order of magnitude below the objective. The 95th percentile of the distribution for individual early fatality risk falls over two orders of magnitude below the corresponding health objective. The health objectives, however, apply to the total risk of the Surry plant. The risk estimates of this study are for accidents initiated by internal events during mid-loop operation and therefore reflect only a fraction of the total risk at Surry.

3.3 CONCLUSIONS

This study was successful in developing a methodology to estimate the risk associated with the operation of a PWR during midloop operation. The methodology developed and the lessons learned from its application provide the NRC with new tools that could be used in subsequent analyses. The study concentrated the effort on midloop operation only. The core damage frequency contributions of other low-power and shutdown POSs were analyzed only in the coarse screening analysis of the Phase 1 study, and remain to be analyzed in the future.

The following sections summarize the conclusions of the study.

3.3.1 Level 1 Conclusions

Internal Events

This study shows that the core damage frequency resulting from internal events during midloop operation at the Surry plant is lower than that of power operation. This is mainly due to the much smaller fraction of time that the plant is at midloop. The conditional core damage frequency, which provides a measure of the vulnerability of the plant configuration with respect to core damage, is actually higher than that of power operation.

The time window approach developed in this study provides a more realistic approach to accounting for the changing decay heat during shutdown. Without it, the core damage frequency estimates could be an order of magnitude higher.

This study discovered that only a few procedures are available for mitigating accidents that may occur during shutdown. Procedures written specifically for shutdown accidents would be useful and should be based on realistic thermal hydraulic analyses.

We assumed that a reduced-inventory checklist was followed, and found that for equipment not on the checklist, maintenance unavailability was a dominant contributor to system unavailability. However, the checklist is believed to be sufficient for ensuring the availability of essential equipment. The dominant cause of damage is operator errors. We recognize that there is very large uncertainty in the human error probabilities used in this study.

Internal Fires

A comparison of the fire-induced core damage frequency during midloop operation with that of power operation shows that, although the plant spends much less time in midloop, the core damage frequencies are comparable. The main reason is that the routing of the cables of the equipment needed to support RHR operation or mitigate an accident during midloop operation is such that a single fire at a few critical locations can damage almost all the equipment needed, while during power operation there are fewer critical locations.

Risk-significant scenarios are found mainly in the ESGR and the cable vault and tunnel (CVT). In the ESGR, several important scenarios (which are also the most risk-significant ESGR scenarios) occur in locations where many cables for the H and the J emergency divisions come together in a close proximity. In the CVT, the tunnel part is a constrained space, where damage would quickly propagate to both divisions (serving many different pieces of emergency equipment). In the containment, the risk significance stems from the relatively high fire frequency and nonseparation of the two RHR divisions. POSs D6 and R6 are much more risk significant than R10, with POS D6 more significant than R6.

Windows 1, 2, and 3 are much more important than window 4, and windows 1 and 2 are more important than window 3. Window 2 is the most risk-significant window.

Internal Floods

The internal flood CDF is dominated by turbine building flood events. These events are primarily initiated by either valve or expansion joint failures in the main inlet lines of the circulating water system. These failures may lead to pipe ruptures upstream of the condenser water box and inlet valves. At Surry the circulating water system is gravity fed from a very large capacity intake canal and it may not be isolated quickly enough. This is in contrast to other common design arrangements where dedicated pumps move the required cooling water through the system.

The potential draining of the intake canal inventory in the turbine building is dominant because of a plant-specific spatial interdependence. For both units the ESGR are located in the service building on the same elevation as the turbine building basement. These areas are separated by a fire door with 2-foot-high flood dikes in front of them. A large-scale flood could overflow the dikes and enter into the two-unit ESGR, leading to the potential loss of emergency power in both units, including the loss of stub busses that support the RHR pumps. The normal offsite power supply to the plant would not be affected since the normal SGR is located at a higher elevation in the service building.

The flood-initiating event analysis indicated that the shutdown, and specifically the midloop operational period, does not pose a unique flood risk with the exception of flood events coupled with loop isolation in time windows 2, 3, and 4. In general, the risk from flood events is relatively significant and is dominated by potential flood events into the ESGR coupled with loop isolation.

Seismic Events

The core damage frequency for earthquake-initiated accidents during refueling outages in POS 6 and POS 10 is found to be low in absolute terms, below 10^{-6}/year. The reasons for this are (1) Surry's capacity to respond to earthquakes during shutdown is excellent, well above its design basis and similar to its ability to respond to earthquakes during full-power conditions; (2) the Surry site is one of the least seismically active locations in the United States; (3) the Surry plant is only in POS 6 and POS 10 (combined) for an average (mean) of 6.6 percent of the time.

The seismic mean CDF during shutdown is small compared with the mean CDF at full power from seismic initiators from NUREG-1150: a factor of about 350 times smaller for the LLNL hazard curves and about 300 times smaller for the EPRI hazard curves.

3.3.2 Level 2/3 Conclusions

The following conclusions can be drawn from this study:

- With many plant features unavailable to mitigate a release, the potential exists for a large release of radioactive material should core damage occur. The containment is likely to be unisolated for a significant fraction of the accidents initiated during mid-loop operation.

- The risks from mid-loop operation are not insignificant compared with the risks from full power operation. Hence the full-power risk distributions by themselves do not completely characterize the risks associated with the operation of this plant. To accurately characterize the plant results from this study, it may be necessary to include other modes of operation in addition to the full-power mode. This can have important implications for assessments that rely on the total risk from a plant, such as when comparisons are made with the safety goals.

- Although only a simplified scoping study of the onsite consequences was performed, the possible consequences of an accident during mid-loop operation could be significant, particularly since in many of the accidents the containment is not isolated, which allows an early release of radioactive material.

4. References

[1] D. W. Whitehead et al., "Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Grand Gulf, Unit 1 Main Report (Sections 1-9)," NUREG/CR-6143, SAND93-2440, Vol. 2, Part 1A, Sandia National Laboratories, June 1994.

[2] D. W. Whitehead et al., "Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Grand Gulf, Unit 1 Main Report (Sections 11-14)," NUREG/CR-6143, SAND93-2440, Vol. 2, Part 1C, Sandia National Laboratories, June 1994.

[3] J. Lambright et al., "Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Grand Gulf, Unit 1 Analysis of Core Damage Frequency from Internal Fire Events for Plant Operational State 5 During an Refueling Outage," NUREG/CR-6143, SAND93-2440, Vol. 3, Sandia National Laboratories, July 1994.

[4] V. Dandini et al., "Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Grand Gulf, Unit 1 Analysis of Core Damage Frequency from Internally Induced Flooding Events for Plant Operational State 5 During an Refueling Outage," NUREG/CR-6143, SAND93-2440, Vol. 4, Sandia National Laboratories, July 1994.

[5] R. J. Budnitz et al., "Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Grand Gulf, Unit 1 Analysis of Core Damage Frequency from Seismic Events for Plant Operational State 5 During an Refueling Outage," NUREG/CR-6143, Vol. 5, Future Resources Associates, Inc., Berkeley, CA, August 1994.

[6] T. D. Brown et al., "Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Grand Gulf, Unit 1 Evaluation of Severe Accident Risk for Plant Operational State 5 During an Refueling Outage Main Report," NUREG/CR-6143, SAND93-2440, Vol. 6, Part 1, Sandia National Laboratories, to be published.

[7] T. D. Brown et al., "Evaluation of Severe Accident Risks: Grand Gulf Unit 1," NUREG/CR-4551, SAND86-1309, Vol. 6, Rev. 1, Sandia National Laboratories, December 1990.

[8] T.L Chu et al., "Evaluation of Potential Severe Accidents during Low Power and Shutdown Operations at Surry Unit-1, Analysis of Core Damage Frequency from Internal Events During Mid-Loop operations, Main Report (Chapter 1-6)," NUREG/CR-6144, BNL-NUREG-52399, Vol. 2, Part 1A, Brookhaven National Laboratory, June, 1994.

[9] T.L Chu et al., "Evaluation of Potential Severe Accidents during Low Power and Shutdown Operations at Surry Unit-1, Analysis of Core Damage Frequency from Internal Events During Mid-Loop operations, Main Report (Chapter 7-12)," NUREG/CR-6144, BNL-NUREG-52399, Vol. 2, Part 1B, Brookhaven National Laboratory, June, 1994.

[10] Z. Musicki et al., "Evaluation of Potential Severe Accidents during Low Power and Shutdown Operations at Surry Unit-1, Analysis of Core Damage Frequency from Internal Fires During Mid-Loop operations, Main Report," NUREG/CR-6144, BNL-NUREG-52399, Vol. 3, Part 1, Brookhaven National Laboratory, July, 1994.

[11] P. Kohut, "Evaluation of Potential Severe Accidents during Low Power and Shutdown Operations at Surry Unit-1, Analysis of Core Damage Frequency from Internal Floods During Mid-Loop operations," NUREG/CR-6144, BNL-NUREG-52399, Vol. 4, Brookhaven National Laboratory, July, 1994.

[12] R. J. Budnitz et.al., "Evaluation of Potential Severe Accidents during Low Power and Shutdown Operations at Surry Unit-1, Analysis of Core Damage Frequency from Seismic Events During Mid-Loop operations," NUREG/CR-6144, Vol. 5, Future Resources Associates Inc., August, 1994.

[13] J. Jo et.al., "Evaluation of Potential Severe Accidents during Low Power and Shutdown Operations at Surry Unit-1, Evaluation of Severe Accident Risks During Mid-loop Operations," NUREG/CR-6144, BNL-NUREG-52399, Vol. 6, Brookhaven National Laboratory, to be published.

[14] U. S. Nuclear Regulatory Commission, "Severe Accident Risks: An Assessment for Five U. S. Nuclear Power Plants," NUREG-1150, Vols. 1-3, December 1990-January 1991.

[15] Virginia Power, Surry Nuclear Power Plant, Individual Plant Examination Program, August 1991.

[16] Electric Power Research Institute, "Probabilistic Seismic Hazard Evaluations at Nuclear Power Plant Sites in the Central and Eastern United States: Resolution of the Charleston Earthquake Issue," Prepared by Risk Engineering, Inc., Yankee Atomic Power Company and Woodward Clyde Consultants, EPRI Report NP-6395-D, April 1989.

[17] D.L. Bernreuter, J.B. Savy, R.W. Mensing and J.C. Chen, "Seismic Hazard Characterization of 69 Nuclear Plant Sites East of the Rocky Mountains," NUREG/CR-5250, Lawrence Livermore National Laboratory, January 1989.

[18] Chanin, D., J. Rollstin, J. Foster, and L. Miller, "MACCS Version 1.5.11.1: A Maintenance Release of the Code," NUREG/CR-6059, October 1993.

[19] National Research Council Committee on Biological Effects of Ionizing Radiation (BEIR V), "Health Effects of Exposure to Low Levels of Ionizing Radiation," National Academy of Sciences, Washington, DC, 1990.

IMPROVING THE ACTION REQUIREMENTS OF TECHNICAL SPECIFICATIONS: A RISK-COMPARISON OF CONTINUED OPERATION AND PLANT SHUTDOWN*

I.S. Kim, T. Mankamo** and P.K. Samanta
Department of Advanced Technology
Brookhaven National Laboratory
Upton, New York 11973

**Avaplan Oy, Finland

Abstract

When the systems needed to remove decay heat are inoperable or degraded, the risk of shutting down the plant may be comparable to, or even higher than, that of continuing power operation with the equipment inoperable while giving priority to repairs. This concern arises because the plant may not have sufficient capability for removing decay heat during the shutdown. However, Technical Specifications (TSs) often require "immediate" shutdown of the plant. In this paper, we present risk-based analyses[1] of the various operational policy alternatives available in such situations, with an example application to the standby service water (SSW) system of a BWR. These analyses can be used to define risk-effective requirements for those standby safety systems under discussion.

1. Introduction

1.1 Current Requirements and Definition of the Problem

Limiting conditions for operation (LCOs) define the allowed outage times (AOTs) and the actions to be taken if the repair cannot be completed within the AOT. Typically, the action required is plant shutdown. However, in situations where the risk associated with the action, i.e., the risk of plant shutdown given a failure in the safety system, may be substantial, a strategy is needed to control the risk implications. When a system needed to remove decay heat is inoperable or degraded at power, shutting down the plant may not necessarily reduce risk, compared to continuing power operation and giving priority to completing the repairs. Analyzing these TS requirements and exploring various available alternatives is the focus of this paper.

For example, for a residual heat removal (RHR) system of a BWR plant in the United States consisting of three trains, a 3-day AOT is defined for single-train failures. However, the action statement requires that the plant is shut down when failures are detected in multiple (i.e., two or three) trains.

These action requirements primarily are directed towards minimizing the risk during power operation, assuming that shutting down the plant is relatively safe; namely, the risk of shutdown is

*This work was performed under the auspices of the U.S. Nuclear Regulatory Commission.

assumed to be negligible. This is not necessarily a reasonable assumption for such a system that removes decay heat. A comparative analysis of risk impacts of action alternatives can address these failure situations.

1.2 Failures in Systems for Removing Decay Heat

When failures occur in the following systems, the ability of the plant to remove decay heat may be impaired:

1) RHR system of a BWR or PWR that provides long-term removal of decay heat

2) Auxiliary feedwater (AFW) system of a PWR which provides feedwater to steam generators to remove decay heat from the primary system

3) Component cooling water (CCW) system of a PWR that provides cooling water to the RHR system

4) Standby service water (SSW) system of a BWR or PWR that subsequently removes heat from the RHR or CCW system for the BWR or PWR, respectively

5) Emergency power system of a BWR or PWR that provides electric power to the systems used to remove decay heat following a reactor scram

Shutting down the plant in such failures may impose substantial risk, which may be comparable or exceed the risk associated with continuing power operation and giving priority to the repairs. Hence, in evaluating the AOTs or action statements for these systems, the shutdown risk can be taken into account explicitly and compared with the risk of continued power operation.

2. Basic Concepts of the Comparative Analysis of LCO Risks

2.1 Comparison of Conditional LCO Operating and Shutdown Risks

When a safety system enters an LCO because of failure of one or more components in the system, TSs allow for one of the two alternatives: a) continue power operation and repair the failed equipment within the defined AOT, or b) shut down the plant to complete the repairs in a shutdown state. We call these alternatives the basic operational alternatives, and the risks associated with these alternatives the LCO risks. The risk associated with repairing the equipment while continuing power operation is called LCO operating risk; the risk associated with shutting the plant down is called LCO shutdown risk.

Figure 1 shows a conceptual plot of LCO operating and shutdown risks in terms of core-damage frequency for failure of a system which is needed to remove decay heat. At time A when the failure is detected, the two basic operational alternatives are applicable, i.e., continued power operation, and plant shutdown. The solid line represents the risk profile for continued operation, while the dotted line is the profile for the shutdown.

Upon detecting the failure at time A, the LCO operating risk increases above the baseline due to the increased unavailability of the initially affected (i.e., failed or degraded) system during potential

occurrences of accident scenarios requiring it to be operational to prevent core damage. The baseline represents the level of risk associated with power operation when no known failures exist.

The initial increase in the LCO shutdown risk (Figure 1) results from the system's unavailability during the potential occurrences of accident scenarios initiated by events occurring while the plant is being brought to shutdown. Specifically, the increase in risk in the initial stage of shutdown arises from: 1) the unreliability of the systems which are needed during the change in plant's state, or which must be started up, and 2) the vulnerability of the plant to transients caused by the changes in the plant's state. After entering a stable shutdown state, the risk level usually decreases with time because of the diminishing decay heat, meaning lower capacity requirements on safety systems, and longer time available for recovery if a critical safety function is lost during a shutdown-cooling mission. Obtaining a lower risk level in a stable shutdown mode, compared to the continued-operation alternative, is the principal motivation of going to shutdown.

At time B, when the component is repaired and returned to service, both operating and shutdown risks decrease. The operating risk decreases to the baseline risk level, i.e., the level before the failure was detected, whereas the shutdown risk decreases below the baseline risk level for the power operational mode, because of the much lower rate of heat production in the reactor during shutdown compared to power operation. Another small peak in the shutdown risk at time C arises from the unavailabilities of systems that are needed when the plant is restarted up, and the plant's vulnerability to transients that may be caused by the changes in the operational mode. In this period, the risk is also a function of the rate of heat production, as represented by a small dip which then slowly increases to the baseline risk level as the plant reaches full power operation.

The period that is directly relevant to evaluating action requirements or AOTs for failures in the safety systems is from time A to time B, i.e., the predicted or actual repair time for the component. The risk over this period, i.e., core-damage probability, can be obtained by integrating the conditional CDF to compare the LCO operating and shutdown risks. If the operating risk is smaller than the shutdown risk, then, from a risk point of view, the alternative of continued operation is preferable to the shutdown alternative, and vice versa.

2.2 Comparison of LCO Operating and Shutdown Risks

Figure 2 compares the core-damage probability (CDP) contributions over the repair time, beginning from time A when the failure is detected. The CDP for operating risk is smaller than that for shutdown risk until time X, when the two curves intersect. Therefore, from a risk perspective, it is more beneficial to continue power operation than to shut down the plant if the operability of the initially affected system can be restored before time X. Where the repair takes longer than the period A to X, it is advisable to shut down the plant.

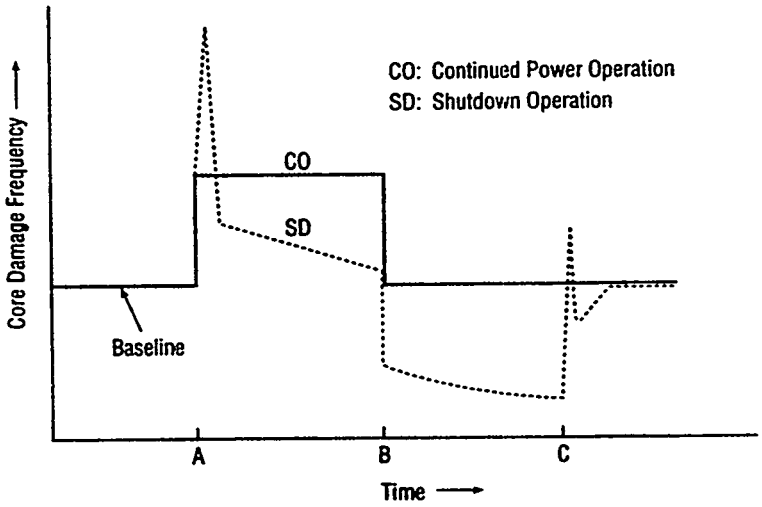


Figure 1 Comparison of LCO risks (core-damage frequency) for the basic operational alternatives of continued power operation and shutdown

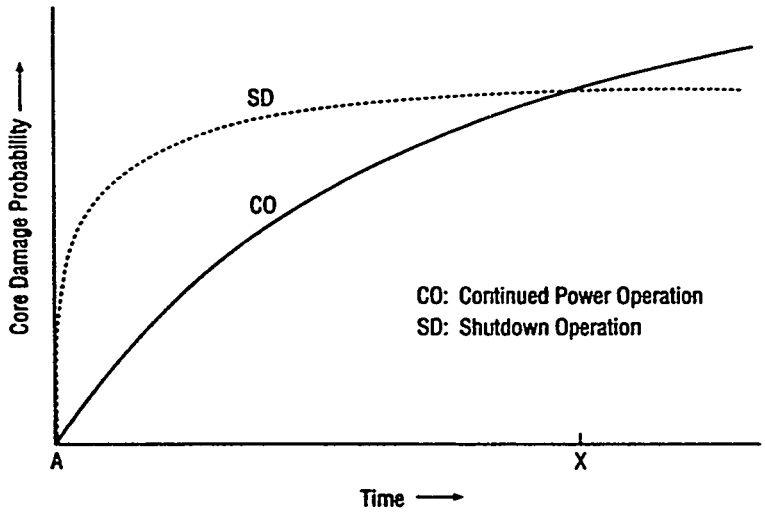


Figure 2 Comparison of LCO risks (core-damage probability) for the basic operational alternatives of continued power operation and shutdown

2.3 Other Considerations in Defining Action Requirements

The risk profiles discussed above are based on several assumptions. An important assumption was that, in the case of the shutdown alternative, the plant is shut down directly after the failure is detected. However, in general, some AOT may be useful so that plant personnel can evaluate the repairs needed and restore the operability of the failed equipment without shutting down the plant, at least for short repairs.

Suppose that 3 days of AOT is given for a failure situation in the technical specifications and that the plant personnel cannot repair the component within the AOT. They may shut down the plant three days after finding the failure. In this case, the failure will incur LCO operating risk from the time the failure was detected until the shutdown is initiated, and also LCO shutdown risk. Compared to a plant shutdown right after the failure detection, this case will incur a larger risk by the risk accumulated before the plant is actually shut down. Hence, the timing of shutdown should be considered in determining risk-effective action requirements that will minimize the total risk impact associated with a given failure.

Furthermore, oftentimes we do not know exactly how long the repair of certain failures will take. The distribution of repair time should be considered in assessing the risk associated with the failures. In addition to the timing of shutdown and the repair time, other issues should be taken into account in determining risk-effective action requirements, e.g., whether the status of redundant train(s) should be checked, and whether the plant should go to hot shutdown or cold shutdown as the optimum target state. These issues can be addressed by sensitivity analyses.

3. Example Application to Standby Service Water System

The method for evaluating LCO operating and shutdown risks, called risk-comparison approach, was applied to the standby service water (SSW) system of a BWR. The event sequences were modeled using shutdown transient diagrams and extended event sequence diagrams, particularly focussing on the transients that may occur during the transition to shutdown.

In this section, we present the results of quantifying the LCO operating and shutdown risks for failures in the SSW system, after briefly introducing the system and the present action requirements. We then summarize the practical insights from these analyses to control the risk implications of such failures. A detailed description of the sequence modeling and sensitivity analyses can be found in Reference 2.

3.1 Standby Service Water System and Present Action Requirements

The SSW system, consisting of three subsystems, A, B, and C, removes heat from plant equipment that require cooling water for a safe reactor shutdown. SSW pumps A and B each has a 12,000 gpm capacity, while SSW pump C, dedicated to the high pressure core spray (HPCS) system, has a much smaller (1,300 gpm) capacity.

The SSW subsystems, especially A and B, provide cooling water to many safety-significant components, such as the heat exchangers of the RHR system, room/pump coolers for the low-pressure core-spray (LPCS) and reactor-core-isolation cooling (RCIC) systems, and jacket coolers of diesel generators. Hence, a failure or degradation in the SSW system will affect the operability of other systems

which are supported by the SSW system. For example, the failure of SSW subsystem A also will cause RHR subsystem A and DG subsystem A to be inoperable along with front-line systems, LPCS and RCIC.

Table 1 summarizes the action requirements for the SSW system which are applicable to the power operation mode. For a single failure, i.e., when SSW subsystem A, B, or C is inoperable, the TS allows 3 days; if the operability of the failed subsystem cannot be restored within 3 days, then the plant must be shut down.

Table 1 Action Requirements for the SSW System

Inoperable SSW Subsystems	AOT
A or B or C	3 days
"A and C" or "B and C"	3 days
A and B[a]	0 hours
A, B, and C[a]	0 hours

[a]Whenever both SSW subsystems (A and B) are inoperable, if cold shutdown cannot be attained as required by this action, the reactor's coolant temperature should be kept as low as practical by using alternate methods of heat removal.

For double failures of the SSW system, the TS gives different AOTs, depending on which subsystems are inoperable. When SSW trains A and C, or B and C are down, the plant may continue power operation with the equipment inoperable up to 3 days; namely, these double failures have the same AOT as the single failures.

When SSW subsystems A and B, or all SSW subsystems (triple failures) are inoperable, the TS requires "immediate" plant shutdown (0 hours of AOT). Then, the TS also limits the timing of shutdown so that the plant at least should be in hot shutdown within the next 12 hours, and in cold shutdown within the following 24 hours.

3.2 Risk Comparison of the Basic Operational Alternatives

Table 2 gives the LCO operating and shutdown risks for failures in the SSW system. Figures 3 and 4 show how the conditional core-damage frequency and core-damage probability change for the continued power operation (CO) and shutdown (SD) alternatives in single, double, and triple failures of the SSW system.

Table 2 Risk Quantification for Failures in the SSW System

LCO State (Failures of SSW Trains)	Core-Damage Frequency in Power Operation State (per year)	CDF Increase Factor	Crossing Point of the SD/CO Alternatives (days)
Baseline	2.1E-6	1.0	N/A
Single (A)	1.5E-5	7.4	~3
Double (AB)	3.3E-4	160	~3
Triple (ABC)	7.4E-3	3600	~14

Core-Damage Probability per Failure Situation		
Continued Operation (CO)	Controlled Shutdown (SD)	CDP Ratio (SD/CO)
N/A	N/A	N/A
2.3E-8	5.7E-8	2.5
4.5E-7	9.6E-7	2.1
1.1E-5	3.3E-5	3.0

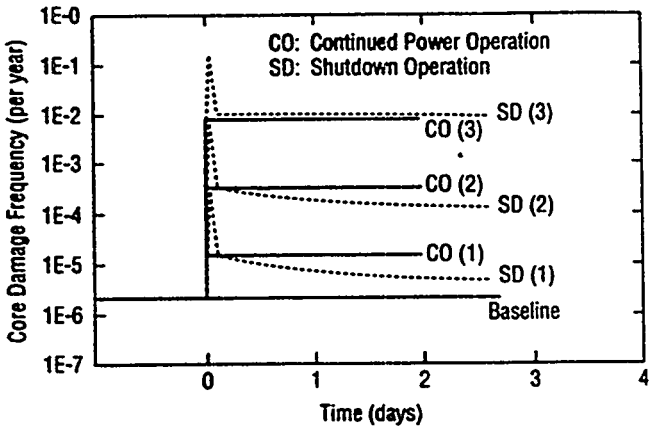


Figure 3 Conditional core-damage frequency for the continued operation and shutdown alternatives in failures of the SSW system (For example, CO(2) denotes the CO alternative for double-train failures)

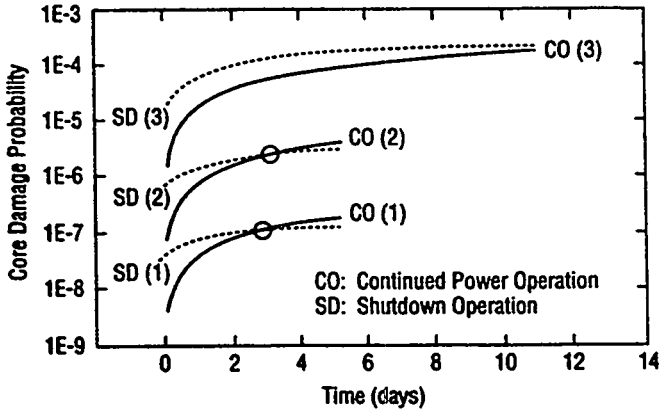


Figure 4 Cumulative core-damage probability over predicted repair time in failures of the SSW system (For example, SD(2) denotes the SD alternative for double-train failures).

1. Single-Failure Situation: Where one SSW train (e.g., train A) is detected failed during power operation, the core-damage frequency increases by a factor of about 7 over the baseline (see, Table 2). If the CO alternative is taken, the core-damage frequency will remain at this level until the operability of the failed train is restored. If the SD alternative is taken (directly after detecting the failure), then the plant temporarily will have higher CDF than the operating CDF during the initial transition period of power reduction and state changes. However, after this initial increase, the CDF slowly declines, resulting in a smaller and smaller CDF compared to the operating CDF. The estimate of CDP over time indicates that the risk of continued operation is smaller than that for shutdown until about 3 days (see, Figure 4).

2. Double-Failure Situation: When two SSW trains (e.g., trains A and B) are detected failed, the CDF profiles for both CO and SD alternatives are similar to those in a single failure, except that the CDF is increased by a factor of 160 over the baseline. Figure 4 shows that the CDPs for CO and SD alternatives again intersect at about 3 days.

3. Triple-Failure Situation: Where all the three SSW trains are detected failed, the conditional CDF dramatically increases by a factor of about 3600 over the baseline. However, in contrast to single-and double-failures, for several days CDF remains higher than for the CO alternative. The intersection of the CDPs occurs about 14 days after shutdown.

Figure 3 compares the SD risk profile for triple failures, with those for single and double failures. When all SSW trains are inoperable, the plant becomes vulnerable to loss of offsite power and loss of instrument air system initiating events, during shutdown as well as during power operation because of the resulting loss of the power conversion system and lack of major means to remove decay heat. In addition, these initiators have a higher frequency in shutdown states than in power operation state. As a consequence, the CDF remains high in the cold shutdown state, and the CDPs for the two alternatives cross at a long predicted repair time, i.e., 14 days (Figure 4).

Table 2 summarizes the results of this case study for failures in the SSW system of the BWR. These results include: 1) the CDF in the power operation state, 2) the increase in CDF for the continued-operation alternative, 3) the crossing point of the core-damage probabilities for the shutdown and continued power operation (SD/CO) alternatives, and 4) the expected core-damage probability for different failure situation in SD/CO alternatives along with the ratio between these probabilities. In particular, the ratio of the CDPs for SD/CO alternatives indicates that the SD alternative is unfavorable in all three failures of the SSW system.

3.3 LCO Recommendations for the Specific Example Analyzed

The risk-comparison analysis of failures in the SSW system of the particular plant resulted in the following recommendations:

1) The present AOT requirement for a single SSW-train failure is 3 days. This AOT may remain the same with the additional condition that, by the end of the first day, redundant trains are tested to assure that there are no additional failures. If the repair of the initial failure is completed within the first day, then no additional tests are required. If feasible, any diagnostic measure that can determine the condition of the redundant train(s), should

precede, or replace the need for, an actual demand test, particularly when the test may have adverse effects.[3]

2) The SSW trains are tested relatively frequently during power operations because they are run for mixing chemical additives and to test other safety-system components. The recommendation to test redundant SSW train(s) should not result in unnecessary additional testing. This recommended test can be omitted if a successful test was performed recently, e.g., in the previous 72 hours, and if there is no clear indication of a common-cause failure.

3) The current LCOs distinguish among different double failures; for example, a 3-day AOT is given for failure of SSW trains A and C, and B and C, but shutdown is required for failure of SSW trains A and B. Similarly, shutdown is required for failure of all three SSW trains. This study recommends 2 days of AOT for double- and triple-failures in the SSW system. With this change, the AOT for all double failures in the SSW system will be the same. This recommendation is justified because the impacts on core-damage frequency of different double-failure combinations are similar.

   In using this 2 days of AOT for double- and triple-failures in the SSW system, a decision needs to be made at the end of the first day whether one of the trains can be completely repaired by the end of the second day. If, by then, it is judged that this cannot be accomplished, then shutdown should be initiated immediately to avoid accumulating risk during power operation.

4) For multiple failures, if the repair time is expected to exceed 2 days, then shutdown should be initiated at the end of the first day, and cold shutdown should be reached within the next 12 hours. The time to reach cold shutdown differs from that currently allowed (12 hours to reach hot shutdown, and 24 hours to reach cold shutdown), because here, to minimize the risk impact, an orderly cold shutdown should be achieved without delay.

4. General Recommendations for Risk-Based Action Statements

The risk-comparison approach discussed thus far also was applied to the auxiliary feedwater system of a PWR.[4] Figure 5 graphically represents the general recommendations drawn from these studies to improve the action statements from a risk perspective:

1) The use of an AOT may be defined in the following manner. The initial portion of the AOT can be used to complete short repairs. For longer repairs, the needed repair time is assessed within the first phase of the AOT. If it is considered longer than the AOT, then shutdown can be initiated to minimize the accumulation of risk during power operation with such a failure. To identify the situation more clearly, especially where common-cause failures are suspected, additional tests of redundant train(s) may be conducted. Then, the applicable AOT should be followed, depending on the outcome of the test.

2) In the case of multiple failures, an AOT should be provided to allow at least one of the failed trains to be restored to operable status. As for a single failure, multiple failures also should have an AOT. This differs from some current TS requirements of immediate shutdown when multiple failures are detected. However, the AOT for multiple failures should be shorter than that for single failures.

3) Assessment of risk impact of staying in a particular mode (e.g., hot shutdown versus cold shutdown) can be used to decide on the applicable mode to be reached when a decision is made to shut down the plant. For example, in a BWR, the conditional CDF of staying in hot shutdown may be high compared to cold shutdown; if so, cold shutdown should be reached without delay.

4) If small risk is incurred, especially for continuing power operation, then the TS requirements can be relatively simple and flexible.

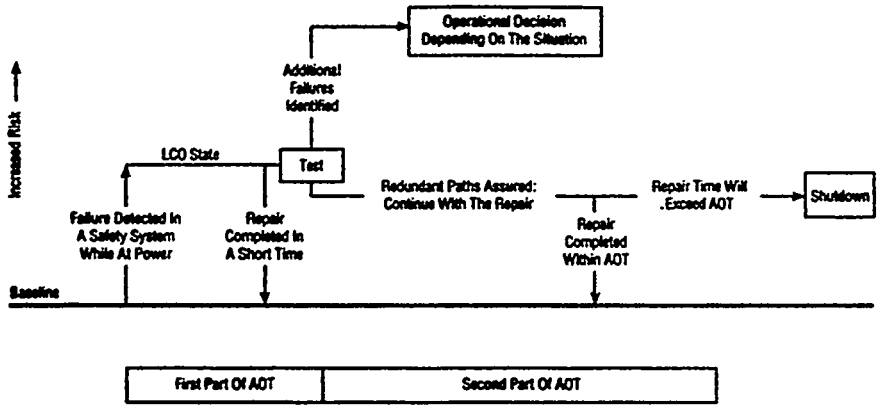


Figure 5 Recommendations for risk-based action requirements

There are several practical points that also should be taken into account in considering possible changes in the action requirements:

1) If an AOT is defined, it must be sufficiently long to complete a large percentage (e.g., ~90%) of repair needs; this will avoid any adverse effects of incomplete or hurried repairs.

2) The AOTs chosen should follow discrete values normally used in Technical Specifications such as 1 day, 2 days, 3 days, or 7 days, for ease of implementation.

3) Care should be taken that the relative risk-comparison of the operation alternatives is not the only factor in defining the action requirements. If mechanically followed, this approach could result in longer AOTs for multiple failures, thus possibly providing

incentives to declare multiple failures when repairs for single failures cannot be completed within the prescribed AOT.

4) When AOTs for multiple failures are defined in TS, it implies that, when one failure is repaired, the action for the remaining fewer failures needs to be followed. There is a significant risk advantage to promptly repairing one of the failures in the case of multiple failures. In principle, AOTs should reflect this risk perspective, where possible, by consistently defining longer AOTs for fewer failures.

5) The requirement for additional testing of a redundant train should consider its adverse effects. If feasible, any diagnostic measure that can determine the condition of the redundant train should precede or replace the need for an actual demand test. In the special case where testing the redundant trains involves substantial adverse effects,[3] then it may be more beneficial not to do so.

REFERENCES

1. P.K. Samanta, I.S. Kim, T. Mankamo and W.E. Vesely, *Handbook of Methods for Risk-Based Analyses of Technical Specifications*, NUREG/CR-6141, BNL-NUREG-52398 (in press).

2. T. Mankamo, I.S. Kim and P.K. Samanta, *Technical Specification Action Statements Requiring Shutdown: A Risk Perspective with Application to the RHR/SSW Systems of a BWR*, NUREG/CR-5995, BNL-NUREG-52364, November 1993.

3. I.S. Kim, S. Martorell, W.E. Vesely and P.K. Samanta, *Quantitative Evaluation of Surveillance Test Intervals Including Test-Caused Risks*, NUREG/CR-5775, BNL-NUREG-52296, February 1992.

4. T. Mankamo, I.S. Kim and P.K. Samanta, *Analyses of Action Requirements for Failures in the Auxiliary Feedwater System of a PWR*, BNL Technical Report L-2289, August 1994.

SAND94-2709C

Human Event Observations in the Individual Plant Examinations*

John Forester

Sandia National Laboratories

Abstract

A major objective of the Nuclear Regulatory Commission's (NRC) Individual Plant Examination (IPE) Insights Program is to identify the important determinants of core damage frequency (CDF) for the different reactor and containment types and plant designs as indicated in the IPEs. The human reliability analysis (HRA) is a critical component of the probabilistic risk assessments (PRAs) which were done for the IPEs. The determination and selection of human actions for incorporation into the event and fault tree models and the quantification of their failure probabilities can have an important impact on the resulting estimates of CDF and risk. Therefore, two important goals of the NRCs IPE Insights Program are (1) to determine the extent to which human actions and their corresponding failure probabilities influenced the results of the IPEs and (2) to identify which factors played significant roles in determining the differences and similarities in the results of the HRA analyses across the different plants. To obtain the relevant information, the NRC's IPE database, which contains information on plant design, CDF, and containment performance obtained from the IPEs, was used in conjunction with a systematic examination of the HRA analyses and results from the IPEs. Regarding the extent to which the results of the HRA analyses were significant contributors to the plants' CDFs, examinations of several different measures indicated that while individual human actions could have important influences on CDF for particular initiators, the HRA results did not appear to be the most significant driver of plant risk (CDF). Another finding was that while there were relatively wide variations in the calculated human error probabilities (HEPs) for similar events across plants, there was no evidence for any systematic variation as a function of the HRA methods used in the analyses. Moreover, much of the variability in HEP values can be explained by differences in plant characteristics and sequence-specific factors. Details of these results and other findings are discussed.

Introduction

The HRA is a critical component of the probabilistic risk assessments (PRAs) done for the individual plant examinations (IPEs). The determination and selection of human actions for incorporation into the event and fault tree models and the quantification of their failure probabilities can have an important impact on the resulting estimates of core damage frequency (CDF) and risk. The two main goals of this paper are to provide an overview of the different human reliability analyses (HRAs) that were conducted

*This work was supported by the U.S. Nuclear Regulatory Commission and performed at Sandia National Laboratories, which is operated for the U.S. Department of Energy under Contract Number DE-AC04-94AL85000.

for the IPEs and an assessment and comparison of the results from the various HRAs and the impact they had on the results of the IPEs. Much of the discussion below is based on a detailed review of the IPEs for 26 plants [11 boiling water reactors (BWRs) and 15 pressurized water reactors (PWRs)]. The sample included plants from the different vendors and from the various categories, such as BWR 2s, 3s, 4s, 5s, and 6s, and PWRs with different numbers of loops, etc. For some of the specific operator actions discussed, data from 17 BWRs and 32 PWRs were examined.

A variety of approaches and methods were used in conducting the HRAs for the IPEs. The quantification methods used included the traditional ones such as THERP,[1] ASEP,[2] SLIM,[3] HCR,[4] and OATS,[5] and more recent methods such as those proposed by Electric Power Research Institute (EPRI) (EPRI NP-6560-L[7] and EPRI TR-100259[8]) and that proposed by Dougherty and Fragola in their recent book.[8] In many cases, combinations of the various methods were used and in several instances, EPRI's SHARP[9] was used as the guiding framework for conducting the HRA. On the basis of the sample of IPEs reviewed, it appeared that any given method was just as likely to be used for analyzing a PWR as a BWR. In other words, there did not appear to be any bias in selecting particular methods for application to particular types of plants.

In general, the different HRA analyses separated the human action events into the traditional categories: pre-initiator and post-initiator (with the post-initiator events subcategorized as either "response actions" or "recovery actions"). In the context of the PRA, pre-initiator human actions are those which, if performed incorrectly or at inopportune times, can render instrumentation or systems unavailable when they are needed to respond to an accident. These actions typically include failures in calibrating instrumentation or failures in correctly restoring systems after maintenance. Post-initiator human actions are those required in response to initiating events or related system failures. Post-initiator response-type actions are generally distinguished from recovery-type actions in that the response actions are usually explicitly directed by emergency operating procedures (EOPs). Alternatively, recovery actions may entail going beyond written procedures, using systems in relatively unusual ways, or recovering failed or unavailable systems in time to prevent undesired consequences. The treatment of each of the three categories of human actions and the basic results are discussed, in turn, below.

Treatment of Pre-Initiator Human Actions

While all of the various HRAs performed for the IPEs addressed pre-initiator human actions in some way, their treatment varied somewhat across plants. For example, several plants simply dismissed the pre-initiator human action events by arguing that their failure probabilities are insignificant or that the human failure probabilities associated with such events are contained within the system unavailability data. Some plants explicitly considered events concerned with the failure to restore systems after maintenance, but dismissed miscalibration events (or at least failed to provide any evidence that they considered them). Other plants used a screening approach in which all the pre-initiator events were assigned relatively conservative failure probabilities and were only quantified explicitly if they proved to be important after initial quantification of the accident sequences. At least one plant calculated HEP values for several general classes of pre-initiator events and applied those values to the relevant actions throughout the fault trees. Of the 26 IPEs reviewed for pre-initiator events, only 13 plants (five BWRs and eight PWRs) performed detailed quantification of all or at least most of the identified pre-initiator

human actions prior to final quantification of the accident sequences. Seven other plants performed detailed quantification on only a few potentially important events (two to five events) that survived initial quantification. THERP[1] and ASEP[2] were the most frequently used methods for quantifying the failure probabilities of pre-initiator human actions.

Results of Pre-Initiator HRA

In general, the average failure probabilities for pre-initiator human actions tended to be slightly lower for PWRs than for BWRs. For the eight BWR plants which conducted detailed quantification on any pre-initiator events (screening values excluded), the mean of the average pre-initiator human error probability (HEP) value from each plant was 0.0075. For the 12 PWRs which conducted detailed quantification of pre-initiator events, the mean was 0.0028.

For the 13 plants that performed detailed quantification of all or at least most of the identified pre-initiator events (as opposed to quantifying only a few potentially significant events), eight of the 10 lowest mean HEP values were from PWRs, with the six lowest values coming from PWRs. The mean pre-initiator HEP values for these 13 plants are presented in Figure 1. Plant type (BWR or PWR) is

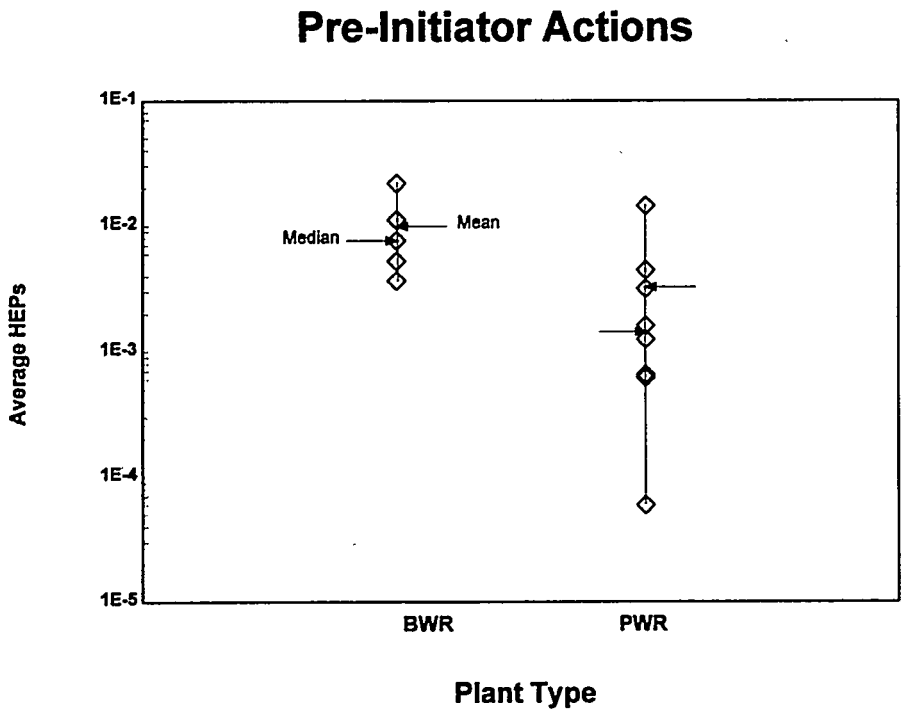


Figure 1. Average Pre-Initiator HEPs for Plants Performing Detailed Quantification of All (or at Least Most) of the Identified Pre-Initiator Events by Plant Type

indicated in the figure. Since the same basic pre-initiator HRA method was used in essentially all the IPEs (i.e., THERP[1]\ASEP[2]), an attempt was made to determine why several plants (which happened to be PWRs) had mean pre-initiator HEP values an order of magnitude lower than the others. The results of the investigation indicated that the plants which obtained the relatively smaller HEPs had performed rather detailed and extensive modeling of the pre-initiator human action events. The smaller HEP values might be attributable to a more thorough application of the pre-initiator HRA methods than was done for some of the other plants. At a minimum, there was no indication that the smaller pre-initiator HEP values were related to careless application of the methods.

While six of the 10 plants with the lowest overall CDF were plants that either used screening values for pre-initiator events or failed to analyze the pre-initiator events, there was little evidence that the treatment of pre-initiator events would correlate strongly with a plant's resulting CDF (see Figure 2). For PWRs in particular, there was no apparent relationship between mean pre-initiator HEP values and CDF.

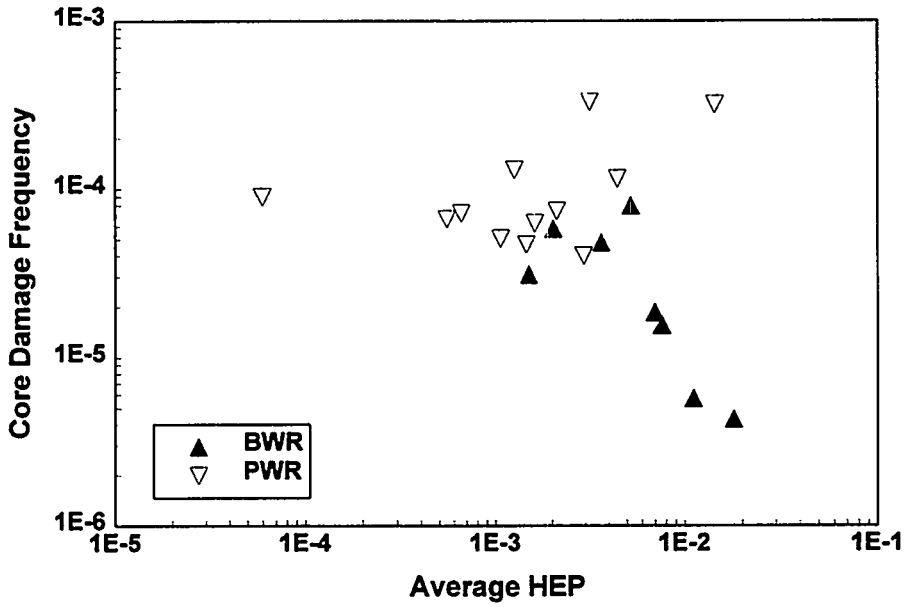


Figure 2. Average of Plant Pre-Initiator HEPs as a Function of Plant CDF

For the BWRs, there was some suggestion that larger mean pre-initiator HEPs were associated with smaller CDF estimates. This pattern of results suggests that the pre-initiator HRA results were not, in general, significant drivers of CDF. Obviously, such a result does not imply that all pre-initiator human error events are unimportant. Specific pre-initiator human error events could still be important contributors to particular accident sequences. However, a review of the IPEs which performed an analysis of pre-initiator events found only four pre-initiator human actions that had been found to be significant on the basis of importance to CDF. The four actions were (1) miscalibration of core spray injection permissive, (2) breaker maintenance error on the 4160-volt bus, (3) failure to realign the fire

water cross-tie valves after test or maintenance, and (4) operator failure to realign standby liquid control (SLC) valves following test or maintenance. All four actions were from BWRs.

Treatment of Post-Initiator, Response-Type Human Actions

The HRA of the post-initiator, response-type human action attempts to quantify the likelihood that operators will fail to conduct the various actions necessary to respond to an initiating event or accident scenario. As noted above, most of the necessary response-type actions would be indicated in the plant emergency operating procedures. The analysis of post-initiator response actions is a critical part of the HRA and there are number of factors related to the methodology and approach used to quantify the actions that could have a significant impact on the results of the analysis. Some of these factors, which were perceived as likely to be important, and their general treatment in the IPEs are discussed below.

In quantifying the HEPs for post-initiator response human actions, several of the plants used a single HRA methodology, while others used a combination of HRA methods to address different aspects of the analysis. In general, it appears that the different methods that were used to accomplish the HRA can be grouped into five basic categories or groups of methods. They include:

1. A modified version of SLIM[3] that relies on subjective estimates of the impact of various performance influencing factors (PIFs) on the operator's likelihood of failure. In addition to being the only method that consistently relies directly on subjective estimates by experts to derive the HEPs for the post-initiator human actions, this method is also distinguished by the fact that the impact of time on the performance of a task is determined on the basis of subjective estimates as opposed to the time reliability correlations (TRCs) used by most other HRA methods. This method was used in seven of the 26 IPEs reviewed.

2. A combination of the decision tree method described in EPRI-TR-100259,[7] along with ASEP[2] and THERP.[1] The decision tree method was used to quantify the diagnosis portion of the action. While the decision tree method may use subjective estimates to determine the degree to which time is relevant to performance on a particular task, the impact of time as a PIF was usually taken into account by using the TRC from ASEP[2] or THERP.[1] That is, when time was a limiting factor, a TRC was used to determine diagnosis failure probability. Values from THERP[1] were used to quantify the execution portion of the human actions. This method was used in six of the 26 IPEs reviewed.

3. The human cognitive reliability (HCR)[4] method or the operator reliability experiments (ORE)-based modification of the HCR method (EPRI NP-6560-L)[6], which are TRC methods that may also use THERP[1] to quantify the execution portion of the action (used in four of the IPEs reviewed).

4. The method described in the book by Dougherty and Fragola[8] that offers a number of different "tools" for doing HRA, but that also proposes the use of TRCs for determining HEPs. In one IPE that used this method, it was stated that the method is functionally a combination of SHARP[9] and HCR[4] and therefore may be similar to method three above (used in two of the IPEs reviewed).

5. The THERP[1] method or the ASEP method (which is a method derived from THERP[1]) or some combination of the two methods (used in seven of the IPEs).

In addition to the basic HRA methodology used to quantify the post-initiator HEPs, there are a number of other factors related to how the analysis was conducted that could have an impact on the results. Many of these factors may or may not have a direct impact on the derivation of HEPs, but may reflect on the nature and extensiveness of the analysis performed for the HRA or on how the HRA was incorporated into the PRA. Thus, their influence could be quantitative, qualitative, or both. Several of these factors and their treatment in the IPEs are discussed below.

One potentially important factor concerns the extent to which accident progression and context effects were taken into account in determining the HEPs. For example, an operator action indicated by the emergency operating procedures can be called for in the context of a variety of different initiators and after different patterns of previous operator and system failures or successes. Therefore, in order to be able to realistically quantify the human potential for failure or success, context effects and dependencies across a given accident sequence should be considered. While most of the IPEs clearly considered context and dependencies in analyzing post-initiator actions, some did not. Two plants analyzed operator actions only to the extent needed to determine the conditions that would yield the highest failure probability for a given human action event. The HEP for the action in that context only was then quantified and the resulting "conservative" value was assigned in all cases where the event occurred. Other IPEs addressed context only in cases where extreme differences in HEPs would be expected, and several either failed to consider context or dependency at all, or at least failed to provide any evidence that they had done so in their documentation.

Another issue concerns whether the human actions were separated into a diagnosis component and an execution component. Except under conditions where the time available for diagnosis is very short or there are no relevant emergency operating procedures, many of the existing HRA methods would produce HEPs for the execution segment that are significantly larger than for the diagnosis segment. However, the HCR model does not in general explicitly quantify the execution phase of the task and assumes that the HCR diagnosis curve is adequate for most situations. Two of the 26 IPEs that were reviewed took such a position.

Other factors having a potential impact on the results of the HRA include whether the analysts conducted simulator exercises to assess the performance of the control room crews in responding to important accident sequences and whether the analysts performed walk-throughs of important operator actions that must be performed outside the control room during emergency situations. Conducting simulator exercises and directly evaluating the demands placed on operators who are carrying out actions inside and outside the control room provide the HRA analysts with important information regarding PIFs that is likely to bear on the probability of successfully completing a given task. Obviously, another important factor is the extent to which important PIFs are considered and applied in determining the HEPs.

The review of the 26 IPEs indicated that essentially all of the HRA analyses attempted to apply the PIFs explicitly indicated by the methodologies being used. However, the level of analysis that accompanied the application of the PIFs appeared to vary across the different plants. For many of the IPEs, it was difficult to determine (on the basis of the documentation provided) exactly how much effort was actually dedicated to a careful analysis of the potential impact of PIFs on HEPs. Objectively, only nine out of the

26 IPEs appeared to conduct simulator exercises and apparently only seven out of the 26 performed walk-throughs of ex-control room actions. These findings are tempered by the fact that the applications of the SLIM-based methodology involved fairly extensive interviews of operators and plant personnel. Operators and relevant plant personnel participated in the SLIM-based analyses and provided their judgments regarding the extent to which various PIFs would affect the performance of important tasks. Thus, even though the SLIM-based HRAs (seven out of the 26) did not typically conduct simulator exercises or walk-throughs of ex-control room actions, they did obtain relevant information. It can certainly be argued that the judgments of the people performing the tasks, in the context of a systematic application of subjective estimate techniques, are as viable a source of information as direct observations by the analysts. Nevertheless, even if the seven IPEs that used the SLIM-based approach are added to the group that clearly did the observations, there remains 30% to 40% of the IPEs reviewed that either failed to obtain information important to valid HEPs or that failed to document that they had done so.

Results of HRA of Post-initiator Response-Type Actions

Summary of Quantification Results for Post-Initiator Response-Type Human Actions

In order to provide a general overview and summary of the results from the post-initiator HRA analyses, several different measures were examined. The measures included the overall average of the post-initiator response HEPs grouped by such factors as plant and plant type, the average of the HEPs for what might be considered the "typical" human actions necessary to respond to various accident scenarios, the average of the HEPs for human actions identified in the IPEs and in NRC reviews of the IPEs as dominant post-initiator human actions, and the specific HEPs for both "typical" and dominant human actions. The results from examining each of these measures are discussed in turn below.

Examination of General Measures of Post-Initiator HRA Results

The average of the post-initiator response-type HEPs for each of the 26 IPEs reviewed is presented by plant type (PWR vs. BWR) in Figure 3. As can be seen in the figure, the range of values across plants is an order of magnitude for both BWRs and PWRs. Similar to the pre-initiator HEPs, the post-initiator HEPs for PWRs tended to be lower than those for BWRs. A Satterthwaite T-test of the difference between means indicated that the mean of the values for PWRs (0.049) was significantly less than that for BWRs (0.101) [$T_{(14df)} = 2.55, p < 0.01$]. In order to determine (at a global level) the extent to which the overall post-initiator HRA analysis for each plant was a significant driver in determining the plant's CDF, a test of the correlation between the average post-initiator HEP for each plant and the CDF for each plant was conducted. While the test failed to indicate a statistically significant relationship ($r = -0.306, p < .10$), the trend was toward an inverse relationship (e.g., the higher the average HEP value, the lower the CDF). This finding indicates that when a general measure of the overall post-initiator HRA analysis is used (the average of the post-initiator response HEPs for each plant), it appears that the HRA analysis of post-initiator response actions is not the most significant driver in determining CDF. It should be noted, however, that these results are based on averages and therefore do not imply that specific human actions are unimportant contributors to CDF or that the results of the IPEs are unaffected by the way in which the HRA methods are applied to the quantification of specific human actions. Clearly, the way in which specific human actions were quantified could have had a significant impact on CDF for particular initiators and sequences, and such effects could be "washed out" by examining only averages.

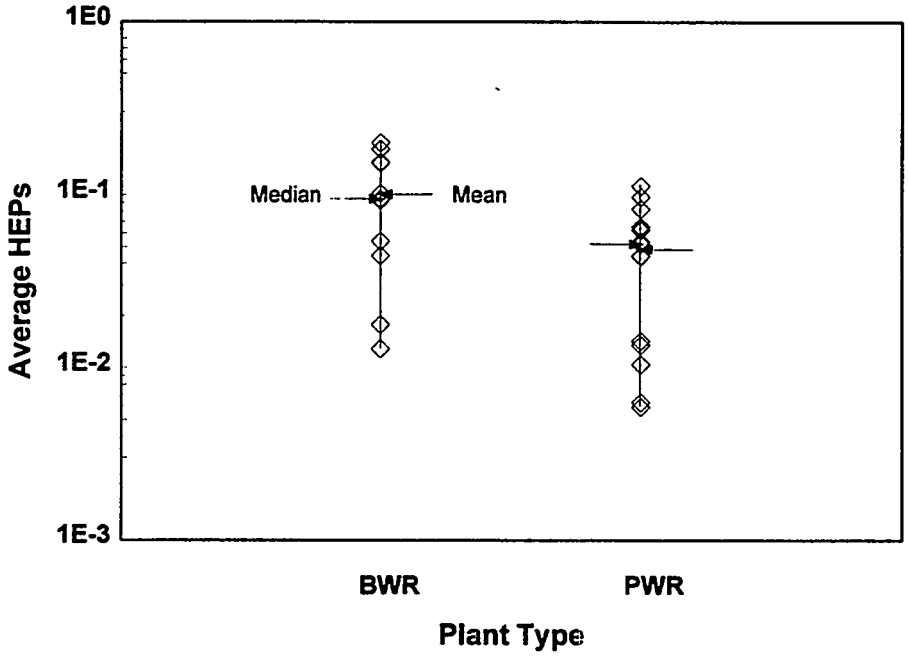


Figure 3. Average Post-Initiator Response Type HEPs by Plant Type

In regard to the impact the different HRA methods may have had on the quantification of the post-initiator HEPs, an examination of the average post-initiator HEPs by the HRA method failed in general to reveal any apparent trends. The only detectable pattern was that the averages of the HEPs from the IPEs using the SLIM-based HRA method tended to be numerically close to one another (e.g., four of the values ranged from 0.045 to 0.062), and to lie toward the middle of the distribution of HEPs.

Another measure used to provide an overview of the results of the HRA analyses was the average of the HEPs on the dominant human actions identified in each IPE. Determination of the dominant human actions was based on the "importance measures" presented in the IPEs and, when available, from comments contained in the reviews of the IPEs conducted by the NRC's contractors. Before discussing the results, it should noted that for some IPEs it was difficult to determine the dominant human actions and for others there were multiple cases of an action that had been identified as being dominant, but little guidance regarding which of the multiple cases was the one which ranked high in the importance measure results. In these cases, all of the values for that event were included as dominant actions and this resulted in some plants having many values contributing to the mean of the dominant human actions, while others had only a few.

The average of the HEPs from the dominant human actions is presented by plant type in Figure 4. As with the overall averages of the post-initiator HEPs, a large range of values was found across plants, with the lowest and highest values differing by two orders of magnitude for both BWRs and PWRs. While six of the nine lowest average values were from PWRs, the means for the dominant human actions for PWRs and BWRs were not significantly different (0.072 and 0.075 respectively). A test of the correlation between the average HEPs for the dominant human actions from each plant and the CDF for each plant

failed to even approach significance (r = - 0.039, NS). An examination of the average dominant human action HEPs by the HRA method indicated that there was no detectable systematic variation in the values as a function of method.

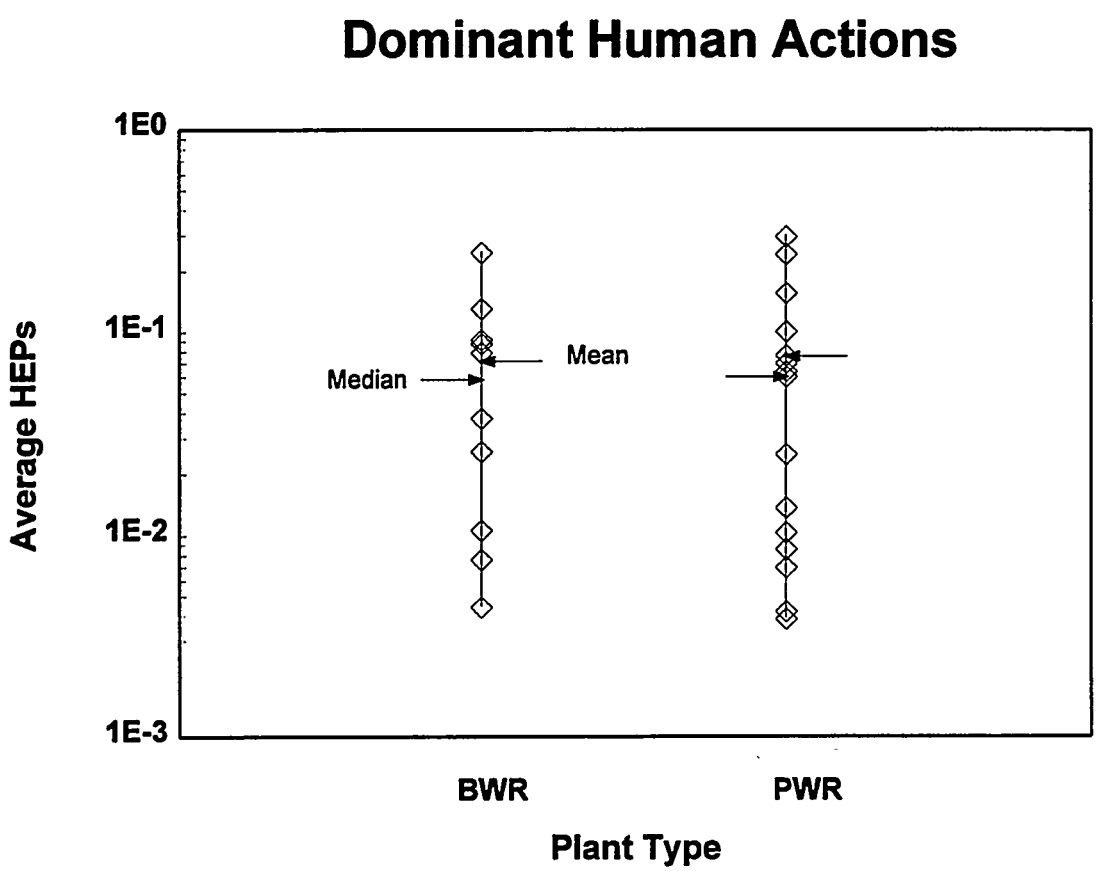


Figure 4. Average HEPs for Dominant Human Actions by Plant Type

The final "general" measure of the results of the HRA analyses was the average HEP from the human actions classified as "typical" human actions. Examples of typical human actions from BWRs included events such as initiation of standby liquid control (SLC), manual scram, level control with high and low pressure systems, inhibition of automatic depressurization system (ADS), manual depressurization, containment venting, and use of the fire water system. Examples from PWRs include events such as boron injection, feed and bleed, switchover from injection to recirculation, containment cooling, initiation of safety injection, providing makeup for alternate or auxiliary feedwater, control of feedwater, use of standby feedwater, steam generator depressurization, and prevention of steam generator overfill.

The results from the examination of the average HEPs for the typical human actions from each plant were only somewhat similar to the general pattern of results found with the two measures discussed

above. While the difference between the mean value for BWRs (0.047) and PWRs (0.034) was not large, the six lowest average values came from PWR IPEs. Furthermore, the range of values was greater for PWRs, with greater than an order of magnitude between the lowest and highest values. The difference between the lowest and highest values for BWRs was only 0.064, indicating that when the HEP values from all typical human actions are taken together, the analyses of BWRs produced similar estimates of the likelihood of human error. The average HEPs for the typical human actions are presented by plant type in Figure 5.

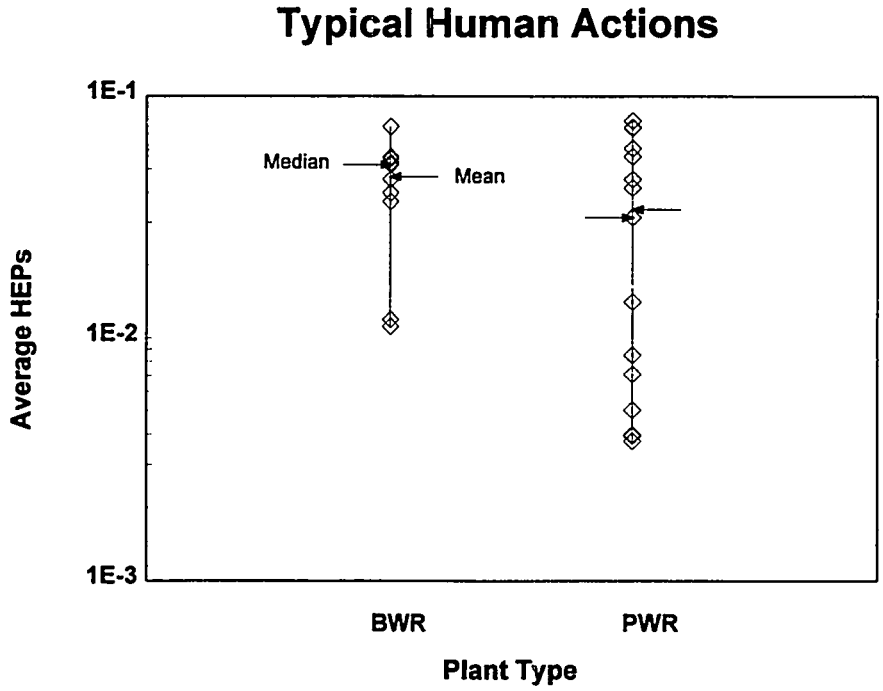


Figure 5. Average HEPs for Typical Human Actions by Plant Type

Examination of Specific Post-Initiator Response-Type Human Actions

Turning to the HEPs for specific human actions, several of the dominant and/or typical human actions from PWRs and BWRs were selected and their HEPs compared across plants. Before discussing the results from this analysis, it should be noted that many of the plants may have had multiple values for a given human action because they considered context and dependency effects, while other plants may have had only a single value or, for various reasons, no value at all. For example, PWRs with automatic switchover from injection with the emergency core cooling system (ECCS) to recirculation did not always model a human action to recover a failed automatic initiation.

The first action examined was the operator action to switch from injection with ECCS to recirculation in PWRs. This action was selected because importance measures indicated that it was a dominant contributor for many PWRs. Figure 6 displays, by PWR vendor [Babcock & Wilcox (B&W),

Combustion Engineering (CE), and Westinghouse (W)], the HEPs for the switchover to recirculation for each of the 32 PWR IPEs reviewed. Values from a given plant are indicted by a number that was arbitrarily assigned to each plant. As can be seen in the figure, a large difference exists in the HEPs for

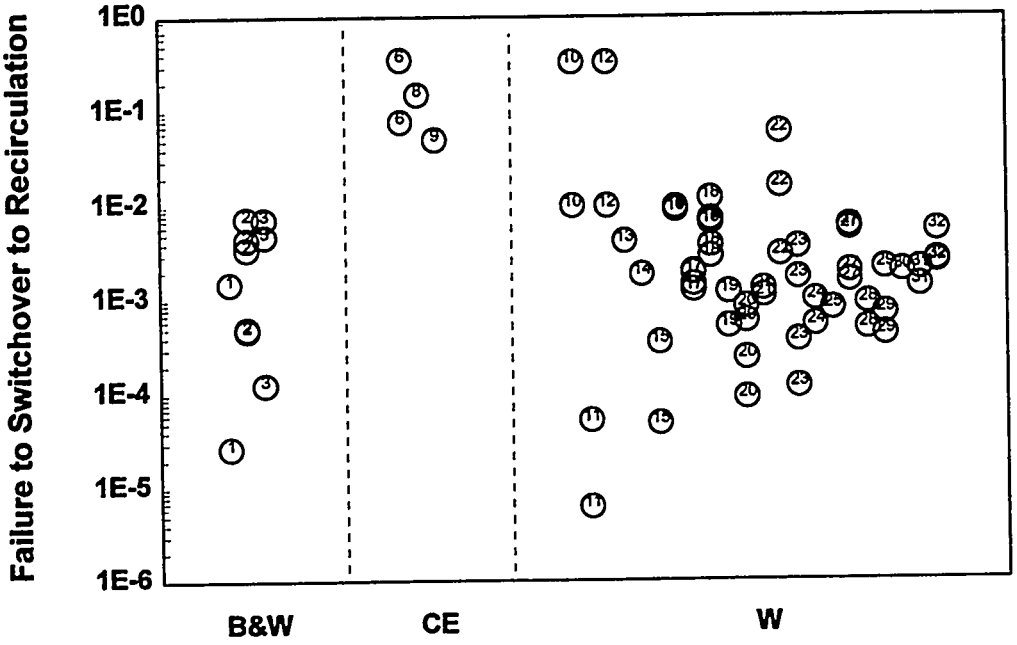


Figure 6. HEPs for Switchover to Recirculation by PWR Vendor
(Data points are numbers which were arbitrarily assigned to identify plants.)

accomplishing this action. The difference between the lowest and the highest value is several orders of magnitude. One reason for the variability in HEPs within a given plant is that success of the switchover was in general (but not always) estimated to be more likely at high pressure [e.g., small loss of coolant accidents (LOCAs)] than at low pressure (e.g., large LOCAs). One advantage for the high-pressure case was that in many instances more time was assumed to be available for the operators to diagnose and accomplish the desired actions. The relationship between failure rates and time available is displayed in Figure 7. Although the effect is not dramatic, HEPs tend to decrease when more time is available. Pressure level also accounts for much of the variance in HEPs within similar types of plants.

Another reason for the large differences in the HEPs across plants is that in some cases the switchover is automatic, while in others it is either a semiautomatic or completely manual operation. For plants with an automatic switchover, the operator action would be a recovery of a failed automatic actuation, while for the other plants the operators would be conducting a normal activity for the accident scenario. Thus, a difference in the HEPs for these situations would not be surprising. Of the 32 PWRs reviewed, apparently 15 required manual alignment and initiation of the switchover, with five plants having semiautomatic initiation and 12 being completely automatic. An average of each plant's average HEP for

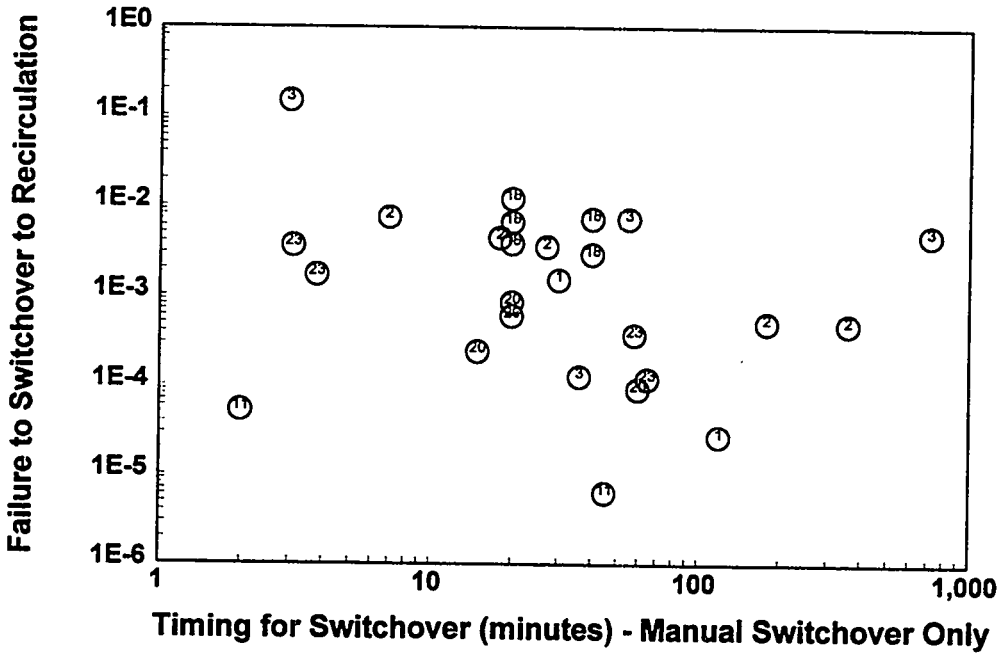


Figure 7. HEPs for Switchover to Recirculation as a Function of Time Available for the Switchover
(Data points are numbers which were arbitrarily assigned to identify plants.)

the switchover action indicated that the average HEP for plants requiring manual alignment tended to be lower than for the semiautomatic and automatic plants -- 5.5E-3, 7.7E-2, and 4.2E-2, respectively. In fact, the plants with the highest HEP values (plants numbered 6,8,9,10, and 12 in Figure 6) all had automatic or semiautomatic initiation of the switchover. The HEPs for the switchover are displayed in Figure 8 as a function of whether the action was performed manually, automatically, or semiautomatically. Semiautomatic switchover implies that either part of the task is done automatically or that under certain conditions the switchover occurs automatically (e.g., automatic under low pressure conditions, but not under high). In addition to the average failure probabilities being different, the variability of the values appeared to be much greater for the plants with automatic initiation (ranging from 0.17 to 8.0E-4), with several of them apparently failing to model human recovery of a failed auto-initiation. The values for the manual plants, however, were reasonably consistent; most of them were within an order of magnitude of each other when the high vs. low pressure factor was taken into account. The reasons for the large variability in the HEPs for the automatic (and semiautomatic) plants were not immediately apparent, but could be related to differences in indicators, procedures, and training for accomplishing a normally automatic task under accident conditions. In general, the more detailed and thorough analyses tended to produce somewhat lower failure probabilities. However, the HRAs for three of the plants with the very lowest HEPs (plants numbered 11, 15, and 20) were apparently conducted by the same analysis team and, since there was nothing obvious that made these plants unique, it appears that they may have tended toward optimism.

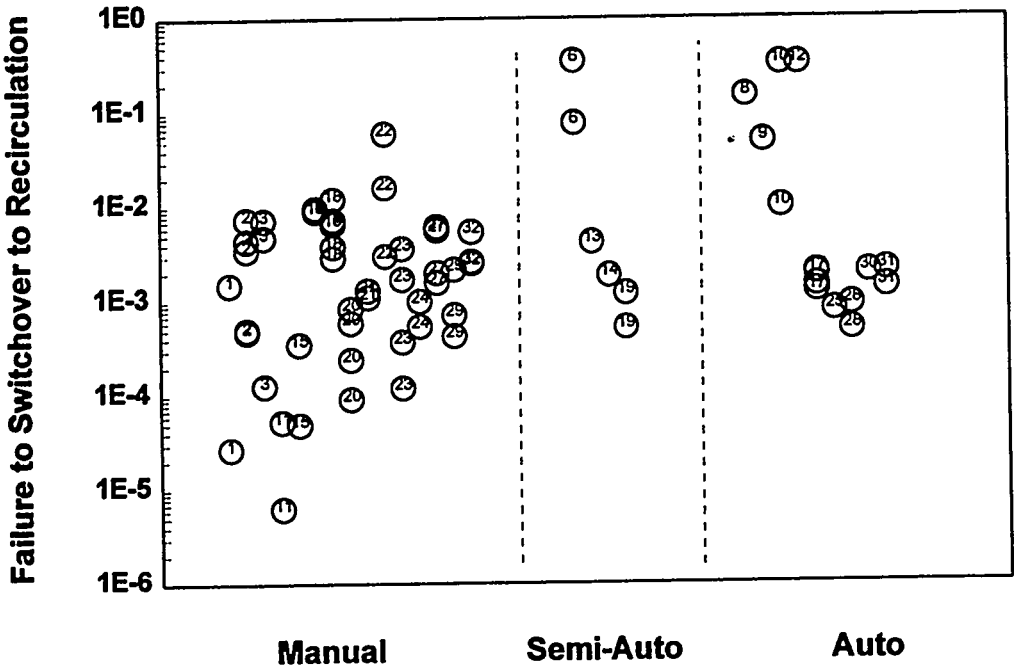


Figure 8. HEPs for Switchover to Recirculation as a Function of Whether the Action is Performed Automatically, Semiautomatically, or Manually
(Data points are numbers which were arbitrarily assigned to identify plants.)

Another specific action examined was the operator action to initiate SLC or add boron during an anticipated transient without scram (ATWS) in BWRs. As can be seen in Figure 9, a large range of values is found for the initiation of an SLC during an ATWS. For the 17 BWRs reviewed, the lowest and highest values differ by more than three orders of magnitude. At least some of the variation in the HEPs can be attributed to the fact that one of the plants has an automatic initiation of SLC and the operator action is a recovery of this failure by manual initiation. The recovery HEP is relatively higher than most of the other values derived for the initiation of SLC. An important contributor to the differences is that some analyses gave credit for initiation of SLC both early and late. In all cases, early initiation of SLC was determined to have a lower failure probability than late initiation, usually with at least an order of magnitude difference. The assumption appeared to be that if the operators failed early, they would also tend to fail late.

Another factor having an impact on the HEP values was whether the condenser was assumed to be available. With the condenser available, more time was allowed for initiation of SLC and therefore lower failure probabilities were obtained. Nevertheless, even when such factors are taken into account, there would still be more than an order of magnitude difference between the lowest and highest values.

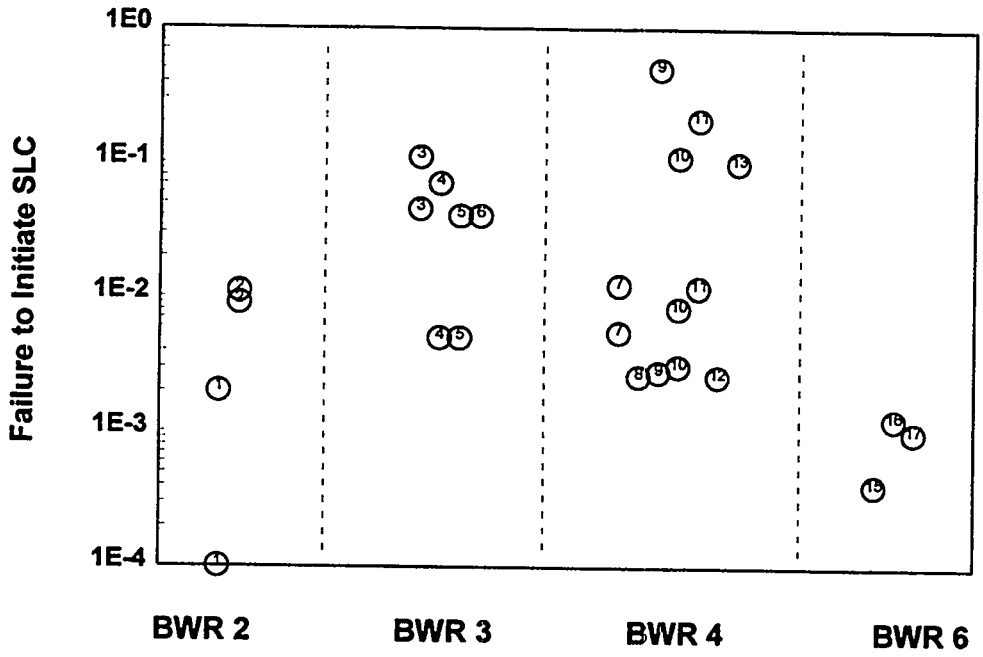


Figure 9. HEPs for Initiation of SLC by BWR Type
(Data points are numbers which were arbitrarily assigned to identify plants.)

Figure 9 displays the HEPs for the initiation of SLC as function of the different types of BWRs. When the differences are examined in this way, it appears that the variation is to some extent related to plant type. In particular, with the exception of the values for one of the BWR 2s, the HEPs for BWR 6s are lower than for all the other plant types. Some of the more extreme high failure probabilities obtained for the BWR 3s and BWR 4s are related to the relatively high failure probabilities derived for initiating SLC late or for initiation of SLC when the condenser is unavailable. For example, the high HEPs values for plants numbered 9 and 11 are values for initiating SLC late and the highest values for plants 3, 4, 5, and 10 are for conditions when the condenser is unavailable. The high value for plant 13 is the recovery value for failure of the automatic initiation of SLC. In any case, even when these extreme values are ignored, there still seems to be a trend for the HEPs to decrease linearly across BWR 3s, 4s, and 6s. (The only BWR 5 reviewed had automatic initiation of SLC and did not quantify a recovery value.) The reason for the downward trend is not obvious, but could be related to a greater willingness on the part of the newer plants to use SLC. In recent years, operators' fears regarding professional repercussions from premature use of SLC seem to have lessened, but in the older plants there may be vestiges of the hesitancy to use SLC. Such a bias may not yet have been completely excised from existing training programs and updated procedures, and was therefore detectable by HRA analysts.

Another specific human action important to the ATWS scenarios in BWRs is the action designated in many of the plant emergency procedures to inhibit ADS. Inhibition of ADS is indicated by the emergency procedures to help avoid activation of low-pressure injection during an ATWS, which could

increase reactivity. One reason this action is interesting is that apparently some IPEs assume that they will go to core damage during an ATWS if ADS is not inhibited. Others assume this is not the case -- that an ATWS can still be mitigated, and that inhibition of ADS can lead to problems in other scenarios if the operators fail to depressurize. As can be seen in Figure 10, there are some fairly wide variations in

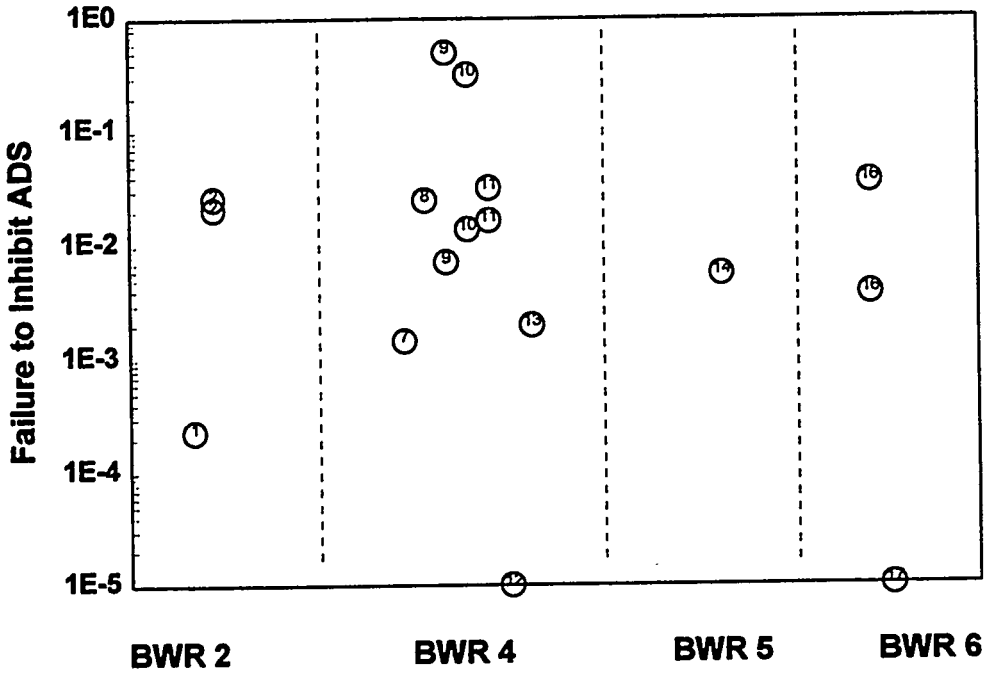


Figure 10. HEPs for Inhibition of ADS by BWR Type
(Data points are numbers which were arbitrarily assigned to identify plants.)

the HEPs for failing to inhibit ADS. However, much of the difference seems to be caused by outliers on both ends of the distribution. The two extreme values (plants 9 and 10) on the high failure probability end of the distribution are related to ATWS events in which no high-pressure makeup is available. The two extremely low values (plants 12 and 17) were both derived by the same analyst, who apparently determined that the training, procedures, and other relevant PIFs at the plants guaranteed a low probability of failure.

The last specific operator action examined was the PWR event for initiating feed and bleed (15 plants sampled). The difference between the lowest and highest HEPs (see Figure 11) is greater than two orders of magnitude, but with the one plant with multiple outlier values excluded, the HEPs tend to be less than an order of magnitude apart. This moderate lack of variability suggests that the feed and bleed operation may be perceived and executed in similar ways across the plants that have the feed and bleed capability.

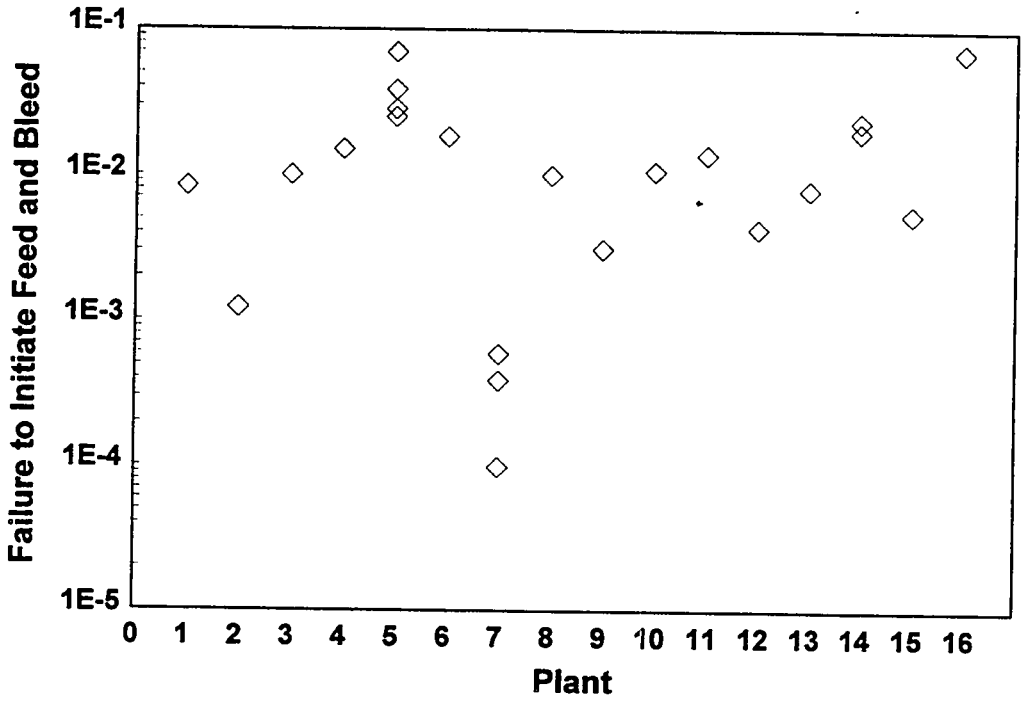


Figure 11. HEPs for Initiation of Feed and Bleed by Plant Number

Influence of HRA Characteristics on Quantitative Results

As discussed above, there are several factors related to how the HRA analyses were conducted that could have affected the results. These factors may affect the quantitative results of the analysis or they may affect only the qualitative results. That is, such factors may lead to variations in the resulting HEPs, or they may just affect the quality and usefulness of the results in terms of what is learned from performing the analysis. To determine whether any of the various factors influenced the quantitative results, the relationships between the post-initiator response-type HEPs (all, dominant, and typical) and whether the HRA analyses considered context effects, conducted simulator exercises, or conducted walk-throughs of ex-control room actions, were examined. The examination failed to detect any apparent relationships between these factors and the averages of the HEP values used in the analysis. Apparently such factors did not influence the more general, and therefore possibly less sensitive, estimates of HEP results.

To further explore the impact of such factors as consideration of context effects, use of simulator exercises, and use of walk-throughs of ex-control room actions on HRA quantification, the relationships between these factors and the HEPs for some of the specific operator actions were examined. Using the data from nine BWR plants for which the relevant information had been obtained, the relationship between the average HEP values for the initiation of SLC and the HRA-related factors was examined. The results of this examination failed to reveal any apparent relationships. However, when the average of

the values for the switchover to recirculation in PWRs was examined (14 plants), some indication of a pattern was detected. Of the 14 plants examined, the plants with the six lowest average HEP values for initiating the switchover were plants that did not perform simulator exercises or do walk-throughs of ex-control room actions. In fact, eight of the 10 lowest values came from plants that did not perform simulator exercises or do walk-throughs. This finding may indicate that simulator exercises and walk-throughs tend to make analysts somewhat less optimistic in their derivation of HEPs.

Treatment of Post-Initiator Recovery-type Actions

A review of 49 IPEs indicated that while most of the IPE reports discussed the need for the identification of potential recovery actions and the application of recovery action HEPs to the cut sets, only 31 (63%) of the IPEs explicitly identified the recovery actions and their HEPs. Of the 31 submittals that did explicitly identify recovery actions and document the quantification results, they all applied essentially the same HRA method that was used in their analysis of the post-initiator human actions. Many of the plants identified only a few recovery actions, while others included many recovery actions in their analyses. One reason for the differences in the number of recovery actions modeled by the different plants was that some of the analyses included multiple occurrences of the same action, with the HEPs for a given action differing as a function of context (e.g., time available to complete the action in different scenarios, etc.). Another reason for differences in the numbers of recovery actions was that some plants appeared to have used screening values for recovery-type actions and only explicitly quantified those that survived screening.

Of the 49 submittals examined, only 21 (43%) included recovery of failed or unavailable systems (exclusive of recovery of off-site power) as part of their recovery analysis. On the basis of a sample of 26 of the 49 submittals, the number of actions involving recovery of failed systems constituted approximately 20% of all recovery actions.

Results of Post-Initiator Recovery HRA

A sample of 26 IPEs was reviewed to obtain estimates of the HEPs obtained for the recovery actions. Of these 26, six BWRs and nine PWRs had explicitly identified and quantified post-initiator recovery-type actions. The average recovery action HEPs for these 15 plants are presented in Figure 12. As might be expected, in general the average HEPs tended to be higher for the recovery-type actions than for the other classes of human actions. However, there were some fairly substantial differences in the mean HEP values across plants. The recovery HEPs for BWRs tended to be somewhat higher than those for PWRs, with the means equal to 0.163 and 0.115, respectively. For actions involving recovery of failed systems, the mean HEP values were 0.332 and 0.11 for BWRs and PWRs respectively.

Summary and Conclusions

Both general and specific measures of the results of the HRAs performed for the IPEs were examined to obtain insights regarding the relationship of the HRA to the results of the IPEs. On the basis of the examination of the general measures, several conclusions are possible. First, there is no evidence of any systematic variation in the HEPs derived for the IPEs that can be attributed to the general HRA method

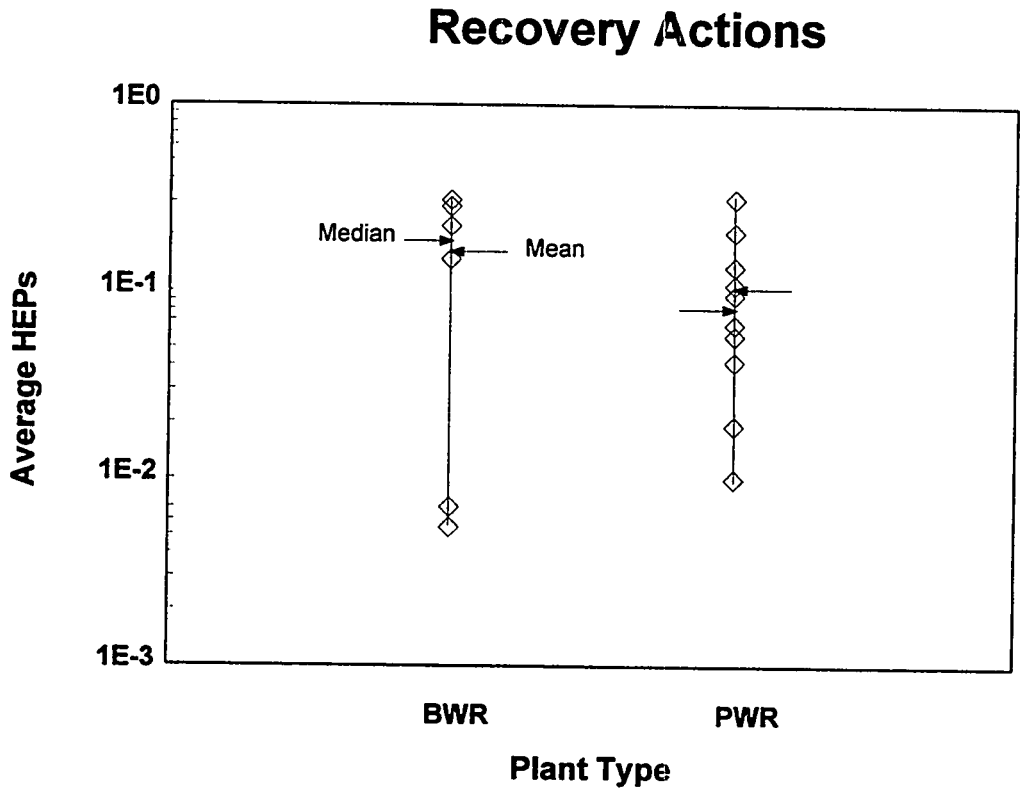


Figure 12. Average HEPs for Post-Initiator Recovery-type Actions

used for quantification. In other words, the methods per se did not appear to account for the variation in HEPs obtained across the different plants.

Second, the evidence does seem to suggest that, in general, the HEPs for PWRs tend to be less than for BWRs. One reason for this trend appeared to be that several PWRs had consistently low failure probabilities relative to other plants. Whether the lower overall (and in some cases specific) HEPs for several particular PWR plants were due to aspects unique to those plants or whether they were due to optimism on the part of the analysts, is difficult to determine. It could very well be that the lower values are due to aspects such as superior training and procedures in certain plants or to somewhat simpler problems, in general, for PWRs. The latter alternative seems less likely since the general measures of HEP results from many PWRs were comparable to those from BWRs.

Next, when the average HEP values from the various submittals were used as predictors of plant CDF, there was little indication that overall HRA results were the main drivers of CDF. While the use of averages obscures the impact of the quantification of specific events on specific CDF sequences, the averages should reflect quantification trends across similar events (i.e., since similar plants tend to include similar human actions in their models, averages should provide at least some indication of the kinds of HEP values being derived for those actions). Thus, the absence of a strong correlation between

these measures and overall CDF at least suggests that other, non-HRA related factors were also important to overall CDF.

Finally, on the basis of most of the measures examined, there did seem to be fairly wide variations in the HEP values obtained for different plants. However, as will be noticed in the discussions of HRA results for specific events, much of the variability appears to be related to plant-specific characteristics and modeling details, as opposed to erratic application of HRA methods.

Turning to the results of the examinations of specific events (e.g., switchover to recirculation in PWRs), perhaps the most striking aspect of the results of examining the HEPs was that there was a relatively high degree of consistency in the derived HEPs. When the various plant characteristics and sequence-specific factors considered by the analysts in determining the HEPs were taken into account, much of the variability in the HEPs could be explained. While this finding is encouraging, there were usually several outlier values found for each event that could not be straightforwardly explained and there did appear to be at least some degree of random variation. Given the current state of the art of HRA methods, it is not surprising that some of the variation in HEPs appears to be random.

A final aspect of the analysis to note is that some of the more general characteristics of how the HRAs were performed (e.g., were simulator exercises conducted, etc.), did not appear to have a consistent impact on the quantitative results of the HRA. As discussed in earlier sections in this paper, there are many aspects of how HRAs are conducted that could have important influences on both the quantitative and qualitative results (e.g., usability of the results after the analysis is completed). On the basis of the measures examined in the present analysis, however, there was only limited evidence that such factors had a significant impact on the quantitative results. Given the degree of what appears to be random variability in the HEPs obtained, it is not surprising that many of the measures used in the present analysis would be insensitive to the impact of such factors. Nevertheless, the lack of detectability should not undermine the importance of thorough application of the existing HRA approaches, particularly in regard to the usefulness of the results for guiding plant improvements.

References

1. A.D. Swain and H.E. Guttman, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Applications : Technique for Human Error Rate Prediction,* NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington D.C., 1983.

2. A.D. Swain, *Accident Sequence Evaluation Program Human Reliability Analysis Procedure,* NUREG/CR-4772, U.S. Nuclear Regulatory Commission, Washington, D.C., February 1987.

3. D.E. Embrey, et al. *Slim-Maud: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment,* Vols. 1-2, NUREG/CR-3518, U.S. Nuclear Regulatory Commission, Washington, D.C., March 1984.

4. G.W. Hannaman, A.J. Spurgin, and Y. Lukic, A Model for Assessing Human Cognitive Reliability in PRA Studies, in *1985 IEEE Third Conference on Human Factors and Power Plants, Monterey, CA, June 23-27, 1985,* NY: Institute of Electronic and Electrical Engineers, 1985.

5. R.E. Hall, J. R. Fragola, and J. Wreathall, *Post-Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation,* NUREG/CR-3010, Upton, NY: Brookhaven National Laboratory, November, 1982.

6. A.J. Spurgin, P. Moieni, and G. W. Parry, *A Human Reliability Analysis Approach Using Measurements for Individual Plant Examinations,* EPRI NP-6560-L, Palo Alto, CA: Electric Power Research Institute,1989.

7. G.W. Parry, *An Approach to the Analysis of Operator Actions in PRA,* DRAFT, EPRI TR-100259, Palo Alto, CA: Electric Power Research Institute.

8. E.M. Dougherty and J.R. Fragola, *Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications*, John Wiley and Sons, 1988.

9. G.W. Hannaman and A.J. Spurgin, *Systematic Human Action Reliability Procedure (SHARP)*, EPRI-3583, Palo Alto, CA: Electric Power Research Institute, 1984.

Development Status of an Improved Method for Conducting an Integrated HRA/PRA Based on Operating Experience

M.T. Barriere,* W.J. Luckas,* S.E. Cooper,** J. Wreathall,+ D.C. Bley,++
A. Ramey-Smith,+++ C.M. Thompson+++

*Brookhaven National Laboratory, Upton, NY
**Science Applications International Corp., Reston, VA
+John Wreathall & Co., Dublin, OH
++PLG, Inc., Newport Beach, CA
+++Nuclear Regulatory Commission, Rockville, MD

Abstract

Since the early 1970s, Human Reliability Analysis (HRA) has been considered an integral part of Probabilistic Risk Assessments (PRAs). However, current limitations of existing HRA approaches become apparent when the role of the human is explicitly examined in the context of real nuclear power plant (NPP) events. Recent serious events indicate that human performance is a dominant source of plant risk. Development of new or improved HRA methodologies to more realistically represent human performance is recognized by the Nuclear Regulatory Commission (NRC) as a necessary means to increase the robustness of PRAs. In order to accomplish this objective, a Detailed HRA Project, under sponsorship of the NRC's Office of Nuclear Regulatory Research (RES), was initiated in late February of 1992 by Brookhaven National Laboratory (BNL). The purpose of the BNL Detailed HRA project is to develop an improved method for HRA that enables a more realistic assessment of the human contribution to plant risk and can be fully integrated with PRA. This paper describes the research and development efforts of the project including: the development of a multidisciplinary HRA framework, the characterization and representation of errors of commission, and an approach for addressing human dependencies. Research implications and necessary development requirements are also discussed.

1.0 INTRODUCTION

This paper describes progress made in the Improved HRA project (FIN L-2415) beyond that presented in late October 1993 at the 21th Annual Water Reactor Safety Information Meeting (WRSM). Note that initial project progress was presented at the 20th WRSM in October 1992.

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 and systematic approach to human reliability analysis (HRA) is currently being developed. It is intended to be fully integrated with probabilistic risk assessment (PRA) methodology and enable a better assessment of the human contribution to plant risk, during all modes of plant operation. Development of new or improved HRA methodologies to better represent human performance was recognized by the NRC as necessary to increase the robustness of PRAs for all modes of plant operation.

The BNL Improved HRA project's completed, ongoing and future efforts are divided into four phases: (1) the completed FY92/93 Assessment Phase, (2) the recently completed FY93/94 Analysis and Characterization Phase, (3) the current FY94/95/96 Development Phase, and (4) the planned FY96 Implementation Phase. The following section provides an overview of these phases.

2.0 PROJECT OVERVIEW

During the FY92/93 Assessment Phase, a Human Action Classification Scheme (HACS) was developed for categorizing human actions and associated influences in actual LP&S events. Review of events reported in Licensee Event Reports (LERs), NRC Regional Augmented Inspection Team (AIT) and Headquarters' Incident Investigation (IIT) Team reports, and NRC/AEOD Human Performance reports identified the risk significance of EOCs, human dependencies, and multiple performance shaping factors (PSFs).

Recognizing that current at-power and LP&S PRAs did not thoroughly account for EOCs, human dependencies and multiple PSFs, a program plan outline to address these observations and improve HRA and its integration with PRA was initiated. The program plan outline also addressed the development requirement for a new, improved multidisciplinary HRA framework needed to describe the relationships among human factors, behavioral science and plant engineering and operations within an HRA and PRA context. The framework would shape further analysis of operational data, guide HRA modeling, and provide the basis for integrating the HRA quantitatively into the PRA. The accomplishments of the entire FY92/93 Assessment Phase (including the details of the BNL and SNL parallel efforts and the program plan) have been documented in NUREG/CR-6093, "An Analysis of Operational Experience During LP&S and A Plan for Addressing Human Reliability Assessment Issues."

The FY93/94 Analysis and Characterization Phase consisted of: (1) the development of a multidisciplinary HRA framework for improving the integration of HRA with PRA and (2) the characterization of EOCs and human dependencies including general guidance for their identification and representation in PRAs. The framework development and the EOC and dependency characterizations will be discussed further in Sections 3.0, 4.0, and 5.0. The results of Analysis and Characterization Phase research efforts, including research implications and a program plan to guide the performance of the current Development Phase will be documented in an FY95 BNL NUREG/CR. This report, identified as NUREG/CR-6265, will be entitled "Multidisciplinary Framework for Analyzing Errors of Commission and Dependencies in Human Reliability Analysis" and is anticipated to be made ready for NRC publication in early 1995.

In the current FY94/95/96 Development Phase the accomplishments of the prior phases are being integrated into the development of a working HRA quantification process that includes: how to identify and incorporate human failure events in the logic models used in PRAs; what information is required to quantify the probabilities of these failure events; how this information is used to estimate the probabilities; and how the probabilities are incorporated into the PRA quantification process. A detailed program plan for performing these development requirements has been defined and is discuss in NUREG/CR-6265 and summarized in Section 6.0 of this report.

It is anticipated that the FY96 Implementation Phase of the project will demonstrate the usefulness and acceptability of the developed methodology's implementation guidelines using a suitable PRA.

3.0 MULTIDISCIPLINARY HRA FRAMEWORK DEVELOPMENT

3.1 Introduction

Recently, there has been a growing recognition that existing HRA methods do not represent realistically the roles of humans in both the creation and the prevention (or mitigation) of accidents at nuclear power plants (NPPs). The nature of these criticisms is the simplistic and narrow consideration of the factors that influence the performance of operators and other plant personnel; the limited consideration of the interactions between people and the plant (particularly the errors of commission [EOCs]); and the frequent assumption of independence between multiple human errors. As a result of these deficiencies HRA, and as a consequence PRA, lack key features of human involvement in serious accidents and near misses. Reviews of the severe accidents at Chernobyl, Three Mile Island (TMI-2), and others, indicate that human reliability plays a much more significant role than that reflected by such errors as omitting a procedural step or selecting an incorrect switch. However, these are the typical human failure modes represented in, for example, NRC-mandated Individual Plant Examination (IPE) studies.

In order to address these deficiencies, it is necessary to formalize the description of the relationships between human errors, and the influences of performance shaping factors (PSFs) and plant conditions on those errors. Therefore, a critical task of this project has been to develop a multidisciplinary HRA framework that defines and integrates these relationships. This provides a basis for subsequent work to explore the issues associated with errors of commission and dependencies between multiple human errors, and can provide a foundation for consideration of ways to model and quantify human errors in PRAs in a more realistic manner.

The formalized description of the framework, illustrating the inter-relationships between unsafe human actions, their influences on the plant, and the influences of the plant and PSFs on the human performance is presented in Figure 3.1.

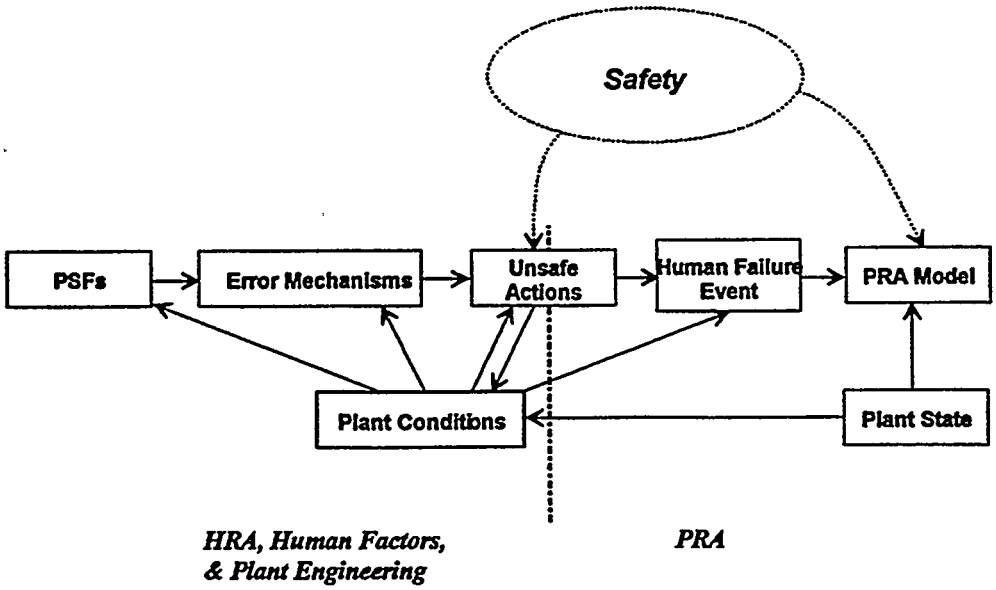


Figure 3.1 Multidisciplinary HRA framework

The elements of the framework presented in this figure accommodates the diverse perspectives of plant engineering and operations, PRA, human-factors engineering, and the behavioral sciences. Thus the framework represents the multidisciplines necessary to gain an adequate understanding of human reliability and its associated influences. This framework has emerged from the review of significant operational events at NPPs by the multidisciplinary project team which represents all of these disciplines. The elements included are the minimum necessary set to describe the causes and contributions of human errors in major NPP events as described in licensee event reports (LERs) and detailed event-based documents such as Augmented Inspection Team (AIT) reports and AEOD Human Performance Studies.

The development and application of this multidisciplinary framework is described in more detail in NUREG/CR-6265, together with a comparison with the implicit framework often used for HRA/PRA integration today. The following sections provide a summary of its elements.

3.2 Elements of the Framework

This section summarizes the principal elements of the framework and why they are important for understanding the human contribution to safety and in the representation of human errors in PRA modeling.

3.2.1 PRA Logic Models and Plant State

The PRA logic models and their associated plant states shown on the right side of the framework are no different from those used in existing PRA methodologies. For the purposes of this HRA development project, the PRA Model and Plant State are included in the framework because they represent an "end-user" of the HRA process. When human performance issues are analyzed, it is in the context of the accident scenarios represented by PRA logic models which are defined by the plant state.

3.2.2 Human Failure Events

The term "human failure event" refers to a specific type of basic event in a PRA logic model involving either an inappropriate action taken or a lack of action by plant personnel that places the plant in a greater risk condition as represented in the PRA. A "human failure event" represents the PRA systems-analysis perspective and is defined as either an error of commission (EOC) or error of omission (EOO).

As will be elaborated on in Section 4.0, there is a distinction between the PRA defined terms - EOC and EOO, and the operational event-data defined terms - unsafe act of commission (UAC) and unsafe act of omission (UAO). The UACs and UAOs are human actions identified in historical event data that degraded plant safety. How they relate to the PRA human failure event representation of an EOC or EOO is dependent on the PRA model and associated plant state. This distinction is necessary because not all unsafe actions identified in historical events are expected to be modeled as human failure events in the PRA. Several unsafe actions could combined into a single human failure event, while others could be represented in initiating event frequencies or hardware failures.

3.2.3 Unsafe Actions

Unsafe actions are those actions taken (or not taken when needed) by plant personnel that lead the plant towards a degraded safety state. Unsafe actions implies nothing about whether the action taken (or not taken) was a "human error," or that the human was the root cause of the problem. Consequently, this distinction avoids any inference of blame. Furthermore, the term "unsafe action" accommodates the assessment, based on the analysis of operational events, that people are often "set up" by cifcumstances and conditions to take the actions that were unsafe.

As alluded to above, unsafe actions depict a "finer" level of detail than most human failure events, and they are often specific to the circumstances in a particular event. For example in the evaluation of the loss of residual heat removal (RHR) cooling event at Prairie Island, Unit 2, in February 1992 (NRC/AEOD Human Performance Study Report), the unsafe actions were associated with erroneous calculations, which led operators to fail to terminate draindown before suction to the RHR cooling loop was lost. The actual observable errors were in the two calculation sheets. However, from the PRA perspective, the human-failure event would be an operator-induced loss-of-coolant accident (LOCA) during draindown to mid-loop, with a consequential loss of core cooling.

A particular attribute of unsafe actions is that they can be classified according to a simple taxonomy of types of unsafe actions developed by Reason (1990). These are slips and lapses, mistakes, and circumventions. Each is summarized below, but the reasons for distinguishing these categories are: (1) the potential impact on safety of each is different, and (2) the factors causing each are different.

Slips and lapses are unsafe actions where the outcome of the action was not what the person performing the action intended. Skipping a step in a procedure or transposing the numbers of an identification label are examples of lapses and slips respectively. The significance to risk of these unsafe actions seems to be quite small for the simple fact that these actions, not being as the "actor" intended, are easily recognized by the person involved and (in most circumstances) easily corrected.

For unsafe actions where the action was as intended, there are two broad classes of unsafe actions, e.g., mistakes and circumventions. Mistakes relate to intentional actions in which the intention is wrong. Mistakes can be considered "rule-based" or "knowledge-based" depending on whether the task is demanding rule-based or knowledge-based performance. For rule-based performance, documented, task-specific instructions are being followed (usually contained in procedures for almost all NPP activities important to safety). For knowledge-based performance, the person involved is relying on ingrained technical and specialist knowledge (as in generalized troubleshooting). Mistakes are perhaps the most significant to risk because they are being followed purposefully by the user.

Circumventions are intended unsafe actions where a person decides to break some rule for what seems to be a good (or at least benign) reason, such as reversing the steps in a procedure to simplify the task. Circumventions are potentially significant contributors to risk in that unanalyzed conditions can result from unexpected combinations of circumventions and other unsafe actions.

3.2.4 Error Mechanisms

Unsafe actions can come about from different error mechanisms. Error mechanisms are not observable in themselves, only their consequences as unsafe actions can be observed. They serve as mediators between the influences of PSFs and plant conditions, and the consequences of unsafe actions.

Examples of error mechanisms include: attentional failures, memory failures, situational appraisal failures, and knowledge failures. Different error mechanisms are primarily associated with different kinds of unsafe actions. For example, incomplete knowledge and failures in situational appraisal are error mechanisms associated with mistakes, whereas failures in attention and failures in memory are associated with slips and lapses. In consequence, the risk impact of the error mechanisms is potentially different according to the different risk impacts of the unsafe action types.

3.2.5 Performance Shaping Factors

In the original (1967) work by Swain (reported in Swain and Guttmann (1983)), a PSF was defined as "any factor that influences human performance." Such a broad interpretation has become narrowed in the practice of HRA to refer to specific features of the human-system interfaces. In the Technique for Human Error Rate Prediction (THERP) presented in Swain and Guttmann (1983), PSFs include features such as the layout and types of displays, the format of procedures, labeling of components, and administrative controls (such as checking). In other methods, PSFs have been related to the timescales of accident conditions, stress, and the availability of training (e.g., simulator training).

Given the differences between the possible error mechanisms that could be the cause of an unsafe action, the use of a single set of performance-shaping factors (PSFs) for all types of error mechanisms is inappropriate. Different error mechanisms have been found to be influenced by different sets of PSFs as identified in Table 3.1.

Table 3.1. Primary Influences Associated with Each Error Mechanism

Error Mechanism	Influences
Attentional Failures	Distraction, high workload, stress, changes in work routines, situations, or plans.
Memory Failures	Distraction, high workload, stress, and task items in which necessary knowledge must be kept in the head rather than being inherent in the task.
Situational Appraisal Failures	Counter-indications to application of appropriate rule embedded in a mass of other signals which indicate the use of a "strong-but-wrong" rule, inadequate training, inadequate procedures, inadequate supervision, and stress.
Knowledge Failures	Inadequate procedures, training, and leadership.

To date, the PSFs used in this project are those identified in the Human Performance Investigation Process (HPIP) (Paradis et al., 1993).

3.2.6 Plant Conditions

Plant conditions are the specific features of the plant and its operating state that led not only to the task being performed, but also the conditions under which it was performed. Plant conditions, in a general sense, *define the context* for the kinds of human actions being performed and the types of errors that can occur. Plant conditions are primarily associated with the state of the reactor and related systems (e.g., at-power vs. shutdown operations, equipment availability), other plant operations, and inherent design problems.

A detailed description of plant conditions is necessary to identify the possible situations where people are almost forced into failure. For example, in the February 1992 loss of residual heat removal (RHR) cooling event at Prairie Island, Unit 2, (NRC/AEOD Human Performance Study Report), the combination of PSFs associated with workload, ambiguous task requirements or instructions, inexperienced and under-trained personnel, and a lack of supervision, *together with* plant conditions associated with a high RCS nitrogen overpressure, led to an overdraining failure by operators who were draining the RCS water level to mid-loop within 48 hours of shutdown. At this time, the decay-heat level was still sufficient to cause boiling in the reactor core within 20 minutes of the loss of cooling flow.
This example indicates the level of specification for plant conditions that needs to be considered in order to define the conditions under which people can fail. In addition, it is this level of description that allows for the identification of significant EOCs since they primarily result from errors during periods of intervention with the plant (such as changing power levels, performing surveillance testing, or during LP&S operations). A more complete evaluation of this event in terms of the framework is included in NUREG/CR-6265.

Plant conditions have also been found to influence many of the other components of the framework: PSFs, error mechanisms, unsafe actions, and human-failure events. These influences are summarized as follows.

Influences on PSFs

Many PSFs are dependent on the plant conditions. For example, consider the differences between LP&S and at-power operations. Procedures are different (and often not as valid for LP&S). Instrumentation displays can be different such as RCS level being read from a plastic tygon tube during shutdown operations, rather than the electronic RCS level-measurement system. Training is different; for example, simulator-based training of operators for LP&S conditions is very rarely performed.

Influences on Error Mechanisms

Plant conditions influence error mechanisms by setting the context which determines the sensitivity of plant personnel to particular PSFs and thereby providing the opportunities for error mechanisms to become manifest and result in unsafe actions.
For instance, plant conditions pertaining draining the reactor water level to mid-loop within 48 hours of shutdown provide specific opportunities for error mechanisms to arise. Activities performed during this operation may require considerable attention to very fine details without detailed procedures and/or training. In those activities, significant opportunities for errors mechanisms associated with, for example, recognition or attentional failures, can be presented that would not be present during simpler plant evolutions.

Interactions with Unsafe Actions

Plant conditions provide the setting in which the occurrence of an error mechanism results in a specific form of unsafe action. In other words, the same error mechanism may lead to very different unsafe actions depending on the plant conditions. In addition, the unsafe actions themselves can change plant conditions, which in turn, create the potential for additional PSFs to become relevant in influencing particular error mechanisms and further unsafe actions.

Influences on Human Failure Events

Plant conditions (partly as an extension of the PRA-defined plant state) set the context for the consequences of unsafe action in terms of the impact on plant systems. For example, the distinction between errors of omission and errors commission in human failure events, is almost entirely set by the conditions represented in the PRA model, although the same unsafe action could be involved. This distinction can be illustrated by considering the unsafe action of skipping a step in a procedure. The consequences of that action under particular plant conditions, could result in, for example, failure to start a safety related system, e.g., an error of omission. However under a different set of plant conditions that unsafe action could result in performing a time critical step, prematurely (e.g., inappropriately activating a particular system that poses a significant hazard), which would constitute an error of commission.

4.0 ERRORS OF COMMISSION ANALYSIS

4.1 Introduction

Errors of commission (EOCs) have been identified as a critical area for HRA based on the review of operational experience conducted during the FY92/93 Assessment Phase of the project as reported in NUREG/CR-6093. For the FY93/94 Analysis and Characterization Phase, the primary objectives concerning EOCs were to develop the understanding necessary to bound the potentially infinite number of possible human actions which could be called "errors of commission;" identify key features of EOCs which can be used to form the basis for quantification methods; and develop guidance for identifying and modeling EOCs to be included in PRA models.

In order to accomplish these objectives, three activities were pursued:

(1) characterization of potential causes of EOCs and principles for modeling EOCs,

(2) identification of opportunities for EOCs, and

(3) development of guidance to HRA and PRA analysts with respect to both the identification and representation of a focused set of potentially risk-significant EOCs to include in PRA models.

A summary of key insights and EOC development efforts are provided in this section. A more detailed description of these efforts can be found in NUREG/CR-6265.

4.2 EOC Definition

For the purpose of this project the term "error of commission" has been defined as:

> *an overt, unsafe act that, when taken, leads to a change in plant configuration with the consequence of a degraded safety-state.*

This definition is consistent with the multidisciplinary HRA framework, and is based on the review of operational experience and the objectives of improving HRA/PRA methods. By this definition, the EOCs of interest do not include all random actions that occur in the plant. Rather, one of the important project goals is to focus more narrowly upon those overt (e.g., openly committed) EOCs that are risk-significant (e.g., degrade plant safety) and, therefore, should be included within the scope of a PRA.

In particular, the multidisciplinary HRA framework recognizes "error of commission" as a PRA term describing the potential manifestations of a human failure event on the hardware portion of the PRA model. By defining "error of commission" in the context of the PRA model, the myriad of human actions that could potentially be labelled "errors of commission" can be effectively bounded. Furthermore, the specific modeling of EOCs is dependent upon what the PRA is modeling (e.g., LP&S and at-power operations) and the objectives of the PRA model (e.g., understanding of risk vulnerabilities, risk management, design verification). Hence, in the context of the multidisciplinary HRA framework, an EOC is a human failure event modeled in a PRA which is identified and defined from the knowledge and understanding of plant conditions, unsafe acts and the objectives of the PRA.

4.3 Approach for Identifying and Characterizing EOCs

The general approach for identifying and characterizing EOCs was to use the results of event data analyses performed in this project. As discussed in Section 3.0, according to the multidisciplinary HRA framework, there is a distinction between human failure events and unsafe acts which has relevance to the use of historical event data in characterizing EOCs.

Human failure events are basic events modeled in the PRAs. Their definition is dependent upon the context of the PRA model (e.g., plant states, initiating event type). Consequently, historical event data cannot be relied upon to define EOCs, or even errors of omission (EOOs), without a specific PRA

context. However, historical event data, as reported in detailed event-based reports and full text LERs, can be reviewed to identify unsafe acts of commission (UACs) and unsafe acts of omission (UAOs). The relationship between UACs and EOCs established by the multidisciplinary HRA framework allows insights regarding the causes of EOCs, influences on EOCs, and characteristics of EOCs in general, to be gained from investigation of UACs in event data. Recognizing that there does not exist a one-to-one correspondence between UACs found in historical event data and the EOCs that get modeled as human failure events in the PRA, the strategy taken has been first to analyze and characterize the relationship between UACs found in historical event data followed by a determination of how they should relate to EOCs or EOOs that would be expected to be modeled in PRAs.

EOC analysis results based upon full-text LERs and event-based reports are briefly given below and are detailed in NUREG/CR-6265.

4.3.1 EOC Insights from LER Data

The HACS database of PWR LP&S events developed in earlier work and reported in NUREG/CR-6093 contained 39 unsafe acts and associated human performance information. Although these results are specific to LP&S conditions, some of the results obtained may have implications for other conditions and, therefore, represent significant insights which are important to the way in which future PRAs should be performed. Examples of such important results are:

- UACs occur more frequently than UAOs in LP&S.
- Human-induced initiators, especially UACs, are the most frequently occurring error kind during LP&S.
- Mistakes are the predominant error type for UACs.
- "Procedures" is the most frequently cited negative PSF associated with UACs, followed by HMI and training.
- For UAC initiators, "procedures" is the most frequently cited negative PSF associated with both slips and mistakes.

4.3.2 EOC Insights from Detailed Report-Based Events

As reported in NUREG/CR-6265, the data analysis results obtained from five events reported in NRC/AEOD Human Performance Study reports and/or NRC Regional AIT reports were judged to be useful in the further investigation and characterization of the causes of EOCs. The five events addressed by these reports are: Braidwood 1 (12/1/89), Loss of RCS Inventory (transition from cold to hot shutdown); Braidwood 1 (10/4/90), Loss of RCS Inventory (during LP&S); Crystal River 3 (12/8/91), Loss of RCS Pressure Transient (startup); Oconee 3 (3/8/91), Loss of RCS Inventory (during LP&S); and Prairie Island 2 (2/20/92), Loss of Shutdown Cooling. With one exception, all of the unsafe acts identified in these events are UACs. In addition, all identified unsafe acts are mistakes. In order to utilize all available information regarding post-accident response, intermediate actions (which would have been unsafe acts if uncorrected) have been included in this analysis. All of the intermediate (or sub-optimal) actions identified from the above reports are also classified as UAC mistakes.

Results obtained from the analysis of the five reports suggest that the underlying causes of EOCs are different for unsafe acts which are either pre-accident or initiating events compared to those which occur in response to accidents.

Insights Regarding Pre-Accident and Initiator Unsafe Acts

Three of the five event-based reports contained significant pre-accident and/or initiator UACs: Braidwood 1 (10/4/90), Prairie Island 2 (2/20/92), and Oconee 3 (3/8/91). All three of these events occurred during LP&S operations. Reviews of these events suggest that the most important influences on the unsafe acts which occurred are PSFs and significant or unusual plant conditions at the time of the event. Detailed discussion of these reviews are provided in NUREG/CR-6265. Several important points with respect to PSFs are the following:

- multiple PSFs were involved in all three events.
- all of the PSFs identified in the events are negative influences (e.g., no significant positive aids to task performance were identified).
- procedures were important to all three events.

In all three events, procedural deficiencies, involving either a lack of completeness (e.g., situation not covered) or no procedure, were a significant negative influence. This type of procedural deficiency resulted in an under-specification in how tasks are to be performed, representing a gap in guidance which allowed undesired variability in task performance. Given that all of the events involved multiple PSFs, the lack of procedural guidance may also have created the opportunity for additional negative PSFs and the unusual plant conditions to play a significant role in influencing task performance.

With respect to significant or unusual conditions, all three events represent planned activities which did not go as planned and involved some sort of change in plant state. Also, all three events involved sensitive operations related to changes in the RCS (e.g., breach of RCS pressure boundary or reduction in RPV level).

Insights Regarding Post-Accidents Actions

All five event-based reports were found useful to the investigation and characterization of causes of post-accident EOCs through the identification and analysis of UACs. Both post-accident actions and intermediate, sub-optimal actions are discussed in this section.

Reviews of the two Braidwood 1 events, and those at Prairie Island 2, Oconee 3, and Crystal River 3, suggest that PSFs and cues for diagnosis are the important influences on the opportunities for post-accident UACs. Both the Braidwood 1 (10/4/90) and Prairie Island 2 events involved significant and unusual conditions, these conditions no longer existed at the time of accident response. Consequently, plant conditions do not seem to be as directly critical to post-accident actions as they are pre-accident and initiator unsafe acts.

As identified for pre-accident and initiating unsafe acts, multiple PSFs were found to be active for many of the post accident actions. However, most of the PSFs which play a role in post-accident actions are

positive factors in task performance. In fact, only positive PSFs were identified for the successful post-accident actions while the intermediate, sub-optimal actions had only one or two negative PSFs in addition to positive PSFs. It was also found that instrumentation plays a more important role in post-accident actions than in pre-accident and initiator unsafe acts. The importance of instrumentation is consistent with the importance of diagnosis and cues for diagnosis for post-accident actions. NUREG/CR-6265 provides further details regarding the influence of PSFs on accident response.

4.3.3 Insights Regarding EOCs

Insights regarding EOCs obtained from the PWR LP&S LERs are that PRAs which address all modes of plant operation should include EOCs, particularly when they are comprised of human-induced initiators and mistakes. Also, improved HRA quantification methods must continue to address the influence of procedures on human performance. The influences of HSI and training should also be addressed. In addition, the observed influence of procedures on both slips and mistakes, indicates that improvements in procedures must address both format and content since slips are commonly associated with formatting and mistakes with technical content deficiencies.

From the reviews of event-based reports, two important insights can be drawn from the analyses of pre-accident and initiator unsafe acts. First, the consistency of results with respect to PSFs between all five events implies that, under current plant practices and the present regulatory environment, it is reasonable to expect that multiple, negative PSFs exist and can potentially influence most activities which are performed during LP&S. Consequently, the "stage" is already set and, given the right opportunity (e.g., plant conditions), an EOC is likely to be committed. Secondly, the opportunities for EOCs, should be defined by the activities which involve plant interventions and the associated conditions under which they are performed.

4.4 Identification of Opportunities for EOCs

An approach for identifying EOC opportunities was developed as an extension of the insights derived from operational experience reviews described in the previous section. In particular, two different approaches are recommended for different time phases.

As previously described, for pre-accident and initiator unsafe acts (especially during LP&S), the "stage is already set" (due to the likely existence of negative PSFs) for EOCs to be committed and that the only additional factor needed was the opportunity. Consequently, investigating features of PSFs which would be in effect when an EOC is committed will most likely not lead to useful insights regarding the occurrence of EOCs. It is reasonable to infer from operational experience that current plant operations will include multiple, negative PSFs on human performance. The opportunities for EOCs, however, seem more a function of plant design, plant conditions, and plant activities. Consequently, they represent a more focused approach (e.g., efficient) for identifying potential EOCs.

The previous section described both cues for diagnosis and the existence of an initial mindset as the important factors in EOC occurrence in the post-accident time phase. Control room instrumentation is the most frequently used, although not the only, source of information used to prompt operators to perform appropriate accident response actions. Recollections of operator training and procedures comprise the likely sources of initial mindsets. In addition, procedures will usually refer to

instrumentation to be used in accident response. Therefore for the post-accident time phase analysis of procedures and training as well as instrumentation availability could lead to important insights regarding post accident EOCs.

Based upon the above discussion, two EOC opportunity search approaches are recommended.

(1) **Mechanism Search.** For pre-accident or initiator unsafe acts, a defense-oriented approach based upon plant design and configuration, coupled with an investigation of controls (or limits) on plant conditions, especially unusual or previously unencountered conditions, and plant activities.

(2) **Procedure Search.** For post-accident unsafe acts and some initiators, a procedure search approach that includes consideration of uncertainty at decision points due to, for example, instrumentation that may be helpful and applicable in accident diagnosis. The focus of the search would be on emergency procedures for post-accident unsafe acts and on outage process procedures for LP&S initiators.

Thus far, the feasibility of these two approaches has been explored but not definitively demonstrated. They will be further refined as part of the project's ensuing Development Phase.

4.5 Guidance for Modeling EOCs

Using the results of event analyses described above, a candidate set of rules for identifying a limited scope of risk-significant EOCs to be included in PRA models has been devised that is compatible with and builds upon current HRA modeling practices. The following provides a brief summary (elaborated on in NUREG/CR-6265) of general guidelines suggested with respect to EOC modeling:

1) Different HRA/PRA modeling (e.g., identification, representation, quantification) techniques are required for EOCs included in PRAs for different plant operating modes (e.g., full-power, startup, shutdown) and different event types (e.g., loss of electric power, loss of DHR),

2) In order to identify the reasons or opportunities for plant intervention and, therefore, opportunities for EOCs, examine plant conditions which are characteristic of each plant mode modeled,

3) Investigate task- (or intervention-) specific PSFs, plant conditions, and instrumentation issues as possible "triggers" for inappropriate interventions with the plant, and

4) Give special attention to dependent unsafe acts; in particular, all typically modeled classes of unsafe acts (e.g., pre-accident, post-accident) should be modeled as usual, supplemented by those initiating and pre-accident events which have dependencies with other events.

5.0 DEPENDENCY ANALYSIS

5.1 Introduction

For the purpose of this project, the term "human dependency" is used to describe the situation where the outcome of a particular unsafe (human) action is related to, and influenced by, the outcome of a prior human action or actions. The dependency is represented by the interaction between the human actions whereby the outcome of the subsequent unsafe action is not independent of those actions preceding it. For example, in a LP&S operations event at Oconee in 1991, a blind flange was installed in the wrong penetration line from the sump to an RHR pump (a pre-initiating unsafe action). Subsequently, operators "stroke-tested" a valve in the line that should have been blocked but which, in fact, was open to the sump. As a result, the RCS was partially drained to the sump. The incorrect installation of the blind flange and the subsequent failure to confirm that the line involving the valve being tested was indeed blocked were not independent; both unsafe actions resulted from all the operators involved relying on identifying the line using an incorrect and unauthorized label. This event is discussed further in Section 5.4.

In PRA terms it is recognized that "dependency" has the property of two or more (PRA) basic events (a, b), e.g., involving unsafe or recovery actions, that causes the following probabilistic relationship to be true:

$$P(a,b) \neq P(a) \times P(b)$$

As will be discussed in Section 5.3, there are several different kinds of dependence mechanisms that can cause this relationship. In most cases, the dependence mechanisms of concern are those that influence multiple human actions in the same PRA cut-set. In keeping with the development of the framework, a multi-disciplinary approach has been taken to identify and characterize the dependence mechanisms, including the perspectives of plant engineering, PRA, and the behavioral sciences.

5.2 Framework Application For Identifying Dependence Causal Mechanisms

Section 3.0 described the multidisciplinary HRA framework that identifies how unsafe actions can contribute to safety and their relationships with the logic models used in PRAs. The framework is divided into a number of elements. These elements include: performance shaping factors (PSFs), error mechanisms, unsafe actions, plant conditions, and human failure events. As was illustrated by the Framework discussion in Section 3.0, PSFs and plant conditions play the critical role in influencing the occurrence and form of error mechanisms whose consequences are observed as unsafe actions. Thus, PSFs and plant conditions play a pivotal role in influencing the occurrence and consequence of unsafe actions. Furthermore, unsafe actions can change plant conditions and make additional PSFs more relevant in creating the opportunity for subsequent, e.g., dependent, unsafe actions.

In addition to a unique contribution to the dependence between unsafe actions, PSFs and plant conditions, have the potential for originating in common (organizational) processes. For example, a plant having an ineffective procedure-development or training program, could lead to deficiencies in those PSFs for several groups involved in numerous plant activities. Similarly, poor planning could allow multiple activities to be performed simultaneously, which can create an unanalyzed plant condition. Catalogs of

organizational processes have been developed in research programs associated with organizational processes and their influence on safety.

5.3 Types of Dependence Causal Mechanisms

NUREG/CR-6265 discusses two preliminary failure paths by which dependence mechanisms can influence unsafe actions, e.g., latent and active human failures. Latent human failures are those unsafe actions that remain hidden, possibly for some considerable time. An example of such a latent human failure was the installation of the blind flange in the wrong line as discussed in the Oconee event above. While that unsafe action did not cause any immediate safety problem; it did in fact removed, an important safety defense against inadvertent RCS draining. Alternatively, an active human failure is an unsafe action that is revealed immediately, usually by its direct impact on plant systems. The unsafe valve stroke-testing, in the Oconee event, without correctly verifying the line intended to be blocked had the immediate effect of releasing RCS inventory to the sump. Many UACs associated with initiating events are active human failures that should be represented as EOCs in PRA human failure events.

Dependence mechanisms associated with a combination of latent and active human failures (as in the Oconee example) are particularly important in PRAs because this combination can both initiate an accident sequence and cause failure of the installed safety barriers and defenses. This can change the relative contribution to risk of such sequences as well as dramatically increase the frequency of core damage, compared with sequences where such failures are truly independent.

The active and latent failure paths may originate from (e.g., be dependent on) a set of *common processes*. These common processes are the activities within the organization, such as planning, procedure development, scheduling, and so on, that fundamentally influence all plant-wide activities important to safety. These can be considered specific common-cause mechanisms. During an outage, such a common process could lead, for example, to the scheduling of maintenance on a component without ensuring alternative equipment is available (a latent failure involving a loss of a defense). For example, with replacement of RCS level instruments during draindown of the RCS level to midloop, a situation exists where the probability is much increased of an active operator error leading to an inadvertent excessive draindown and loss of core cooling.

However, not all dependencies result directly from these common processes. There can be cases where *common PSFs* may influence the probabilities of occurrence for multiple unsafe acts. Simple examples would include: the workplace environment (heat, light, displays, and so on); procedures and training; and factors directly related to human behavior, such as "ownership" of the plant, morale, motivation, technical knowledge, skills and abilities, and local peer work norms (important for circumventions).

In addition to the common PSFs, there are *plant conditions* that could result in levels of dependence between multiple unsafe acts. These include: timing between events (e.g., one event masks or coincides with another), the rates of change in plant parameters, and the inherent hazards associated with unique plant evolutions. For example, the hazards associated with partial draining of the RCS during shutdown are much greater shortly following a reactor trip (when the decay heat is high) than after an extended period of time. Because of the nature of this hazard, unsafe actions that would normally be considered independent because there is adequate time for operators to diagnose and correct each of them now compete with each other in terms of the resources to diagnose and correct them. For instance, at Prairie

Island in February 1992, where RCS overdraining occurred within 48 hours of the shutdown, operators only had a time window of about 20 minutes to diagnose and correct all failures associated with loss of RHR cooling.

Finally, there can be cases where *one failure causes another*, particularly when one failure changes the plant conditions in subtle or hidden ways. For example, a latent failure could occur during calibration actions on level measurements; the miscalibrated level instrument leads an operator to over-drain the reactor vessel. If the calibration task is being performed concurrently with the draining operation, the miscalibration has changed the plant conditions from the initial set, when the instrumentation was operable and accurate. This potential is not discussed as a primary causal mechanism because of the initial influences of a common process, common PSFs, or initial plant conditions (or, indeed, a combination of all three).

5.4 Review of Causes of Dependent Events

The purpose of this section is to review the experience of the causes of dependent events as defined above. Each of the categories of causes will be reviewed in turn. To help in this review, examples of these causes are quoted from one of the significant operational events described previously, the March 1991 event at Oconee Unit 3. NUREG/CR-6265 describes the event in terms of the multidisciplinary HRA framework and the related dependence mechanisms discussed above.

5.4.1 Common Processes

Common processes are those that, by their nature, are common-mode influences to whole groups of human actions. These include: senior management decisions, work organization and planning, procedure and training development, and other programmatic functions within the plant or utility. Deficiencies in these processes can lead to poor or erroneous performance simultaneously in most plant departments, and between work teams within departments. One simple example would be 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 would be the development of technically inaccurate procedures within the procedure-writing function, that led to errors in performance by both operations and maintenance.

The Oconee event identifies the existence of common processes. First, there were common deficiencies in the written instructions (procedures and work orders) concerning the formal identification of equipment. Neither the work instructions nor the procedures used to check the work formally identified the specific penetration number, resulting in two groups of operators separately using informal markings as the basis for identification. A further deficiency in the procedures was the absence of any requirement on the part of the final group of operators to confirm or recheck that the blind flange was correctly installed before effectively opening an un-isolated RCS drain path. This combination of deficiencies is an initial indication that the procedure development program at that plant, at that time, was deficient.

In addition, the lack of any true independent checking by the second group of operators and by the operators immediately prior to opening of the isolation valves indicated a common over-reliance on the work performed previously. There seemed to be no analysis of how the penetration could have been not isolated by the blind flange, and therefore what steps were required to confirm the correctness of the in-

stallation, either by the operator "checker" or the test crew. These unsafe actions were well separated in time (several days from start to finish). Rather than being associated with specific PSFs or the local factors such as common supervision, these actions indicate a common organizational process that tolerated the use of informal markings and an over-reliance on the quality of previous work.

For the development of an improved HRA methodology, the final quantification process will need to include an increased sensitivity to these issues that have been found in the data reviews. Approaches have been developed to evaluate the effects of common processes (Barriere et al, 1994; Davoudian et al., 1994; Williams, 1991). The integration with and application of these approaches in the development of an improved HRA methodology will be considered in the current Development Phase of the project.

5.4.2 Common PSFs

The category of common PSFs relates to the potential effects of such influences as a common procedure, a common human-systems interface, and a common training program. These have the potential, if less than adequate, of causing a significant increase in the probabilities of failures for all those actions affected by the common influences.

An example of such a common influence was observed during the event at Oconee. 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 (e.g., common PSF). 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.

The second example of a common PSF was the deficiency in training that was reflected by the inadequate checking of prior work. Standard operating practices such as rechecking the configuration prior to opening a potential RCS drain path are normally part of the training program related to this kind of activity. However, in this event, no such rechecking was performed by the operators opening the isolation valve. This failure, together with the failure to detect the incorrect installation by the checking crew, reflects a lack of training in standard operating practices.

5.4.3 Plant Conditions

In addition to the common processes and the common PSFs, the plant conditions are an important factor in creating the potential for dependent failures. The plant conditions create the environment within which the work is being performed, which can play a significant influence on all the tasks being performed. Perhaps the broadest view of plant conditions during LP&S operations is that many of the plant systems and features taken for granted during at-power operations are not available. For instance, the plant may have only one incoming electrical supply and normal instrumentation may be disconnected or non-operational, with operators having to rely on temporary measuring systems (as with level sensing at midloop at many PWRs). For most plants, limiting conditions of operation associated with the availability of equipment do not exist during outages. In addition, operators and other (sometimes transient) plant personnel are making many more manual interventions with the plant, so there are many more opportunities for EOCs or other errors that create unusual failure modes. The unusual failure modes in turn create new opportunities for error because of the previously unplanned conditions.

Beyond these very general aspects of plant conditions are the more direct task-relevant plant conditions. For example, the failures or deficiencies of temporarily installed level instrumentation have been observed to play a significant role in several events as discussed in several evaluations of LP&S events, including NRC's NUREG-1449. This particular plant condition is considered different from the PSF of human-system interface by the fact that it is the condition of the plant that renders the instruments deficient. System failures of instrumentation have the potential to cause multiple unsafe actions because they create a false perception in the minds of the operators as to the condition of the plant. This can cause operators to take inappropriate actions, which can also create difficulties in recovering from those inappropriate actions.

5.6 Analysis of Dependencies in Event Data

An analysis of the incidence of dependence mechanisms identified in reports of events is presented in NUREG/CR-6265. The following is a summary of this analysis.

Both LER and the more detailed AEOD and AIT event reports were reviewed to identify dependence mechanisms associated with multiple unsafe actions. Because of the limited descriptions in the LERs, no dependence mechanisms were identified in the relatively few events involving multiple unsafe actions.

Seven LP&S events were described in either AIT or AEOD human performance study reports. In five of the seven events, multiple unsafe actions were identified. With one exception, dependence mechanisms were identified in these events. These events are detailed in NUREG/CR-6265. Table 5.1 summarizes these events and the findings concerning dependence mechanisms.

Table 5.1 Summary of Review of AIT and AEOD Human Performance Study Reports

Plant/Event Data	Number of Unsafe Actions	Dependence Mechanisms Identified
Braidwood 1 (12/1/89)	2	common process: procedures
Diablo Canyon 1 (3/7/91)	2	common PSFs: communications, org. factors
Oconee 3 (3/8/91)	3	common PSFs: procedures, org. factors
Crystal River 3 (12/8/91)	2	common PSFs: procedures, stress
Catawba 1 (3/20/90)	2	none identified
Braidwood 1 (10/4/90)	1	none - one unsafe act
Prairie Island 2 (2/20/92)	1	one - one unsafe act

5.7 Implications

This section summarizes some simple rules to provide an initial basis for assessing the dependence between multiple human failure events in PRA models. These rules will be re-assessed during the extension of the database and the development of the quantification methods during the next phase of the project. These rules are "crude" in the sense that they are basic, simplistic, and probably do no more than bound the potential for dependencies on the basis of the observed events.

1. **Dependence between unsafe actions is the rule.** Independence requires that there be:
   - no common procedures,
   - no common PSFs,
   - no common hardware, and
   - no common personnel,

   even if the actions are well separated in time. The sparse reporting of dependencies in the LERs is seen more as an omission in the reports than as an absence of dependencies in the events. Of the five AIT or AEOD reports identifying more than one unsafe act, only one did not identify dependencies.

2. **Any initiating event that is instrument-driven will have adverse effects in the recovery phase.** Numerous examples exist where a faulty or flawed instrumentation system induced operators to initiate an accident and subsequently, limited their ability to diagnose the accident.

3. **Operations that are not as planned, or as intended by the planners or supervisors, degrade the ability of operators to terminate problems.** Such operations have been reported during LP&S operations, as in the case of the loss of RHR cooling at Catawba 1 (3/20/90).

6.0 CONCLUSIONS

As discussed in the preceding sections, the FY93/94 Analysis and Characterization Phase included the development of a multidisciplinary framework for integrating HRA with PRA, and the characterization of EOCs and human dependencies including general guidance for their identification and representation in PRAs. Implications from these accomplishments are summarized below, followed by a discussion of follow-on efforts in support of the project's current Development Phase.

6.1 Research Implications

Framework Implications

The multidisciplinary HRA framework discussed in Section 3.0, represents an important accomplishment of the Analysis and Characterization Phase in that it provided an orderly and rational structure for the consideration of human-systems interactions in NPP safety. To understand required areas for development in HRA, e.g., to address concerns that HRA techniques do not represent realistically the roles that humans play, both in creating and preventing accident conditions (e.g., NUREG-1050), it was necessary to develop an explicit framework of how the disciplines of human factors, behavioral science,

plant engineering, HRA and PRA are related. The development of this explicit framework was based on a review of significant operational events and the intention to make any new developments in HRA to be as representative of real-world events as possible.

In order to best address current HRA concerns, it was important that the framework describe the relationships between PSFs, human error mechanisms, unsafe actions and plant conditions. In addition, to enable integration into the PRA, the framework needed to identify the relationship between human failure events, associated PRA models, and plant states (e.g., as defined by the PRA). By identifying the linkages between these framework elements, a more explicit description of the human contribution to risk and the salient characteristics of severe accidents is discernible.

As utilized in the Analysis and Characterization Phase, the framework provided the capability to identify factors that influence humans to perform unsafe actions and thereby created a systematic basis for evaluating the significance and characteristics of EOCs and dependency, from operational events. Thus, the framework has enabled important aspects of EOCs and dependency to be considered in the development of an improved HRA methodology and has clarified the requirements for their more realistic inclusion in PRA models. By the framework's provision of a single language and common structure for relating the different dimensions of human-system interactions, the evaluations of EOCs and dependencies has been demonstrated to be both tractable and tenable. Considering the importance of these issues in NPP safety, this change is an important advance. These EOC and dependency capabilities will be refined and expanded upon in subsequent tasks pertaining to the Development Phase.

Finally, the use of the framework and its applications to consideration of errors of commission and dependencies will provide a rational basis for the estimation of their associated error probabilities and incorporation into PRA human failure events. While the details of these activities are still under development, it is clear that the systematic structuring of the different dimensions influencing human-system interactions brings a degree of clarity and completeness to the process of modeling human errors in the PRA process. The absence of this systematic approach has limited the ability to incorporate human errors in the PRA process in a way that could satisfy both the engineering and the behavioral sciences. The consequence has been a lack of credibility of the results of PRAs in terms of their representation of the contribution of human errors to power-plant safety, particularly when compared with the experience of major power-plant accidents and incidents, where human error has proved to be the dominant factor.

As was stated earlier, the framework continues to evolve. It is expected that as knowledge in the behavioral sciences develops, as more events are reviewed, and as subsequent tasks are performed, the framework will expand. This capability to adapt and expand the framework is seen as an important feature in support of developing an improved HRA method.

EOC Implications

The research efforts summarized in Section 4.0, provide valuable insights concerning EOCs. The identification of important EOC characteristics required a break from the familiar perspective on human reliability influences and the underlying assumptions of PRA models. This capability was provided through he use of the framework elements. For instance, plant conditions, when defined at a more detailed level than currently used in PRA models, were shown to be important influences on both human performance and accident consequences. For example, interpretation of instrument indications and implementation of procedures cannot be assumed to be correct or uniform under the variety of possible

plant conditions. Based upon these insights, plant conditions, PSFs, and instrumentation are considered important factors in the identification, representation and quantification of EOCs, due to their significant influence on EOC occurrence.

This work indicates that the previously perceived infinite sink of EOCs, in fact, can be bounded. The EOCs which should be explicitly modeled in PRAs can be found through the approaches for identifying opportunities for EOCs that degrade plant-safety. It is recognized that certain EOCs can continue to be modeled implicitly in PRAs through initiating event frequencies and hardware unavailabilities. The next phase of this project will refine the guidance for which EOCs to explicitly or implicitly model and how to conduct appropriate EOC search techniques; e.g., procedures (EOPs) and mechanism searches. The incorporation of these EOC insights into an improved, integrated HRA/PRA approach will be a stepwise improvement in current PRA modeling practices, rather than a complete departure from them.

Dependency Implications

The evaluation of operational events (e.g., described in the more detailed AIT and AEOD reports) in the context of the multidisciplinary framework, indicated that, a majority of the events do involve multiple unsafe actions for which there exist dependence mechanisms. These dependent mechanisms were defined as common processes, common PSFs and Plant Conditions. Based on the research efforts summarized in Section 5.0, it has been demonstrated that these dependence mechanisms represent a useable and useful taxonomy for understanding the specific causes of dependent unsafe actions and developing an aid for the analysis of events and the structuring of data. This taxonomy will allow the explicit consideration of dependence mechanisms in the PRA modeling and quantification stages to be developed in the next phase of this project. In the interim, some simple rules for modeling human failure events in PRAs have been provided.

6.2 Follow on Efforts

The primary product of the current Development Phase will be a working HRA quantification process that includes the following: how to identify and incorporate human failure events in the logic models used in PRAs, what information is required for probabilities to be assigned to these failure events, how this information is used to estimate the probabilities, and how the probabilities are incorporated into the PRA quantification process. A detailed program plan for performing the development requirements has been defined as in included in NUREG/CR-6265. The following briefly summarizes the development approach.

Development Approach

The results of these research efforts pertaining to the project's Analysis and Characterization Phase have set in place the basic concepts of an improved HRA method. They have served as the basis for retrospective analysis of real operating event histories. That retrospective analysis has identified the context in which severe events can occur; specifically, the plant conditions, significant PSFs, and dependencies that "set up" operators for failure. It remains to specify how to use the framework to perform prospective analysis; i.e. how to specify the context so that we can identify and predict important EOCs and crucial dependencies.

In order to relate an expanded description of human-system interactions to the PRA modeling process, it will be necessary to develop specific changes for PRA logic models that enable the accommodation of an expanded understanding of human-system interactions; e.g., based on the detailed analysis of operating experience from a multidisciplinary perspective. This will be especially relevant for the accommodation of EOCs in event trees, the ability to link multiple failure dependencies in fault trees, and the handling of recovery modeling in both (event trees and fault trees).

In order to improve its usefulness to the overall methods development phase effort, several improvements to the project's multidisciplinary framework are necessary. These improvements include a more explicit representation of circumventions and their associated PSFs, and the development of a taxonomy for plant conditions. Specifically, the development of taxonomies associated with plant conditions are expected to be both engineering-related and (human) behavioral-related; they will clarify potential plant conditions associated with LP&S and at-power operations as well as RCS parameters. Finally, there will be a simplification of the current error mechanisms classification.

In support of any achievements made during this development phase the importance of basing them on actual operating experience can not be over stated. Consequently, the development of an extended database that describes "real-world" events involving human-system interactions is considered a critical activity. The expansion of the database will provide a basis for an improved quantification process with respect to supporting operating experience insights that can be described and presented in relation to the components in the multidisciplinary framework. In support of expanding the database, a detailed analyses of events will be conducted and include the assessment of time scales of dynamic human-system interactions. While the goal is to analyze about 30-40 events, it is realized that each analyses, to be conducted appropriately, is very labor-intensive. Consequently, the need for collaboration with other potential data sources is recognized.

The final requirement to improve the HRA methodology is the need to develop an expert-judgment elicitation process for quantification. In order for this elicitation process to be effective it considered paramount that the process be based on "real-world" experience, interpreted by a multidisciplinary team of experts (e.g., plant engineering, human factors, and behavioral science). In order to present real world experience for consideration by the experts the need for developing an operational experience frame of reference manual has been identified. The expertise required to be involved in the actual elicitation process includes plant engineering and operations, human error analysis and PRA. To improve the acceptability of the expert elicitation process an extension of currently existing expert-elicitation processes is required. Of equal, if not greater importance, is the need for the process to handle PRA requirements. This includes, for example, the capability of the process to provide point estimates, uncertainties, and sensitivities.

NUREG/CR-6265 provides further details on these requirements.

7.0 References

Barriere, M.T., Luckas, W.J., Stock, D.A. and Haber, S.B., "Incorporating Organizational Factors into Human Error Probability Estimation and Probabilistic Risk Assessment," Technical Report A3956-3/94, Brookhaven National Laboratory, Upton, NY 1994.

Davoudian, K., Wu, J. S., and Apostolakis, G., "Incorporating Organizational Factors into Risk Assessment Through the Analysis of Work Processes", *Reliability Engineering and System Safety*, Elsevier: New York, NY 1994.

NRC/AEOD Human Performance Study Report, Braidwood Unit 1, October 4, 1990, "On-Site Investigation and Analysis of the Human Factors of an Event," U.S. Nuclear Regulatory Commission: Washington, DC, October 1990.

..., Catawba Unit 1, March 20, 1990, "On-Site Analysis of the Human Factors of an Event," U.S. Nuclear Regulatory Commission: Washington, DC, May 1990.

..., Crystal River Unit 3, December 8, 1991, "On-Site Analysis of the Human Factors of an Event (Pressurizer Spray Valve Failure)," U.S. Nuclear Regulatory Commission: Washington, DC, January 1992.

..., Oconee Unit 3, March 8, 1991, "On-Site Analysis of the Human Factors of an Event (Loss of RHR Cooling)," U.S. Nuclear Regulatory Commission, Washington, DC: May 1991.

..., Prairie Island Unit 2, February 20, 1992, "On-Site Analysis of the Human Factors of an Event (Loss of RHR Cooling)," U.S. Nuclear Regulatory Commission: Washington, DC, March 1992.

NRC Regional Augmented Inspection Team Report, Braidwood Unit 1, December 1, 1989, "Loss of RCS Inventory via RHR Relief Valve," Report No. 50-456/89-006, U.S. Nuclear Regulatory Commission, Washington, DC: December 29, 1989.

..., Diablo Canyon Unit 1, March 7, 1991, "Loss of Off-Site Power," Report No. 50-275/91-009, U.S. Nuclear Regulatory Commission: Washington, DC, April 17, 1991.

..., Oconee Unit 3, March 8, 1991, "Loss of RHR," Report No. 50-287/91-008, U.S. Nuclear Regulatory Commission: Washington, DC, April 10, 1991.

..., Prairie Island Unit 2, February 20, 1992, "Loss of RHR," Report No. 50-306/92-005, U.S. Nuclear Regulatory Commission: Washington, DC, March 17, 1992.

NUREG-1050, "Probabilistic Risk Assessment Reference Document", U.S. Nuclear Regulatory Commission: Washington, DC, September, 1984.

NUREG-1480, "Loss of an Iridium-192 Source and Therapy Misadministration at Indiana Regional Cancer Center, Indiana, Pennsylvania on November 16, 1992", U.S. Nuclear Regulatory Commission: Washington, DC, 1993.

NUREG-1449, "Shutdown and Low Power Operation at Commercial Nuclear Power Plants in the United States", U.S. Nuclear Regulatory Commission: Washington, DC, 1994.

NUREG/CR-6093, "An Analysis of Operational Experience During LP&S and A Plan for Addressing Human Reliability Assessment Issues," Barriere, M.T., Luckas, W.J., Whitehead, D.W., and Ramey-Smith, A., Brookhaven National Laboratory: Upton, NY and Sandia National Laboratories: Albuquerque, NM, 1994.

NUREG/CR-6265 (DRAFT), "Multidisciplinary Framework for Analyzing Errors of Commission and Dependencies in Human Reliability Analysis," Barriere, M.T., Luckas, W.J., Cooper, S.E, Wreathall, J., Bley, D.C. Bley, Ramey-Smith, A., and Thompson, C.M., Brookhaven National Laboratory: Upton, NY, 1994.

Paradies, M., Unger, L., Haas, P. and Terranova, M., "Development of the NRC's Human Performance Investigation Process (HPIP)", NUREG\CR-5455, System Improvements, Inc.: Aiken, SC, October 1993.

Reason, J., *Human Error*, Cambridge University Press: Cambridge, MA, 1990.

Swain, A.D. and Guttmann, H.E., "Human Reliability Analysis with Emphasis on Nuclear Power Plants", NUREG/CR-1278, Final Report, Sandia National Laboratories: Albuquerque, NM, August 1983.

Williams, J.C., The Management Assessment Guidelines in the Evaluation of Risk (MANAGER) Technique, *Proceedings of the International Conference on Probabilistic Safety Assessment and Management (PSAM)*, Elsevier: New York, NY, 1991.

Operational Reliability of Standby Safety Systems[a]

Gary M. Grant, Corwin L. Atwood, and Cynthia D. Gentillon
Idaho National Engineering Laboratory

Dale M. Rasmuson and John R. Boardman
U.S. Nuclear Regulatory Commission
Office for Analysis and Evaluation of Operational Data

ABSTRACT

The Idaho National Engineering Laboratory (INEL) is evaluating the operational reliability of several risk-significant standby safety systems based on the operating experience at U.S. commercial nuclear power plants from 1987 through 1993. The reliability assessed is the probability that the system will perform its Probabilistic Risk Assessment (PRA) defined safety function. The quantitative estimates of system reliability are expected to be useful in risk-based regulation. This paper is an overview of the analysis methods and the results of the high pressure coolant injection (HPCI) system reliability study. Key characteristics include (1) descriptions of the data collection and analysis methods, (2) the statistical methods employed to estimate operational unreliability, (3) a description of how the operational unreliability estimates were compared with typical PRA results, both overall and for each dominant failure mode, and (4) a summary of results of the study.

1. INTRODUCTION

The U.S. Nuclear Regulatory Commission's (NRC's) Office for Analysis and Evaluation of Operational Data (AEOD) is sponsoring a program to monitor and report on the performance of certain systems and components in U.S. commercial nuclear power plants. These systems and components were chosen for their importance to safety. As part of the program, the performance of the high pressure coolant injection (HPCI) system found in boiling water reactor (BWR) plants was evaluated.

The HPCI system performance study[1] was based on operating experience during 1987 through 1993 as reported in Licensee Event Reports (LERs) and monthly nuclear power plant operating reports. The study had three objectives:

---

a. Work supported by the U.S. Nuclear Regulatory Commission, Office for Analysis and Evaluation of Operational Data, under DOE Contract No. DE-AC07-94ID13223.

1. Analyze the trends and patterns in HPCI system performance, including increasing or decreasing failure probabilities with time, effects of regulatory actions, variation in performance among the plants and identification of significantly higher or lower-than-average unreliability, and identification of the predominant causes of failures.

2. Quantitatively estimate HPCI system operational unreliability, including industry-average and plant-specific unreliability and the statistical uncertainty of these results.

3. Compare HPCI system performance as predicted by PRAs to HPCI system performance based on industry experience.

Future AEOD studies will (a) evaluate the frequency trends for accident initiating events, (b) develop component performance studies for selected components of particular interest to safety, and (c) periodically update each of the system and component performance studies by adding the latest operational experience and using improved methodologies.

2. METHODS OF ANALYSES

To characterize HPCI system performance, operational data from U.S. commercial nuclear power plants from 1987 through 1993 were collected and reviewed. Because HPCI is a safety system, any malfunctions that result in the system not being operable as defined by the respective plant technical specifications or the Safety Analysis Report are required by 10 CFR 50.73 to be reported in LERs. Therefore, only the LERs were searched for such events.

In this paper, the term ***inoperability*** is used to describe any LER-reported HPCI event in which the HPCI system did not meet the operability requirements identified in applicable plant technical specifications or the Safety Analysis Report. It is distinguished from the term ***failure***, which is an inoperability for which the safety injection function of the system (the ability to inject coolant on demand) is lost. Failures include such problems as failures to start and failures to run. Inoperabilities include these, and also problems such as events related to seismic design, and administrative events such as late performance of a test. Because analysis of the containment isolation safety function of HPCI was not performed in this study, events such as failure to isolate the turbine steam supply were regarded as inoperabilities but not failures.

The analyses presented in this paper have a progressively narrower focus. First, the inoperabilities, both failures and nonfailures, are summarized and examined for simple trends or patterns. Then, the failures are characterized from an engineering perspective to identify the major issues of system performance. Then, the system's ***operational unreliability*** is estimated from the failures for which the number of system demands could also be determined or estimated. The term operational unreliability is used to describe the probability that the system will fail when demanded, and the word operational emphasizes that it is estimated from train-level LER data. Figure 1

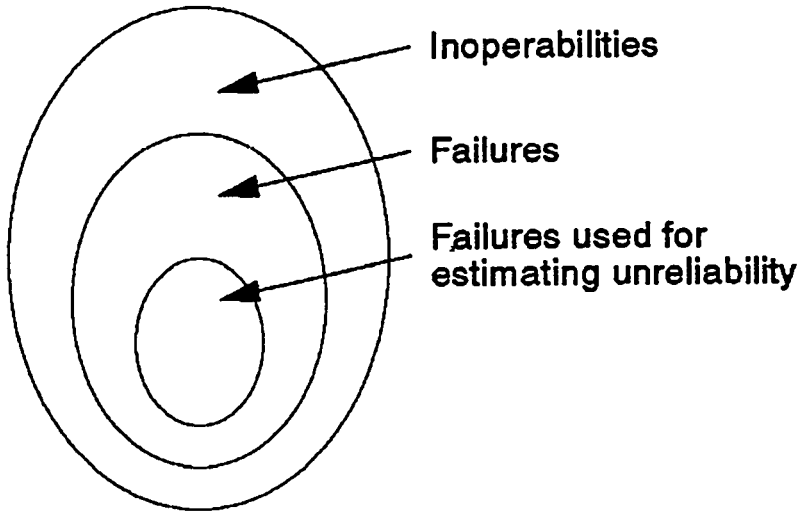


Figure 1. Illustration of HPCI inoperability and failure data sets.

illustrates the inoperability and failure data sets. The comparisons with PRAs use both the engineering assessment of failures and the estimated unreliability.

The scopes of analyses considered in each phase of the study are described briefly in subsections below.

2.1 Data Collection and Classification

2.1.1 Inoperability and Failure Data

To identify HPCI inoperabilities reported in the LERs, the Oak Ridge National Laboratory Sequence Coding and Search System (SCSS) LER database was searched for all records for the years 1987 through 1993 that refer to an actual or potential HPCI system inoperability. Each identified LER was read completely to determine the types of failures, the causes, and other useful information, and the data used for this study were entered into a database. To characterize HPCI system performance, each inoperability was classified by:

- Whether the HPCI system's safety injection function was lost
- The method of discovery of the event
- The immediate cause of the event (e.g., equipment, personnel, or procedures), the subsystem and component involved in the inoperability, and other useful descriptions.

For failures, a particularly important additional event attribute is the system failure mode. When the HPCI system receives an automatic start signal as a result of an actual low RPV water level condition, the system functions successfully if the turbine starts and obtains rated speed and coolant pressure, the injection valve opens, and rated coolant flow is delivered to the RPV until the flow is no longer needed. Failure may occur at any point in this process. For the purposes of this study, failure modes that can occur in response to an actual low RPV water level are defined below.

- Maintenance out of service (MOOS) occurs if, due to testing or maintenance, the HPCI system control switches are blocked and, thus, the system is prevented from starting automatically.

- Failure to start (FTS) occurs if the system is in service but fails to automatically start, obtain rated speed in the turbine, develop design coolant pressure, or achieve at least 90% of the rated coolant flow. As described in Section 2.3.1, this failure mode was divided into two modes for the quantification.

- Failure to run (FTR) occurs if, at any time after the system is delivering at least 90% of the rated coolant flow, the HPCI system fails to maintain this flow while it is needed.

A final failure attribute that deserves mention concerns whether operator actions successfully recover from a failure. To recover from failure to start, operators had to recognize that the system was in a failed state, restart it without performing maintenance (for example, without replacing components), and restore coolant flow to the RPV. An example of such a recovery would be an operator (1) noticing that the injection motor operated valve (MOV) had not opened during an automatic start of the system and (2) manually operating the control switch for this valve, thereby causing the MOV to open fully and allow rated coolant flow to the RPV. Recovery from failure to run similarly defined. Each failure is evaluated based on whether recovery by the operator occurred.

The failures were then characterized from an engineering viewpoint to identify the dominant modes and causes. This engineering review was a major element of the study.

2.1.2 Selection of Unplanned Demand Data

To estimate operational unreliability, information on the frequency and nature of HPCI demands was needed. The LERs provided information on unplanned demands following plant transients that resulted in an actual low RPV water level condition, that is, in an actual need for the HPCI system. These demands were identified by searching the SCSS database for all HPCI actuations. Unplanned HPCI demands are a 10 CFR 50.72/73 reportability requirement, and, therefore, the count of unplanned demands of the system is believed to be correct.

The unplanned demand records were screened to identify the nature of the HPCI demand. Many of the demands were either actuations of only a part of the system, or actuations of the feedwater coolant injection system. The partial actuations included suction path shifts and relay actuations related to plant maintenance actions such as removal of a fuse or shorting of test leads. These partial actuations did not exercise the HPCI system in response to an actual need for injection. Therefore, these records were excluded from the count of HPCI unplanned demands.

In approximately five percent of the remaining events for which RPV inventory needed to be restored, HPCI was not actually used to inject coolant because the need was met by the RCIC system or main feedwater. The HPCI turbine was started in most of these events, but in all these cases either the system was secured by plant operators or RPV level was restored prior to the logic being satisfied to open the HPCI injection MOV. These incomplete HPCI demands were used only in the estimation of the MOOS failure probability. Depending on the nature of the demand, they may also indicate success for the system starting, except for the injection MOV. However, they were not used in this way in this study because the LER narratives did not clarify whether rated pressure was achieved.

2.1.3 Selection of Surveillance Data

Routine surveillance tests of the HPCI system are performed every operating cycle, quarter, and month; these tests may provide more data for estimating HPCI system reliability. HPCI failures during these tests are a 10.CFR 50.73 reportability requirement, since HPCI is a safety system. Therefore, the failure count from routine surveillance tests is believed to be as complete as possible. To ensure accuracy in comparing the surveillance test demands and associated failures with the type of demand modeled in the PRAs, the completeness of each of these tests was evaluated based on a detailed review of technical specifications for design class 3 and 4 BWRs. The conclusions of the technical specifications review are as follows:

- The cyclic surveillance tests require the system to be functionally tested. This testing includes simulated automatic actuation of the system throughout its emergency operating sequence and verification that each automatic valve in the flow path actuates to its correct position. The ability of the HPCI turbine to sustain coolant flow (in a recirculation mode) over a period of time is also verified. However, these cyclic surveillance tests do not in all cases challenge the injection MOV at the pressures, flow rates, and temperatures that the system would experience during a demand for emergency operation. Some plant technical specifications actually state that injection of coolant into the reactor vessel may be excluded from the test. Therefore, the cyclic surveillance tests were regarded as demands on the system except for the injection MOV. Test failures reported in LERs can be identified as occurring on cyclic tests by supplementing the LER narrative with the event date and the dates of the plant's refueling outages, because cyclic tests are typically performed just after a refueling outage.

- The quarterly tests also test the entire system except for the injection MOV. However, the LERs do not always specify what type of surveillance test was being performed when a failure occurred. For some plants, failures during quarterly tests and postmaintenance tests are indistinguishable in the LERs. The date of the event does not help distinguish the two. Since postmaintenance surveillance tests are not periodic, realistic demand counts for these tests cannot be estimated. Therefore, both quarterly and postmaintenance test results were not used for estimating unreliability.

- Monthly tests exercise even less of the system, and, therefore, were not used.

Only the estimation of unreliability involved data exclusions; the engineering evaluation used all system failures identified from the data searches.

The overall number of cyclic surveillance tests was approximated by assuming that there was a test following each refueling outage. If successive refueling outages were more than 18 months apart and outside the technical specification requirements for the testing periodicity, an additional test was assumed to have occurred during the mid-cycle outage.

2.2 Engineering Review of HPCI Failure

An engineering review evaluated the HPCI system failures. The review evaluated, from an engineering perspective, the overall significance of HPCI system failures and the nature of failures at particular plant units. It focuses on the failure modes, subsystems, and causes of the active system failures that occurred on unplanned demands and surveillance tests.

2.3 Estimation of HPCI Unreliability

This analysis used failures only for which a corresponding number of demands could be determined or estimated. The probability of failure on demand was then estimated for the relevant failure modes, which are, in rough terms, out of service for testing or maintenance, failure to start, failure to run, and failure to recover. The analysis considered possible differences in failure probabilities between years, plants, and/or stations. The HPCI unreliability was evaluated using a simple fault tree model of system failure in terms of the failure modes. The evaluation resulted in a mean probability of system failure on demand, which is the best estimate of the unreliability, and a tolerance interval for the unreliability, which provides reasonable upper and lower limits.

Methods for three topics are outlined in this section: selection and use of the data to estimate probabilities for each individual failure mode, estimation of the corresponding failure probability distributions (generic or for particular years and plants, and estimation of the operational unreliability for continuous injection (generic or for particular years and plants).

2.3.1 Preliminary Analysis of Individual Failure Modes

For the evaluation of unreliability, six failure modes were defined: (1) out of service for maintenance or testing at the time of a demand (MOOS), (2) FTS from injection valve problems (FTSV), (3) FTS from other than injection valve problems (FTSO), (4) failure to recover from failure to start (FRFTS), (5) failure to run for the required duration of HPCI performance given a successful start (FTR), and (6) failure to recover from failure to run (FRFTR).

These failure modes are derived directly from the failure mode codes assigned to the LER failure records, with two exceptions. First, the fail to start mode was split into two modes because, as stated above, the cyclic surveillance tests rarely provide an adequate challenge for the RPV injection valve. The possibility of injection valve failures interfering with continuous injection was deemed negligible, so the FTR mode was not split into failure from injection valve and other problems.

The second difference in failure mode usage for estimation of operational unreliability concerns the treatment of FTR injection valve failures that occurred during *intermittent* HPCI system RPV injection. (Intermittent injection, in which the system alternates between injection and pressure control, is discussed in Section 3.2.) These events were excluded from the FTR quantitative analysis. From the data, intermittent injection appears to cause a higher level of stress on the injection valve than ordinary continuous injection. Therefore, FTR probabilities for the intermittent injection scenario need to be estimated separately from the FTR probability during the initial (continuous) phase of HPCI injection. However, the LERs that describe unplanned demands of the HPCI system do not consistently address whether this mode of operation was used. Thus, even for unplanned demands, the number of successful intermittent injection operations of the HPCI system is not known, and a separate probability cannot be estimated from the existing LER data. Also, intermittent injection is not an operational mode for response to design basis events, as modeled in the PRAs.

Failures from common cause events that might affect both HPCI and RCIC were not analyzed in a special way; if such an event caused HPCI to fail, it was simply counted as a failure.

To estimate failure rates for the six failure modes under consideration, the number of failures and demands for each failure mode must be determined. Two issues require resolution in this process. First, selection of the data sets to use for these determinations is required. There are two possible data sets: unplanned actuation data and cyclic surveillance data. The second issue is the adjustment of overall demand counts for particular failure modes. These are discussed below.

MOOS is seen only with unplanned demands, so only MOOS events occurring on unplanned demands were used to estimate maintenance unavailability. The probability of failure to start from injection valve problems (FTSV) was also quantified using only unplanned demand data because, as stated above, cyclic

surveillance tests do not adequately challenge the injection valve. The same comment applies to the two recovery failure modes (FRFTS and FRFTR), since recovery goals differ for tests and for unplanned demands (during tests, diagnostic actions are more important than quick recovery actions).

For the two remaining failure modes, FTSO and FTR, cyclic surveillance test data were analyzed in addition to data from unplanned demands. The total numbers of failures and demands were counted or estimated for each failure mode and each data source separately.

Note that, in this analysis process, the FTR probabilities were based on failures to meet a demand for performance for some (possibly unstated) mission time. This differs from the conventional approach, which finds a failure rate, λ, and specifically accounts for the resulting fact that the unreliability tends to increase as the mission time gets longer. Time-based estimates were not generated in this operational unreliability study because of the difficulty of quantifying mission times and operational times. To the extent that these times are known for the operational events, they are relatively short (e.g., less than ten minutes). For this study, the failure to run probabilities are assumed to be independent of mission time over the range of actual mission times occurring in the operational data.

2.3.2 Distributions for Each Failure Mode

Distributions for the failure probability for each failure mode were estimated. In this process, two kinds of variation were considered: random variation in failure counts and systematic variation between different years and plants . The ideas are illustrated here in terms of plants, but they apply equally to years and stations.

For each failure mode, the first assessment dealt with whether the variation between plants was large enough to be estimated. In principle, such variation exists, but it may be completely masked by the random variation in the event counts. A distribution describing the variation between plants was estimated from the data. The resulting generic distribution is called the *empirical Bayes* distribution because it is the distribution that is combined with plant-specific failure data to yield plant-specific failure probability distribution for each plant.

When the variation between plants was too small to be estimated from the available data, the failures from all the plants and the demands from all the plants were each pooled. Parameters were computed to determine a single beta distribution describing the generic failure probability for the failure mode. Percentile bounds for this distribution are numerically similar to confidence intervals and become more narrow as additional data accrue.

In summary, the empirical Bayes method, which was used whenever possible, modeled between-plant variation and yielded a generic industry distribution and a plant-specific distribution for each plant. The simple Bayes method, which was used when the variation between plants was too small to estimate, yielded a generic distribution for the failure probability that reflected the

randomness of the failure data but did not account for any variation between plants.

The Jeffreys noninformative prior was used for the simple Bayes method. The empirical Bayes prior distribution was estimated by maximum likelihood. For particular analyses, year or plant distributions that maximize the influence of the plant-specific data were needed, even if the data showed no particular evidence of between-plant differences; in these cases, the plant-specific data were combined with a diffuse prior distribution having the industry mean. All plant-specific distributions included modeling that accounted for the uncertainty in estimating prior distribution parameters. All assumed models were checked to make sure that they adequately fitted the data.

2.3.3 Operational Unreliability

The operational unreliability of the HPCI system was evaluated using the failure probability distributions for the six failure modes. The logic for combining these distributions was provided by the fault tree model shown in Figure 2. The IRRAS[2] software package was used to evaluate the fault tree logic to produce a mean value for the probability that the system will fail to provide continuous injection for the required mission time and the bounds on a 90 percent uncertainty interval for the value of the failure probability. The

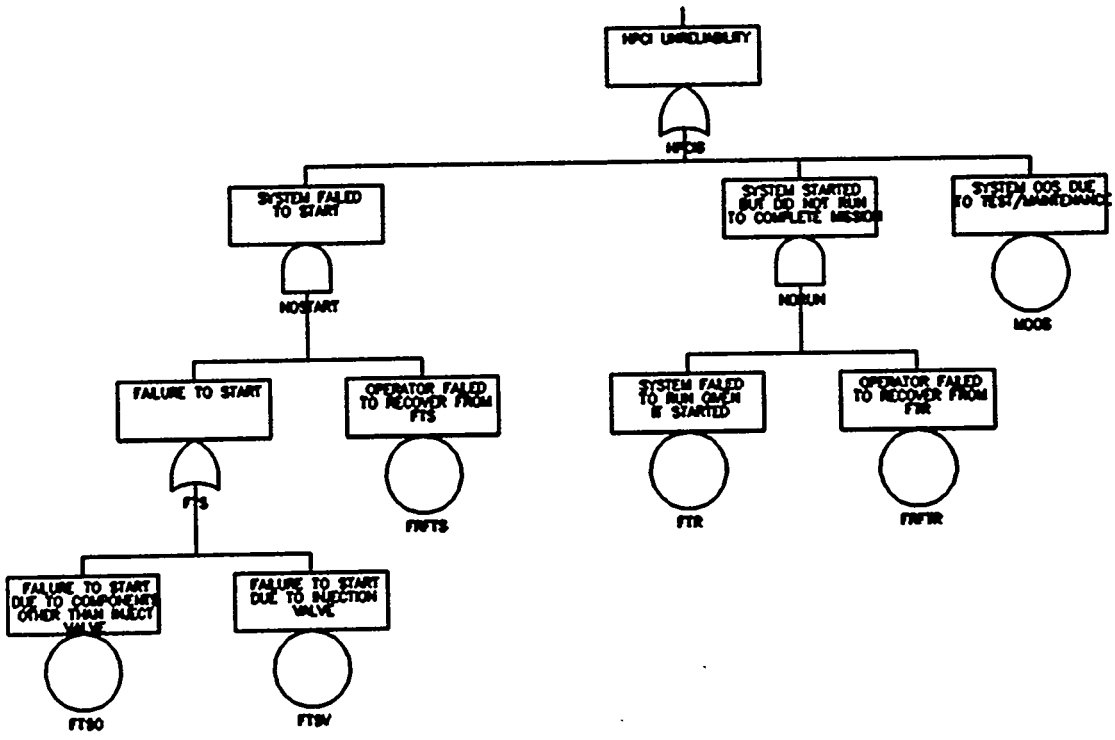


Figure 2. HPCI unreliability evaluation model (includes recovery).

mean failure probability that was determined is the best estimate of the operational unreliability based on all of the BWR operating experience during the period from 1987 through 1993. The bounds on the uncertainty interval for the operational unreliability were determined by a 5000-sample Monte Carlo analysis of the system failure probability performed by the IRRAS code.

Operational unreliabilities and associated uncertainty intervals for specific plants and specific years were evaluated using failure probability distributions for the six failure modes based on plant- or year-specific operating experience. These values were not determined using the IRRAS code, but were, instead, closely approximated algebraically.

The operational unreliabilities determined using industry operating experience are probably nonconservative relative to reactor transient or accident conditions. This nonconservatism is due to the FTR probability distribution being based on the results of cyclic surveillance tests and unplanned demands, which were caused by a loss of feedwater, not on design basis demands (LOCAs), which have much longer mission times than were actually observed. For example, if an observed demand occurred in which the HPCI system was required to be run for only ten minutes, and it did, the event was counted as a success. If the system was needed for two hours but only ran for one hour, then the event was counted as a failure. The operating experience during the study period provided the best available data on which to base an evaluation of operational unreliability, but none of the observed demands had mission times on the order of 10 to 24 hours, which are typically used in modelling the HPCI system in plant PRAs.

2.4 Analysis of Operational Unreliability

The industry experience with HPCI performance, both plant-specific and industry-wide, was used to assess the modeling of this system in selected full-scale plant PRAs. In order to make this assessment, it was necessary to adjust both the fault tree model used to evaluate system unreliability shown in Figure 2 and the plant PRA fault tree models to obtain comparable results. The need for these adjustments limited the number of PRAs that could be assessed to three for which IRRAS databases were readily available.

The fault tree in Figure 2 was adjusted by removing the failure to recover basic events (FRFTS and FRFTR), since these events were not modeled at the system level in PRA fault trees. The resulting fault tree, shown in Figure 3, was used to evaluate the HPCI failure probability and associated uncertainty interval using the same probability distributions for the remaining basic failure events that were used to evaluate system unreliability. The evaluation was performed using the IRRAS code.

The PRA fault trees were adjusted to remove failures due to support systems in order to compare unavailability based on models similar to the operational experience models. The cutsets that were removed involved loss of AC power buses that supply the HPCI inverters and loss of emergency service water used to cool the HPCI room coolers. Once the cutsets were removed, quantification of the failure probability and Monte Carlo analysis of the

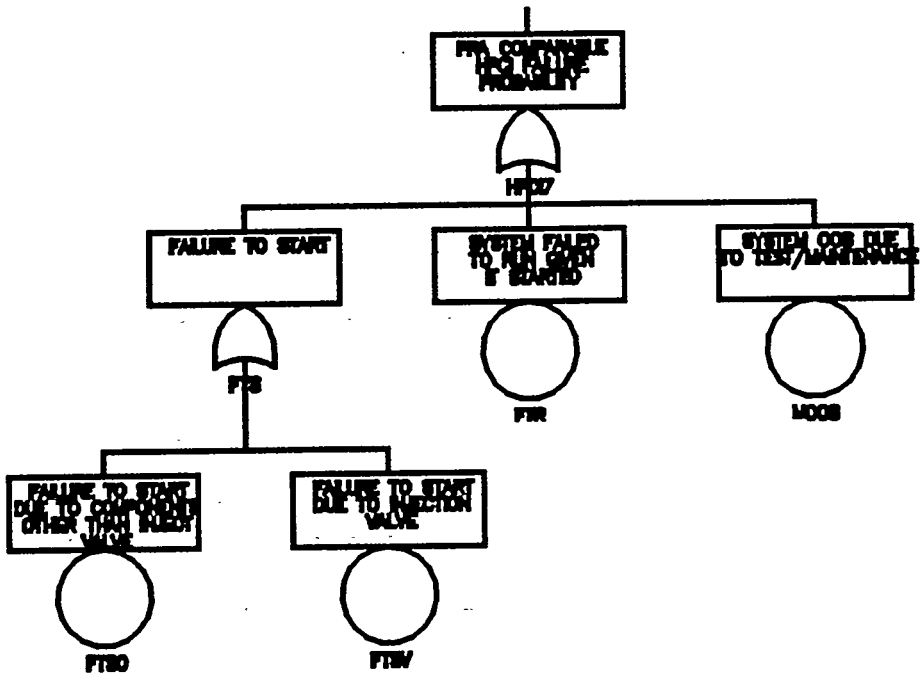


Figure 3. HPCI PRA comparison model (excludes recovery).

uncertainty were performed. The support systems were removed because no HPCI failures reported in the operational data resulted from support system failures, and the total contribution of support systems to the HPCI failure probability in the PRAs was typically less than five percent.

The failure probability and uncertainty intervals for the system and the basic events from the industry experience and the PRAs were compared on as consistent a basis as possible. However, one inconsistency remained that may cause the system failure probabilities based on industry experience to be lower than those predicted by the PRA modeling. In virtually all PRAs, the model of the HPCI system assumes the system is required to operate for a specific mission time, typically 10 to 24 hours. For this study, the FTR probability distribution was based on observed demands for which the mission times were significantly shorter than those assumed in the PRAs. Success or failure was simply based on whether or not the system ran for the mission time required by the observed demand.

3. HPCI ANALYSIS RESULTS

The study's findings, based on the methods described above, are now summarized.

3.1 Data Summary

Results of the trends and patterns analysis of the HPCI inoperabilities, failures and unplanned demands are displayed in Table 1 and Figures 4 and 5.

Table 1. Number of HPCI system inoperabilities failures and unplanned demands by year.

Classification	1987	1988	1989	1990	1991	1992	1993	Total
Inoperabilities	38	31	39	35	31	22	44	240
Failures	26	18	22	23	21	13	22	145
Unplanned demands	16	10	7	13	9	6	2	63
Unreliability	0.042	0.038	0.072	0.052	0.074	0.064	0.046	0.056
Operational years	15.0	14.3	15.9	18.29	17.8	17.6	17.9	116.6

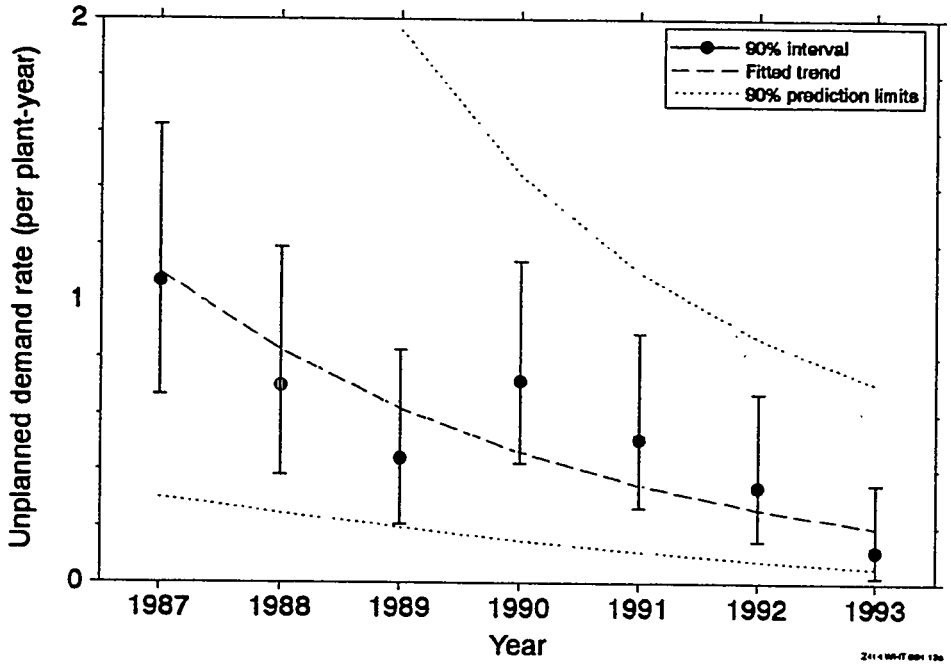


Figure 4. HPCI unplanned demands per plant operational year with 90% confidence intervals and fitted trend. The trend is statistically significant.

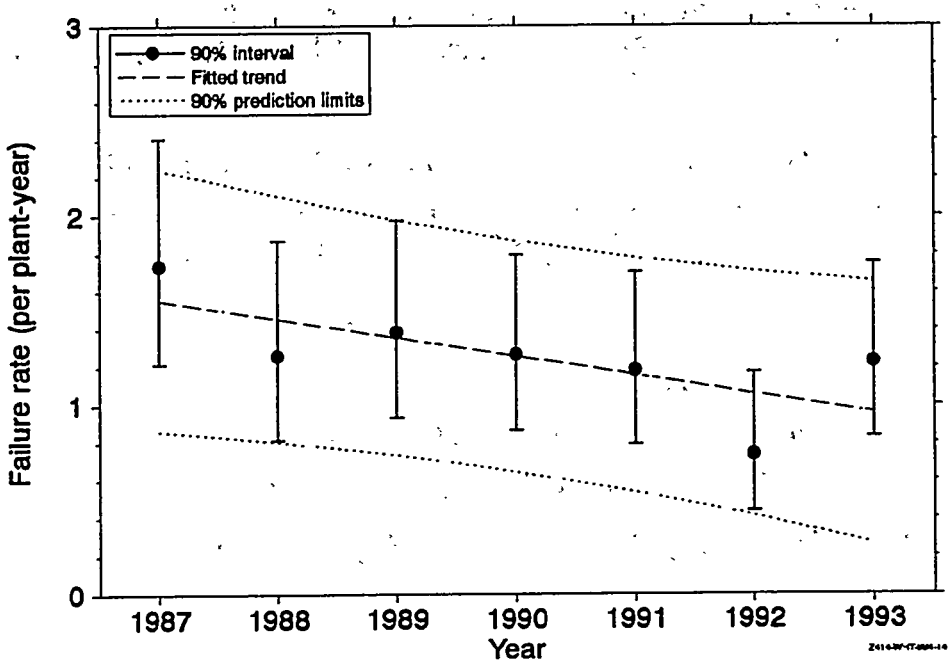


Figure 5. HPCI failures per plant operational year with 90% confidence intervals and fitted trend. The trend is almost statistically significant.

The analysis indicated that

- There was no observed trend in the overall number of LERs reporting HPCI system inoperabilities per year during the study period.
- The number of HPCI system unplanned demands per year has decreased during the study period and is statistically significant; the probability of seeing such a slope from chance alone is only 0.01. Figure 4 provides as illustration of the HPCI system unplanned demands per year.
- The number of HPCI system failures per year has decreased during the study period, and the trend (slope) is almost statistically significant; the probability of seeing as large a slope from chance alone is only 0.07. Figure 5 provides an illustration of the HPCI system failures per year.

3.2 Engineering Review

The engineering assessment of all the reported HPCI system active failures, i.e., failures observed during surveillance tests and during unplanned demands, indicate that the two significant failure modes, failure to run (FTR) and failure to start (FTS), differ in these two data sets. The

contributions of these failure modes are different because the mechanism of system failure varies based on how the system is operated. During surveillance tests, failures associated with the turbine and turbine control subsystem were observed most often. Failures in this subsystem were a significant contributor to both the FTS and FTR failure modes. Unplanned demand failures associated with the turbine and turbine control subsystem were also observed, but were only a significant contributor to the FTS failure mode. In aggregate, these factors tend to indicate that the stresses placed on the turbine from a cold quick start during surveillance testing closely mimic the stresses the turbine would encounter during an unplanned demand.

The FTR system failures that occurred in response to unplanned demands on the system were not typical of the failures observed during surveillance testing. These FTR events during an unplanned demand on the system were dominated by MOV problems, which were observed primarily with the injection MOV. These FTR events occurred when the system was used in the pressure control mode of operation, which differs considerably from the HPCI operations modeled in most probabilistic studies. Surveillance test failures of these MOVs were a small percentage of the overall test failures. However, the system is not tested for switching from the pressure control mode to the injection mode of operation. In addition to the injection MOV problems, governor problems also increased in relative contribution to the number of failures. This increase in the relative number of governor failures appears to be related to the length of time the system is operated. It appears that the length of time the system is operated in the pressure control mode of operation is longer than the time it is operating during surveillance testing. Therefore, the length of operation and mode switching of the system are not tested, and, therefore, the system is not stressed during surveillance tests to the extent in which it is operated during an unplanned demand.

3.3 Unreliability Evaluation

The analysis of continuous injection unreliability shows that, based on the industry experience over the seven year period from 1987 through 1993, there is approximately a 0.056 chance that the HPCI system will fail to inject coolant into the reactor vessel for the required mission time. Because operator recovery appears likely after failure to start but unlikely for problems that develop during injection, the failure to run has a bigger impact on this result than failure to start. An uncertainty interval that includes 90 percent of the simulated distribution for this unreliability is from 0.02 to 0.11. No aging or calendar year trends were found in the unreliability assessment. Figure 6 provides an illustration of the HPCI System Reliability by year. A trend line is fitted, but it is virtually constant.

Two important uncertainties exist for these data beyond the sources of variation that were modeled. While the statistical analysis dealt with the variations that could be observed in sampling and between such groupings as plant units, such an analysis cannot provide a basis for assessing the impact of the following:

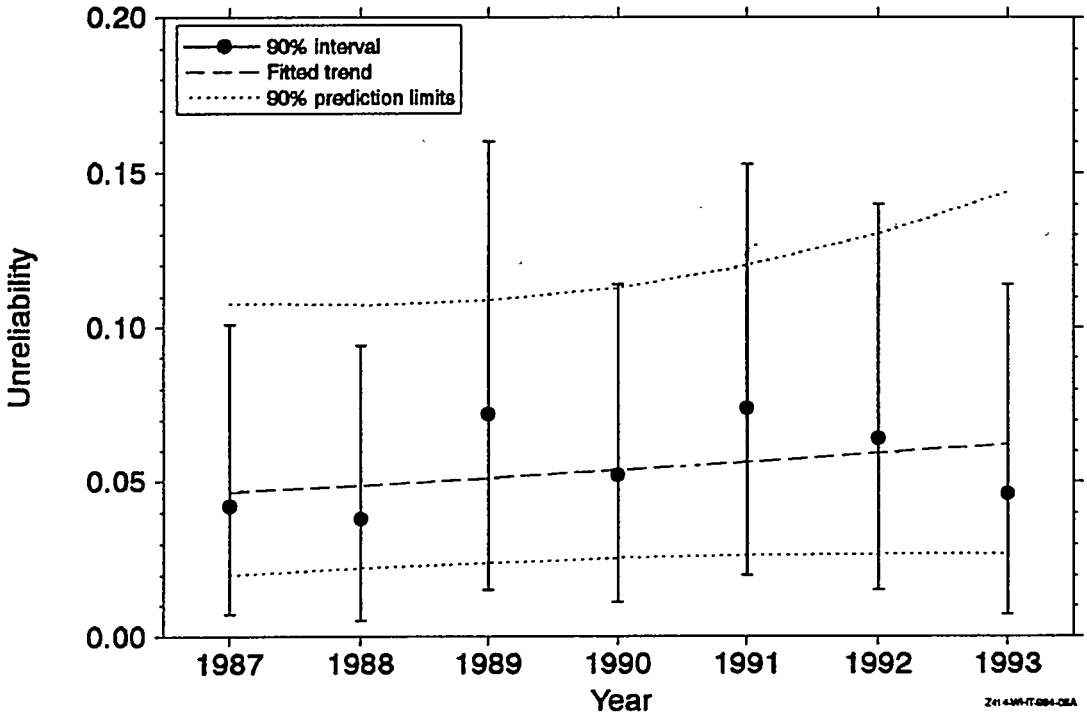


Figure 6. Unreliability by year, based on diffuse prior distributions and annual data. The plotted trend is not statistically significant.

- Whether the HPCI system will run for 24 hours, as is typically modeled in PRAs. The run times observed in the operational data and taken as successes were typically five minutes or less.

- Whether the HPCI system will function after it has been deliberately isolated by plant operators. The HPCI system has been observed to fail to inject coolant when required after it has been shifted from the RPV injection mode of operation into a recirculation mode. This study did not quantify the probability of this failure since precise data on the frequency of this operational shift and subsequent need for injection were not available.

3.4 PRA Comparison Conclusions

The HPCI system failure probabilities predicted by the Peach Bottom[3] and Brunswick Units[4] 1 and 2 PRAs are basically consistent with the HPCI system failure probability based on industry experience over the seven years from 1987 through 1993. Table 2 provides the HPCI failure probabilities from the selected PRAs and industry experience. Figure 7 illustrates these probabilities. This consistency is supported by the agreement of the failure probabilities of the principal contributors to the system failure probability from the PRAs and industry experience. Industry experience thus confirms the

Table 2. Comparison of HPCI failure probability from selected PRAs and industry experience.

PRA	HPCI failure probability		Dominant contributor	Dominant contributor probability
	Original PRA	Without support system failures[a]		
Peach Bottom	9.9E-2	9.5E-2 (2.1E-2, 2.7E-1)	TDP-FTR[b] TDP-FTS[c]	5.0E-2 3.0E-2
Brunswick 1	1.9E-1	1.8E-1 (5.3E-2, 4.5E-1)	TDP-FTS TDP-TM[d]	1.2E-1 5.9E-2
Brunswick 2	1.5E-1	1.4E-1 (4.2E-2, 3.4E-1)	TDP-FTS TDP-TM	9.0E-2 4.3E-2
Industry-Wide Experience	–	1.4E-1 (5.8E-2, 3.1E-1)	FTSO[e] FTR[e]	6.0E-2 4.2E-2

a. Uncertainty interval values in parentheses are lower bound, upper bound.

b. TDP-FTR = Turbine-driven pump fails to run.

c. TDP-FTS = Turbine-driven pump fails to start.

d. TDP-TM = Turbine-driven pump unavailable due to testing or maintenance.

e. FTSO and FTR do not necessarily refer to the turbine driven pump but rather to the start or run phase of the operations.

HPCI system failure contribution to the core damage frequency prediction in the PRAs.

The agreement of the HPCI system failure probabilities (plant-specific and industry-wide) based on industry experience with the plant PRA results indicates that the industry experience represents a level of risk that is not significantly higher than previously predicted.

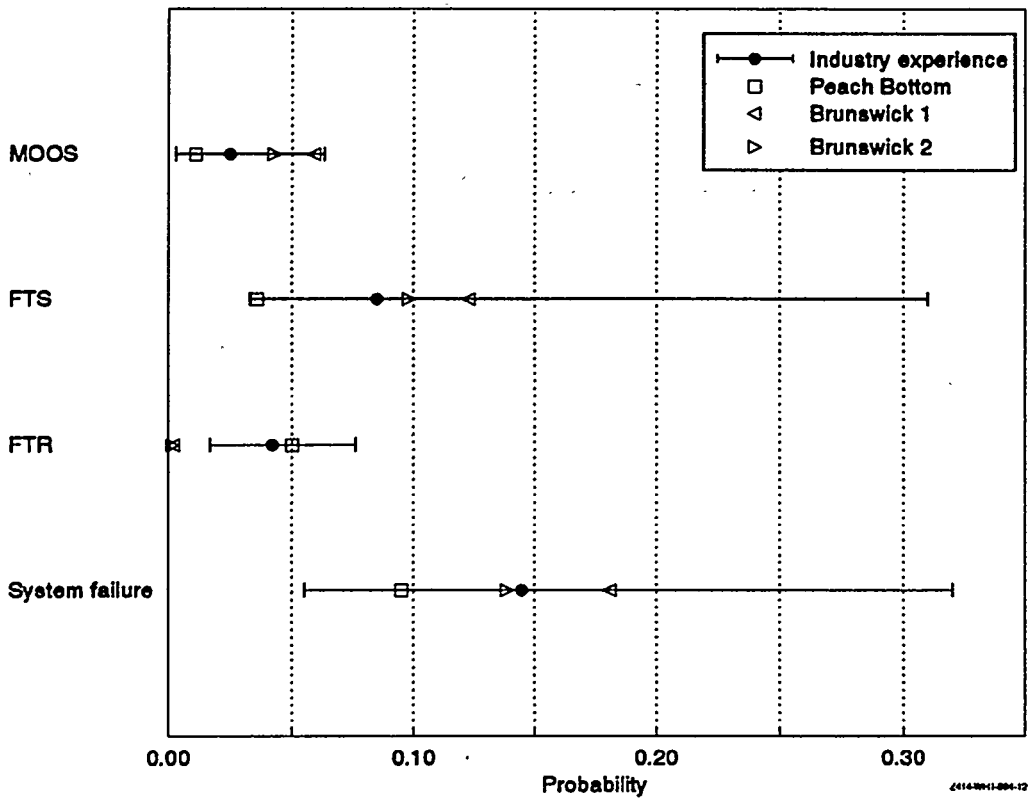


Figure 7. Comparison of principle contributors to HPCI system failure modes.

ACKNOWLEDGMENTS

Douglas G. Hall, John B. Hudson, and Martin B. Sattison contributed significantly to portions of this work.

NOTICE

4. REFERENCES

1. G. M. Grant et al., High Pressure Coolant Injection System Performance, 1987–1993 (Draft). EGG-10929, September 1994.

2. K. D. Russell et al., SAPHIRE Technical Reference Manual: IRRAS/SARA Version 4.0, NUREG/CR-5964, January 1993.

3. A. M. Kolaczkowski et al., Analysis of Core Damage Frequency: Peach Bottom Unit 2, NUREG/CR-4550, Vol. 4, Rev. 1, August 1989.

4. Carolina Power & Light Company, Brunswick Steam Electric Plant Probabilistic Risk Assessment, April 1988.

SAPHIRE Models and Software for ASP Evaluations*

Martin B. Sattison**
John A. Schroeder**
Kenneth D. Russell**
Steven M. Long***
Dale M. Rasmuson***
Richard C. Robinson***

**Idaho National Engineering Laboratory
Lockheed Idaho Technologies Company
Idaho Falls, Idaho 83415

***United States Nuclear Regulatory Commission

ABSTRACT

The Idaho National Engineering Laboratory (INEL) over the past year has created 75 plant-specific Accident Sequence Precursor (ASP) models using the SAPHIRE suite of PRA codes. Along with the new models, the INEL has also developed a new module for SAPHIRE which is tailored specifically to the unique needs of conditional core damage probability (CCDP) evaluations. These models and software will be the next generation of risk tools for the evaluation of accident precursors by both NRR and AEOD. This paper presents an overview of the models and software. Key characteristics include: (1) classification of the plant models according to plant response with a unique set of event trees for each plant class, (2) plant-specific fault trees using supercomponents, (3) generation and retention of all system and sequence cutsets, (4) full flexibility in modifying logic, regenerating cutsets, and requantifying results, and (5) user interface for streamlined evaluation of ASP events.

*Work supported by the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, under Department of Energy Contract No. DE-AC07-76ID01570.

1. INTRODUCTION

In the spring of 1993, the Office of Nuclear Reactor Regulation (NRR) contracted the Idaho National Engineering Laboratory (INEL) to develop (1) a set of SAPHIRE[1] risk models covering all operating commercial nuclear power plants for use in the Accident Sequence Precursor (ASP) program, and (2) a user interface specifically designed for event evaluations. The plant models were to be based on work previously performed by Science Applications International Corporation (SAIC) under subcontract to the Oakridge National Laboratory. SAIC's work produced a document entitled, "Daily Events Evaluation Manual."[2]

The Daily Events Evaluation Manual (DEEM) identified three classes of boiling water reactors (BWRs) and six classes of pressurized water reactors (PWRs) based on similar plant responses to transients and accidents and the systems designed to perform those responses. For example, BWR Class A contains all the older BWRs with isolation condensers and feedwater coolant injection systems. The DEEM contained event tree models for each plant class and provided plant-specific system models for twelve different nuclear power plants (with at least one representative from each plant class).

The project at the INEL was tasked with constructing these models using SAPHIRE 4.16 and then proceding on to develop 63 other models to cover all the operating commercial nuclear power plants in the United States. The work was actually accomplished in phases. The first phase was to develop a working model for a single plant, Byron. Once this model was developed and the valuable lessons learned were understood, the next phase was started: development of a lead plant model for each of the remaining plant classes. After that, the remaining plant models were created based on the lead plant models. The final phase of the initial project was to gain experience and insights using the models on event evaluations and then develop a user-friendly interface specifically designed to streamline the analysis and reporting processes.

The Byron plant model was created over a period of about three months. The lead plant models for the other plant classes each took about three weeks to complete, and the remaining 66 models averaged about a week to produce. The last plant model was delivered to the NRC at the end of June 1994.

2. THE MODEL STRUCTURE

2.1 Event Tree Models

Each BWR plant model database contains event trees for three initiating events: transients, loss of offsite power (LOOP), and small loss of coolant accidents (LOCA). The transient event tree has a transfer to an Anticipated Transient Without Scram (ATWS) event tree. The other event trees do not develop the ATWS sequences, but just assume core damage.

PWRs model the same initiating events as BWRs plus an additional event tree is developed for steam generator tube ruptures. Again, only the transient event tree transfers to the ATWS event tree. Figure 1 is the transient event tree for Millstone 2, a typical PWR model.

The event trees are of a size and complexity somewhat smaller and simpler than the typical NUREG-1150 Level I internal events PRA. There are several areas in the event trees where credit was not given to third tier backup systems or extraordinary human recovery actions and core damage was assumed for the sake of keeping the models as managable as possible. These areas may be expanded in the future should the affected sequences become important. The typical BWR model contains about 100 - 120 core damage sequences and the typical PWR model has about 50 - 75.

2.2 Fault Tree Models

For every event tree top event a fault tree model was developed. Because of changing success criteria or impacts due to previous failures in the accident sequences, additional fault trees had to be created as well. Thus, there are anywhere from 35 to 45 fault trees in each plant model. Each fault tree has been kept small enough to be printed out on a single page with only a few exceptions such as high pressure recirculation (HPR) and feed and bleed cooling (F&B). Figure 2 shows a typical fault tree. The fault trees contain much of the detail of the more complex models of a typical PRA by combining serial components and their failure modes into a single supercomponent basic event. For example, a typical high pressure injection (HPI) pump train basic event may consist of the following:

Table 1. Example HPI Pump Train Supercomponent Basic Event.

BASIC EVENT	COMPONENT DATA			BASIC EVENT PROB
	COMPONENT NAME	FAILURE MODE	FAILURE PROB	
HPI-MDP-FC-1A	HPI MDP 1A	Fails to start/run	3.7E-3	3.9E-3
	Discharge check valve	Fails to open/plugs	1.0E-4	
	Suction MOV	Fails to remain open	4.0E-5	
	Discharge MOV	Fails to remain open	4.0E-5	

This supercomponent contains four different components and six different failure modes. The general principle for combining components and failure modes into a supercomponent is the requirement that each of the components and associated failure modes must impact the overall system and accident sequence performance in the same manner. Thus in the example above, it doesn't matter whether the discharge check valve fails to open or the suction motor-operated valve inadvertently transfers closed, both lead to failure of flow through a given pipe segment of the HPI system. This basic event may be used in several different fault trees such as HPI, F&B, and HPR. In fact, proper modeling requires that the same components and failure modes be called the same basic event name throughout the entire model regardless of where they appear. It is imperative that the supercomponent basic events be defined such that the same components

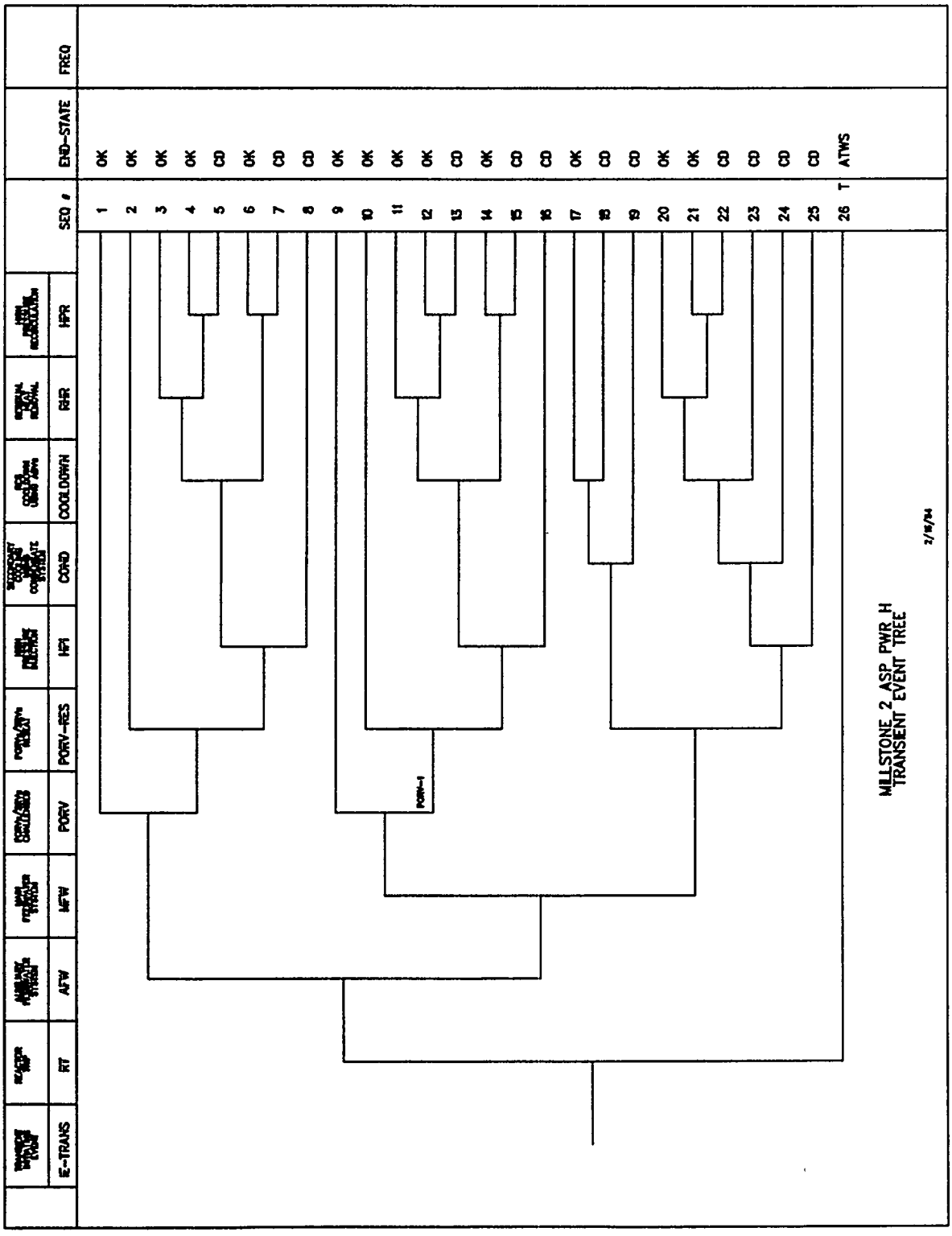


Figure 1. Millstone 2 transient event tree.

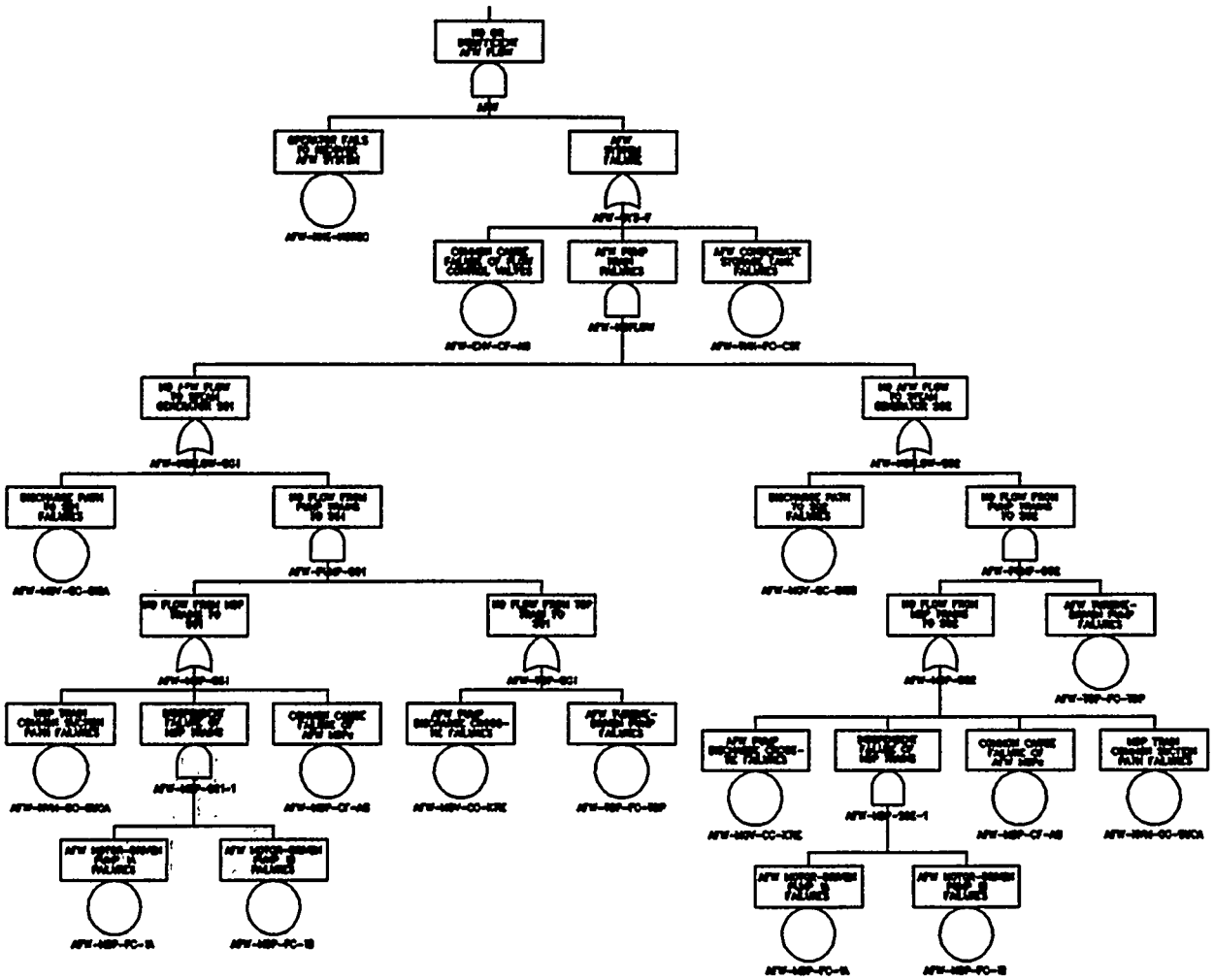


Figure 2. Millstone 2 Auxiliary Feedwater System fault tree.

and failure modes are included in one and only one basic event. This allows the PRA software the ability to properly perform Boolean reduction including the delete term process of eliminating impossible combinations of failures and successes. By using this method, the number of basic events per plant model has been held down to 90 to 120.

The system fault tree models include the following features:

- Human actions to actuate a system when no automatic actuation is expected.
- Recovery actions to restore a system to operability given a system failure.
- Common cause failure of a sufficient number of redundent components to render the system inoperable.
- Simplified dependencies on emergency AC power for fault trees used in the LOOP event tree.

Specifically excluded from the fault tree models are contributions to front-line system failures due to support system failures (except for emergency power in LOOP situations). Support system models were not developed for several reasons: (1) the models would quickly become very large and not easily manipulated, (2) the current policy is to explicitly model the impacts of any support system failures, and (3) the availability of sufficient information to accurately model support systems is limited without putting forth an effort larger than could be afforded by this project.

2.3 Basic Event Data

The basic event failure probabilities were calculated based on the individual components, failure modes, and mission times involved in each basic event.

The supercomponent basic event failure probabilities were calculated by hand and loaded into the SAPHIRE database. For example, the failure probability for the HPI motor-driven pump train shown in Table 1 is calculated as follows:

ASEP Data:

Motor-driven pump fails to start	3.0E-3/d
Motor-driven pump fails to run	3.0E-5/h
Check valve fails to open/plugs	1.0E-4/d
Motor-operated valve fails to remain open	4.0E-5/d

mission time = 24 hours

Failure probability of HPI MDP 1A = P(fts) + P(ftr)
= 3.0E-3 + (3.0E-5/h)(24h)
= 3.72E-3

Failure probability of discharge check valve = 1.0E-4

Failure probability of suction MOV = 4.0E-5

Failure probability of discharge MOV = 4.0E-5

Total failure probability of HPI-MDP-FC-1A = 3.9E-3

2.3.1 Independent Hardware Failures

The raw data for failures on demand and failure rates (per hour) were obtained from one or more of the following sources:

- The Accident Sequence Evaluation Program (ASEP) database as reported in EG&G Idaho report EGG-SSRE-8875, "Generic Component Failure Data Base for Light Water and Liquid Sodium Reactor PRAs."[3]
- The Daily Events Evaluation Manual (DEEM).
- An NRC-supplied plant-specific full-scope PRA or Individual Plant Examination (IPE).

The ASEP database was the default source whenever a better data source was not available. The DEEM was used for many of the initiating event frequencies. The initiating event frequencies were developed from Final Safety Analysis Reports (FSARs), NUREG-1032,[4] and NUREG-1150.[5]

2.3.2. Common Cause Failures

Common cause failure basic events were quantified using the Multiple Greek Letter method and generic values from NUREG/CR-5801[6] unless there was more specific data available from a PRA or IPE. Common cause failure analysis methodology is one of the topics for further evaluation in an AEOD follow-on project, ASP Methods Improvements, JC E8257.

2.3.3 Human Errors and Recovery Actions

The human error probabilities from the DEEM were used as screening values for these ASP models. These probabilities are based on observations from actual operational events reported in the Licensee Event Reports (LERs) and analyzed by the ASP program.

3. MODEL QUANTIFICATION

The ASP models were processed by SAPHIRE 4.16 to generate all possible system and accident sequence minimal cutsets. This was done by turning off all truncations. Due to cutset storage limitations in SAPHIRE 4.16, there were a handful of accident sequences in most plant databases that were automatically truncated after generating several thousand minimal cutsets. Thus, all

possible minimal cutsets were generated and quantified for all systems and over 90 percent of the accident sequences. The remaining accident sequences retained and quantified several thousand minimal cutsets each. Most plant models contain 20,000 to 150,000 accident sequence cutsets.

In this fiscal year, the models will be converted to SAPHIRE 5.0 and will be available for use with a special event assessment module designed specifically to aid the analyst in ASP-type evaluations. The increased capabilities of the software will allow rapid regeneration of accident sequence cutsets to whatever truncation requirements desired.

The accident sequences were quantified using initiating event frequencies on a per hour basis. Once again, this is to facilitate the analysis of operational events. Operational events fall into two categories: (1) those that involve an initiating event, and (2) those that involve some potentially important reduction in safety system reliability or functionality without causing an initiating event (these events are called "conditions"). For condition events, the initiating event frequencies are multiplied by the number of hours the condition was known to exist as an approximation for the probability of occurrence of each initiating event during the condition, thus creating a conditional core damage probability for each accident sequence in each event tree. Thus, it is more convenient for the initiating event frequencies to be expressed on a per hour basis.

All quantifications were performed as point estimates. The databases do not contain any uncertainty information at this time. AEOD is currently sponsoring a project investigating many potential improvements to the ASP models and uncertainty is one of the major areas being addressed.

4. THE EVENT ASSESSMENT MODULE OF SAPHIRE

Just as there are some unique features required of the PRA models, the evaluation of operational events also requires some unique features of the software. The SAPHIRE PRA software has been extended with some of these features in an event assessment module. This module was specifically designed to allow the analyst to easily perform the types of analyses encountered in the ASP methodology.

To understand the requirements and features of the software, one must first have a basic understanding of the ASP methodology. As explained above, operational events fall into two categories: initiating events and conditions.

For initiating events, the analyst must determine what the initiating event is and adjust the model initiating event frequencies and related basic events accordingly. The initiating event of concern is set to its short-term recovery value and all other initiating events are set to FALSE. For a LOOP, the short-term and long-term recovery values and the probability of a seal LOCA before emergency power recovery are all dependent on the type of LOOP; grid-centered, plant-centered, severe weather, or extermely severe weather. Additionally, any equipment failures or unavailabilities must be modeled by adjusting the appropriate basic event values. The accident sequences associated with the initiating event are then requantified and summed and the result is the conditional core damage probability (CCDP).

For conditions, all initiating event frequencies are multiplied by the duration of the operational condition obtain the initiating event probabilities during the duration of the condition. All the accident sequences in the model are requantified with these initiating event probabilities. This establishes the base case conditional core damage probability associated with operating the plant for the time of concern. Next, the analyst adjusts the basic event probabilities to reflect the status of plant equipment during the condition. The entire model is requantified and the difference between the base case and the condition case is the CCDP.

The event assessment module automates as much of this process as possible. The first thing asked of the analyst is whether the event being analyzed is an initiating event or a condition. If it is an initiating event, the analyst is asked to indicate which one it is. Once that is established, the software sets all other initiating event frequencies to FALSE and the initiating event of concern to its short-term recovery value if there is one, otherwise it is set to 1.0. If the initiating event is one of the types of LOOP, the software also adjusts the various recovery values and the seal LOCA probability. The analyst is next asked to input any changes to the basic event probabilities to reflect any equipment failures or unavailabilities. Once that is done the model is requantified and the results are displayed.

If the analyst indicated that the event being evaluated was a condition, the user is asked how long the condition existed and to input any basic event probability changes to reflect equipment failures or unavailabilities. The model is then requantified and the results show the base case risk, the risk associated with the condition and the resulting CCDP.

With the current event assessment module, the ASP model databases must already be loaded with the various recovery values and seal LOCA probabilities before any analyses can be performed. Work for this fiscal year will allow the software to calculate the various recovery values based on the models currently contained in the STATION BLACKOUT[7] code.

5. REFERENCES

1. K. D. Russell, et al, SAPHIRE Technical Reference Manual: IRRAS/SARA 4.0, NUREG/CR-5964, December 1992.

2. Science Applications International Corporation, Daily Events Evaluation Manual (Draft Report), 1-275-03-336-01, January 31, 1992.

3. S. A. Eide, et al, Generic Component Failure Data Base for Light Water and Liquid Sodium Reactor PRAs, EGG-SSRE-8875, February 1990.

4. P. W. Baranowsky, Evaluation of Station Blackout Accidents at Nuclear Power Plants, NUREG-1032, June 1988.

5. U.S. Nuclear Regulatory Commission, Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, NUREG-1150, December 1990.

6. A. Mosleh, Procedure for Analysis of Common-Cause Failures in Probabilitistic Safety Analysis, NUREG/CR-5801, April 1993.

7. J. W. Minarick, Revised LOOP Recovery and PWR Seal LOCA Models, ORNL/NRC/LTR-89/11, August 1989.

Methods Improvements Incorporated into the SAPHIRE ASP Models*

Martin B. Sattison**
Dale M. Rasmuson***
Harold S. Blackman**
Steven D. Novack**
Curtis L. Smith**

**Idaho National Engineering Laboratory
Lockheed Idaho Technologies Company
Idaho Falls, Idaho 83415

***United States Nuclear Regulatory Commission

ABSTRACT

The Office for Analysis and Evaluation of Operational Data (AEOD) has sought the assistance of the Idaho National Engineering Laboratory (INEL) to make some significant enhancements to the SAPHIRE-based Accident Sequence Precursor (ASP) models recently developed by the INEL. The challenge of this project is to provide the features of a full-scale PRA within the framework of the simplified ASP models. Some of these features include: (1) uncertainty analysis addressing the standard PRA uncertainties and the uncertainties unique to the ASP models and methods, (2) incorporation and proper quantification of individual human actions and the interaction among human actions, (3) enhanced treatment of common cause failures, and (4) extension of the ASP models to more closely mimic full-scale PRAs (inclusion of more initiators, explicitly modeling support system failures, etc.). This paper provides an overview of the methods being used to make the above improvements.

1. INTRODUCTION

The first set of seventy-five Accident Sequence Precursor (ASP) models developed for use with the SAPHIRE[1] suite of PRA computer codes were based on work previously performed by Science Applications International Corporation (SAIC) under subcontract to the Oakridge National Laboratory. SAIC's work produced a document entitled, "Daily Events Evaluation Manual."[2]

*Work supported by the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, under Department of Energy Contract No. DE-AC07-76ID01570.

These models were improvements over the ASP models used in the past in several areas, including: 1) development of Anticipated Transient Without Scram (ATWS) sequences for transients, 2) credit for centrifugal charging pumps, and 3) credit for BWR containment venting. Just the fact that the models were based on the linked fault tree/event tree methods and could be modified such that new minimal cutsets could be generated and quantified was a major step forward for the ASP program. The first set of SAPHIRE-based ASP models were intentionally kept simple and did not incorporate a number of features and capabilities known to be desirable.

After the initial set of ASP models were delivered to the Office of Nuclear Regulatory Regulation (NRR) as part of JC J2033, the Trends and Patterns Branch of the Office for the Analysis and Evaluation of Operational Data (AEOD) contracted the Idaho National Engineering Laboratory (INEL) to develop a plan to upgrade the ASP models. This plan was accepted and the ASP Methods Improvements project, JC E8257, was started. The project work scope includes establishing modeling requirements in the following areas:

- Uncertainty Analysis
- Human Reliability Analysis
- Common Cause Failure Analysis
- Modeling level of detail and scope

Each improvement will be demonstrated on several plant models selected from a set of prototype models consisting of Byron, St. Lucie, Peach Bottom, Oconee, and Three Mile Island.

2. UNCERTAINTY ANALYSIS CAPABILITY

The ASP models have never had the ability to give an uncertainty estimation. It was well-known that a basic parameter uncertainty estimation capability comparable to that of a typical full-scope PRA was necessary and practical. The INEL was also tasked with investigating how to estimate the unique modeling uncertainty associated with simplified ASP models.

2.1 Parameter Uncertainty

The SAPHIRE-based ASP models use conventional event trees to model the plant response to initiating events in the manner of the small event tree/large fault tree PRA method. However, the fault trees are simplified by modeling pump trains and pipe segments with supercomponent basic events. Each supercomponent basic event represents a number of components and failure modes typically modeled by separate basic events in a conventional PRA. The use of supercomponents prevents modeling parameter uncertainty in the standard fashion.

The tasks for incorporating parameter uncertainty to the ASP models include:

- Developing the uncertainty parameters for the supercomponent events in an ASP database.
- Verifying the validity of assuming that supercomponent events are lognormally distributed.
- Investigating uncertainty issues relevant to Monte Carlo and Latin Hypercube sampling.
- Evaluating the potential benefit of using transfers to "mini" fault trees rather than "rolled-up" supercomponent events.
- Comparing event assessment uncertainty results between ASP models and full-scope, detailed PRA models.

2.1.1 Supercomponent Basic Event Evaluation

The supercomponent basic events were individually modeled by small fault trees explicitly showing each component and failure mode. The basic events in these "mini" fault trees were assigned uncertainty distributions in SAPHIRE 5.0. If the supercomponent contained two or more components of the same type (e.g., two check valves), the components' failure data were correlated. The supercomponent fault trees were then solved to determine their uncertainty parameters.

Once all the supercomponent fault trees were evaluated, the error factor for each supercomponent was calculated. These error factors and means are used in the lognormal distributions assigned to the supercomponent basic events in the ASP models.

2.1.2 Comparisons of Uncertainty Distributions

Lognormal, beta, and gamma distributions were compared to determine which distribution should be used for the ASP model basic events. Five supercomponent basic events were used for this comparison. The five supercomponents were converted into "mini" fault trees. The mean and error factor for each individual component were put into the SAPHIRE database and identical components were correlated. The fault trees were then analyzed.

The mean and standard deviation calculated for each supercomponent were used to determine the uncertainty parameters for each of the three distributions. The uncertainty parameters that were determined were the error factor for a lognormal distribution, the b parameter for a beta distribution, and the r parameter for a gamma distribution as defined for input to the SAPHIRE software. Once the uncertainty parameters were determined, they were applied to a single basic event. The single basic event was evaluated using Monte Carlo sampling. The resulting quantiles of the lognormal, beta and gamma distributions for each supercomponent were compared to the original supercomponent quantiles. Also, a Kolmogorov-Smirnov (K-S) test was performed to determine which distributions should be rejected from further consideration when performing parameter uncertainty analysis. The result plots and the K-S test demonstrated that the lognormal distribution plots tended to fit the original supercomponent plots the closest.

2.1.3 Uncertainty Sampling Issues

A comparison of Monte Carlo and Latin Hypercube sampling was performed to determine which type of sampling should be used for parameter uncertainty. To perform this comparison, two supercomponents and two ASP plant models were used. For each comparison, the mean, standard deviation, 5th percentile, and 95th percentile were plotted against the number of samples used for both Monte Carlo and Latin Hypercube sampling. The analysis showed that the mean and percentiles converged with sample sizes greater than 3,000 for Latin Hypercube sampling and 5,000 for Monte Carlo sampling. Why it took this many samples is still under investigation.

2.1.4 Comparisons of ASP Uncertainty Modeling Methods

Four modeling methods were compared to determine which method should be used for ASP parameter uncertainty. The four methods were:

1. Treat the supercomponents as single basic events using the calculated means and error factors (no correlation).

2. Correlate the basic events and supercomponents in conjunction with 1. above.

3. Transfer from the ASP fault tree into the supercomponent "mini" fault trees (no correlation).

4. Transfer from the ASP fault tree into the supercomponent "mini" fault trees with all individual components and human actions correlated.

The four methods were applied to the Byron and Oconee ASP databases. For each method, a system and sequence cut set generation was performed on the ASP databases. Also, for each method, an uncertainty analysis was performed on each ASP models' systems, sequences, and family results. The results for the four methods were fairly consistent. The correlated, not transferred method (method 2 above) resulted in the largest mean for the family compared to the other three cases. The results for this method also showed the mean for the systems and sequences to be consistently larger (or close to the largest) than the other mean values.

2.1.5 Event Analysis Comparison between ASP and Full PRA Models

Five different evaluations were used to compare the ASP models against their respective full-scope PRA models. The ASP models used in the comparison contained their supercomponents as single basic events (i.e., not transferred) with all the basic events correlated. The two ASP and PRA models used in the comparison were San Onofre and Peach Bottom. The five comparisons of the two models were:

- The complete full-scope PRA model results compared to the ASP model results.

- The PRA model using the same Initiating Events (IE) as the ASP model.

- The safety injection pump train failed in both the PRA and ASP model.
- Steam generator tube rupture IE set to TRUE and the others set to FALSE for both models (San Onofre only).
- The LOOP IE set to TRUE and the others set to FALSE, with one diesel generator failed, for both models.

In general, the ASP models' mean and minimal cutset upper bound estimate for each comparison were up to three times larger than the full-scope PRA models. This can be attributed to the simplification of the models and the use of generic data compared to plant-specific data. The ASP models also had wider uncertainty distributions associated compared to the PRA models.

2.2 Model Uncertainty

Preliminary work related to the evaluation of model uncertainty for the ASP models has been performed. Measuring the ability of the ASP models to accurately predict the conditional core damage probability (CCDP) requires that the "true" value of the CCDP be known. Since enough data may be difficult (if not impossible) to obtain to adequately estimate the "true" CCDP, several potential measurable estimates related to the CCDP estimate are being investigated.

Additional work will attempt to define and measure the ASP model uncertainty importance. For the proposed estimates of the "true" CCDP, additional work will be performed to 1) investigate what has been done previously in the area, 2) provide details on how the "true" CCDP estimate will be used to measure model uncertainty, and 3) determine the benefits and limitations of the estimate.

During the model uncertainty work, the "true" CCDP will be estimated using one or more proposed estimation methods. While the measurement of the model uncertainty will focus on the ASP model's prediction of the CCDP estimate (i.e., how well the ASP CCDP compares to a detailed, full-scope Level 1 PRA core damage frequency), the causes for the uncertainty will also be investigated. For those analysis cases where the ASP model exhibits measurable model uncertainty, the model will be scrutinized to determine the cause of the model uncertainty. It is believed that, by evaluating various ASP models for diverse types of events, the high-importance model uncertainty types will be revealed along with their potential impact on the overall model uncertainty.

3. HUMAN RELIABILITY ANALYSIS

The purpose of this task was to make improvements in the current practice for human reliability analysis (HRA) for the ASP program. Specific areas needing attention were the treatment of recovery errors and the assessment of dependency. The goal was to develop a general, easy-to-apply, method which handled actuation, recovery, and dependency through a consistent model of human behavior.

3.1 Method Description

A general criticism of HRA methods is the inability to tie these methods back to first principles in human behavior. Generally HRA methods identify a set of factors believed to be related to performance (e.g. stress, training, procedure quality), or focus on classes of human error (omission, commission, mistakes, slips) or even general classifications of human behavior (rule, skill, knowledge) and then manipulate those factors to arrive at a failure rate. The obvious problem with these approaches is completeness. How does one know that the set of identified factors is, in fact, complete? To our knowledge, no single model begins with a theory of human behavior, to ensure that all relevant factors are addressed and accounted for, and works forward to identify demonstrated, underlying mechanisms that we know influence and are predictive of behavior. To avoid this basic flaw in method development, some time was spent identifying an underlying model of human behavior from which a clearly supportable and complete method for ASP could be developed.

3.1.1 Model of Human Performance

The model of human behavior selected was developed out of some early work in cognitive science principles and is generally termed an information processing approach to human behavior. Table 1 illustrates the model and its basic elements. The factors that comprise the basic elements of this model come from the literature surrounding the development and testing of general information processing models of human performance. The result, from a psychological viewpoint, is a comprehensive list of factors that influence human performance.

3.1.2 Operational Factors

For the purposes of ASP, the psychological elements were developed into the practical and operational factors more commonly identified in nuclear power plant operation. These factors were listed under the general categories of the model of human performance where they come into play. The operational factors are given in Table 2. These operational factors, readily identifiable in NPPs, can be directly associated with basic elements in a generally accepted model of human performance. These factors can then be applied to tasks and potential errors which primarily rely on one portion of the model. This approach (1) clearly establishes why these operational factors are considered and what portion of human information processing model they are associated with, (2) gives assurance of completeness of the factors considered, and (3) provides a firm basis for how the factors impact performance.

Table 1. Human Behavior Model

Opportunity Time Goals Beliefs Organization of the perceptual field Learning Training Demand of the task Physical and mental health Crew Cognitive skills Complexity of the task environment ⬇					
Inflow of Information ➡	Filters ➡	Perception ⬌	Working Memory/ Short Term Memory ⬌	External Memory ⬌	Processing and Long Term Memory
Visual - graphic Verbal Written - Semantic	Management and administrative environment	Vision Auditory Tactile Sensory Store (<STM)	Attention Capacity Time constraint Serial processing	Environmental cues Job aids Procedures	Associatively organized Scripts Schema Selective recall Hierarchy-based Existing heuristics Development of new/ alternative strategies
⬇					
Response: Implementation of decisions made Physical strength Sensory acuity Practice/skill Time to react/time available Existing models for behavior					

Table 2. Operational Factors

Inflow and Perception	WM/STS	Processing and LTM	Response
Presence[1,5] (is the necessary signal there at all) Human sensory limits[4] Medium[1,4,5] (verbal, graphic, text) Interference[1,4] (signal/noise) Ergonomics[1] of presentation (strength, degree of clarity, degree of redundancy, appropriate grouping, appropriate coding) • organization of the perceptual field • complexity Environmental degradation[2] • complexity Physical and mental health[6]	Limited capacity[4] • serial processing Only good for a short time (20 sec)[2,4] Right amount of attention required[2,4] • rehearsal[2,4] • physical and mental health[6]	Training[3] (models, problem-solving, behaviors) • learning Experience[3] (models, problem-solving, behaviors) • learning Culture[5] (societal, organizational, interpersonal (crew)) • learning Intelligence/cognitive skills[5] (decision-making, problem-solving) Interference factors[1,2,5] (distraction) Available time[2] Physical and mental health[6]	Training[3] (actions) • existing models of behavior • practice and skill Experience[3] (actions) • existing models of behavior • practice and skill Proper control available[1] Human action limits[6] (physical strength and sensory acuity) Ergonomics of controls[1] • complexity Environmental degradation[2] Time to react vs. time available[2]

SUMMARY LEVEL FACTORS

1. Ergonomics
2. Complexity, stress, and workloads (including time)
3. Experience/Training
4. Procedures (job aids)
5. Crew dynamics
6. Fitness for duty

The operational factors were associated with six summary level factors, listed at the bottom of Table 2. These are:

- complexity, stress, and workload (including time)
- experience/training
- procedures (job aids)
- ergonomics
- fitness for duty
- crew dynamics

Definitions of these factors follow:

- Complexity, stress and workload (including time)

This factor considers the influence of the threat, stress, and relative adequacy of the time. Stress refers to the level of undesirable conditions and circumstances that impede the operator from easily completing a task. Stress can include mental stress, environmental stress (such as heat, noise), and excessive workload. Threat, in the context of stress, refers to the situation where the operator feels physically threatened or feels that others at the plant or loved ones may be physically threatened by the circumstances at hand. A common contributor to stress is fatigue. Several event investigations have shown that stress was related to fatigue or duty hours. These events commonly occur during the early morning hours of 3 am to 5 am, at the end of a graveyard shift, sometimes on the last night of a 5-day rotation. It has also been observed that when equipment fails, such as safety relief valves (SRVs), that high levels of stress are created. Time refers to the ratio of time available to complete a task to the time required to complete a task. If the ratio is less than 1 then time is inadequate, if the ratio is between 1 and 1.5 it is adequate, and if it is greater than 1.5 it is expansive. Operators will perceive more stress if the time available to perform the task is short.

- Experience/training

This factor considers the experience and training of the individual(s) who are performing the task. Experience refers to the experience of the operators involved in the task. Included in this consideration are years of experience of the crew or individual, and whether or not the scenario is novel or unique. Training refers to whether or not the operator/crew has been trained on the type of accident, and on the systems involved in the task and scenario. Specific examples where training has been found deficient are guidance for bypassing engineered safety features (ESFs), guidance for monitoring reactor conditions during reactivity changes, and guidance for monitoring plant operation during apparently normal, stable conditions for the purpose of promoting the earlier detection of abnormalities.

- Procedures

This includes whether formal operating procedures exist and are used and their overall quality (good or bad). A common procedure problem seen in event investigations is when procedures

give inadequate information regarding a particular control sequence. Another common problem is the ambiguity of the steps of a procedure, and the fact that a procedure (function oriented) sometimes maintains the safety function but does not aid in the diagnosis and mitigation of a given event.

- Ergonomics

This factor considers the ergonomics of the equipment, the displays and controls that the operator must interact with in the given task(s). Ergonomics is categorized by the vintage of the plant and then the quality. Ergonomics refers to the layout and composition of the controls and displays that the operator is required to interface with to carry out the tasks.

The plant vintage categories are:

- old plant - refers to the older analog style control rooms
- retrofit plant - refers to hybrid controls that may have undergone some changes introducing more modern digital equipment
- new plant - modern controls that integrate the state of the art in digital controls.

Examples of poor ergonomics may be found in panel design layout, annunciator designs, and labeling. In panel design layout, event investigations have shown that when necessary plant indications are not located in one place, it is difficult for an operator to monitor all the necessary indications to properly control the plant. Examples of poor annunciator designs have been found where only a single acknowledge circuit for all alarms is provided which increases the probability that an alarm may not be recognized before it is cleared. Another problem exists where annunciators have setpoints for alarms that are set too close to the affected parameter for an operator or crew to react and perform a mitigating action. Poor labeling has been seen where labels are temporary, informal, illegible, or multiple names are given to the same piece of equipment. In general, labels must be accurate and referenced properly in procedures if they are to be reliable to operators and maintainers.

- Fitness for duty

This factor considers the fitness for duty of the individual(s) who are performing the task. Fitness for duty refers to whether or not the individual performing the task is physically or mentally fit or impaired to perform the task at that time. Things that may affect fitness include drug use (legal or illegal), sickness, fatigue, personal problems and distractions. Fitness for duty is a factor associated with individuals, but not related to training, experience, etc.

- Crew Dynamics

The primary aspect of crew dynamics is how well the particular crew interacts and communicates. Crew dynamics includes consideration of coordination, command, and control. Crew dynamics also includes any management/organizational/supervisory factors that may affect performance.

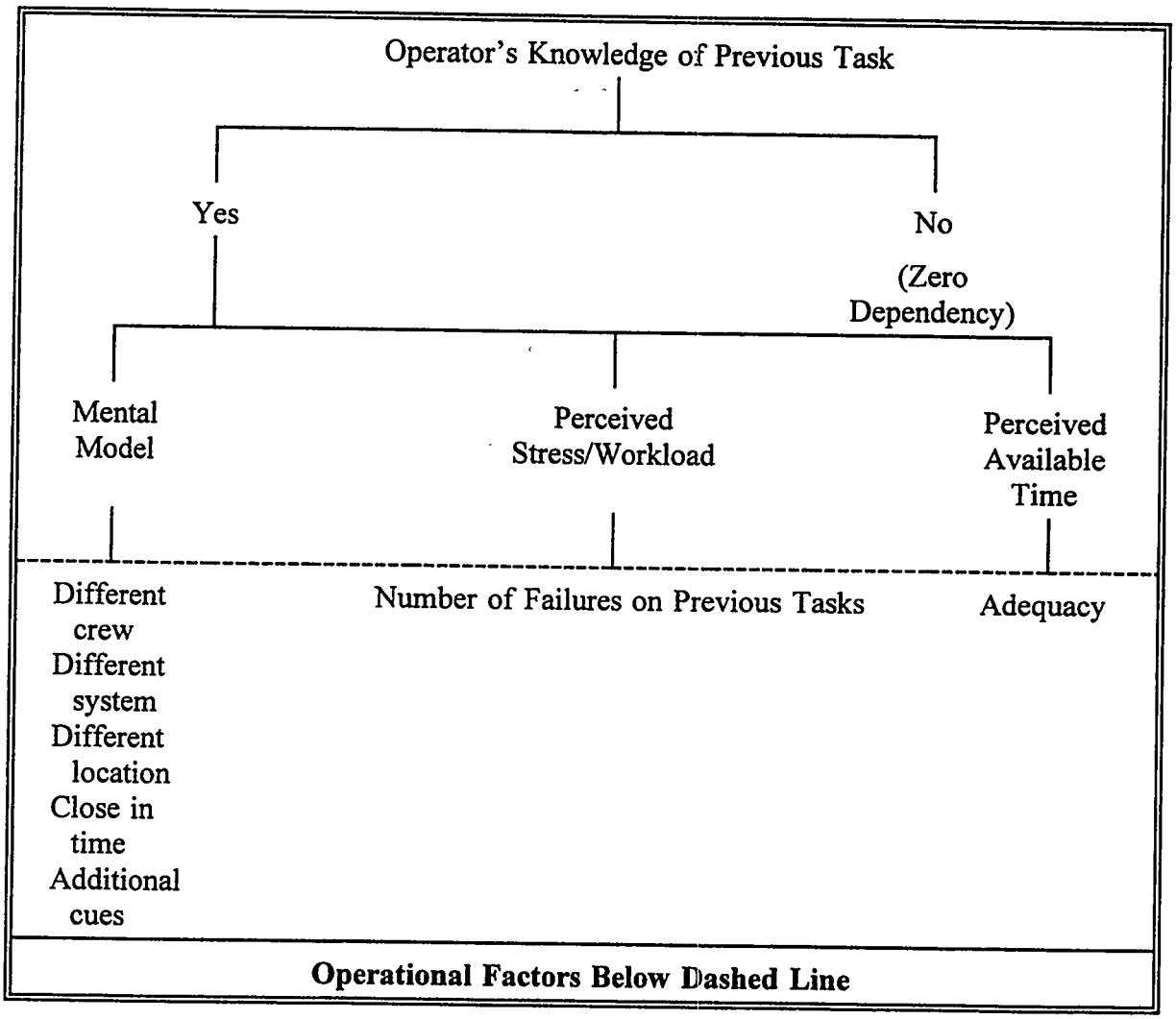
Examples seen in event investigations are problems due to information not being communicated during shift turnover as well as poor communications with maintenance crews and auxiliary operators. The role that the shift supervisor plays at a power plant is also a major factor. Instances where the shift supervisor gets too involved in the specifics of the event instead of maintaining a position of leadership in the control room indicate a breakdown in the crew dynamics.

Table 2 shows the relationship of the summary level factors to the total factors by superscript coding. As can be seen, the various summary factors affect performance across input, processing, and response portions of the model.

At this point, the appropriate level of detail for the human reliability analysis in ASP had to be established. It is not useful for a method to be developed that is impractical in terms of application or that has a higher level of precision than the rest of the model. Keeping this in mind, the means of evaluating each of the summary level factors was developed, using the simplest possible descriptors of each of the six summary level factors. This resulted in decision flows requiring analysts to make judgments of the summary level factors for either generic or specific events.

In addition to the basic decision flows, the method had to consider dependency. Dependency of one task upon another arises from the knowledge or lack of knowledge of the performer of the second task with respect to the occurrence and/or effect of the previous task. This dimension of knowledge cuts across the model of human performance in Table 1. Such knowledge contributes to the building and maintenance of mental models or representations from which the human operates. Mental models are in turn impacted by the same summary level factors that are shown in Table 2 (complexity, stress, and workload; experience/training; procedures (job aids); ergonomics; fitness for duty; and crew dynamics). Figure 1 shows the relationship of these factors to the dimension of knowledge of the previous task. At the top level, if the operator has no knowledge of the prior task or its effect then there is no dependency. If the operator has knowledge of the prior task then consideration must be given to what that knowledge could affect. The next level shows that mental model, perceived stress/workload, and perceived available time are most likely to be affected by knowledge of the prior task. For perceived stress/workload, the primary factor contributing to dependency is whether or not the prior task has failed and hence created a higher level of stress. For perceived available time, the important factor is whether perceived available time is adequate to perform the current task. Listed below mental model, perceived stress/workload, and perceived available time are the operational factors which are observable and which contribute most to the creation of dependency. For mental model, these factors include whether the crew performing the current task is the same or different than for the prior task, whether the current task is being performed on the same or different system than the prior task, whether the current task is being performed in a different location than the prior task, whether or not the current task is being performed close in time to the prior task, and whether there are additional cues available for the performer of the current task. These factors are combined into 24 rule combinations yielding a dependency rating from zero to complete dependence. These levels match the nomenclature used in THERP.

Figure 1. Dependency Model.



3.2 Quantification

The next step was to identify a scheme for quantification. A reasonable approach was to base the numbers on those which were consistent with the literature in HRA. The source selected for the numbers was THERP.[3] Modification factors and dependence equations were taken from the tables of THERP, making as few interpolations and extrapolations as possible. To summarize, an approach was developed to quantify both errors of actuation and recovery errors (accounting for dependency) which is both practical and at an appropriate level of detail, and has been developed from first principles and a generally accepted model of human behavior.

To provide a benchmark of this method to the existing ASP method, the new method was applied to a single task (an initiation) and was compared to the existing ASP recovery factors and numbers for the same task. The results are given in Table 3.

Table 3. Comparison of New Values to Previous ASP Recovery Values

FAILURE DESCRIPTION	PREVIOUS	NEW
Failure did not appear to be recoverable in required period, either from the control room or at failed equipment.	1.00	1.00
Failure appeared recoverable in required period at failed equipment, and equipment was accessible; recovery from control room did not appear possible.	.34	.55
Failure appeared recoverable in required period from the control room, but recovery was not routine or involved substantial stress.	.12	.1
Failure appeared recoverable in required period from control room and was considered routine or procedurally based.,	.04	.01

In the table, the new ASP values are in each case quite close and comparable to the previous values. This comparison shows that the new modeling is within the same order of magnitude of quantification, but have been derived from a method based on sound theoretical ground and scrutable practice.

3.3 Using the ASP Human Error Method

Two worksheets, the ASP Human Error Worksheet and the ASP Human Error Probability for Sequence Worksheet, have been developed as aids in applying the method. These worksheets are shown in Figures 2 and 3.

The ASP Human Error Worksheet is completed for each human error being evaluated in each core damage sequence in the ASP model. This includes both errors of actuation as well as errors of recovery. The ASP Human Error Probability for Sequence worksheet is completed for each core damage sequence involving one or more human errors.

At the top of the front side (Page 1) of the ASP Human Error Worksheet there is a space for recording the specific plant, the specific ASP scenario, the sequence number, and the specific error being evaluated. The analyst evaluates each of the 6 categories listed by making the appropriate decision at each branch point. After making this selection, the analyst circles the number next to the choice.

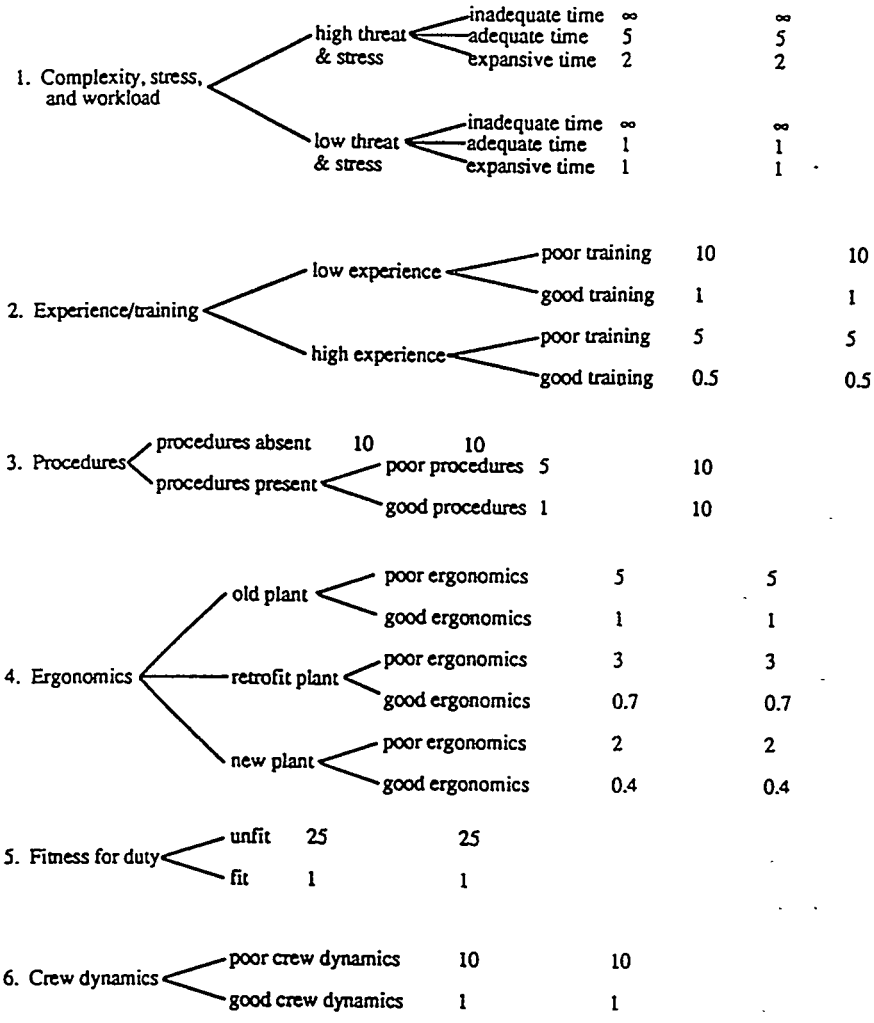
Note that there are two numbers next to each final choice (e.g., high threat and stress, adequate time has a 5 next to it, then a space, then another 5). The duplicate numbers allow for a dual rating on each factor. Ideally, the analyst should separate out the mental processing portion of the task to be rated from the physical response portion of the task, and rate each category separately for each portion. Mental processing refers to tasks (or portions of tasks) which require

Figure 2. ASP Human Error Worksheet.

ASP HUMAN ERROR WORKSHEET (Page 1 of 2)

Plant:_____ Scenario: _____ Sequence Number:_____

Task Error Description:_____



Task Portion	Complexity, stress, and workload	Experience/ training	Procedures	Ergonomics	Fitness for duty	Crew dynamics	
Processing: 10 E-2	x_____	x_____	x_____	x_____	x_____	x_____	= _____Processing Failure Probability
Response: 10 E-3	x_____	x_____	x_____	x_____	x_____	x_____	+ _____Response Failure Probability
							_____Task Failure Probability Without Formal Dependence

Figure 2. (Continued)

ASP HUMAN ERROR WORKSHEET (Page 2 of 2)

DEPENDENCY CONDITION TABLE

Condition Number	Crew (same or different)	System (same or different)	Location (same or different)	Time (close in time or not close in time	Cues (additional or not additional)	Dependency	Number of Human Action Failures
1	s	s	s	c	–	complete	if this
2	s	s	s	nc	na	high	
3	s	s	s	nc	a	moderate	error is the
4	s	s	d	c	–	high	
5	s	s	d	nc	na	moderate	third error
6	s	s	d	nc	a	low	
7	s	d	s	c	–	moderate	in the
8	s	d	s	nc	na	low	
9	s	d	s	nc	a	low	sequence
10	s	d	d	c	–	moderate	
11	s	d	d	nc	na	low	then the
12	s	d	d	nc	a	low	
13	d	s	s	c	–	moderate	dependency
14	d	s	s	nc	na	low	
15	d	s	s	nc	a	zero	is moderate,
16	d	s	d	c	–	zero	
17	d	s	d	nc	na	zero	if it is the
18	d	s	d	nc	a	zero	
19	d	d	s	c	–	low	fourth error
20	d	d	s	nc	na	zero	
21	d	d	s	nc	a	zero	dependency
22	d	d	d	c	–	zero	
23	d	d	d	nc	na	zero	is high
24	d	d	d	nc	a	zero	

Using N=Task Failure Probability Without Formal Dependence (calculated on previous page):

For Complete Dependence the probability of failure is 1.

For High Dependence the probability of failure is (1+N)/2

For Moderate Dependence the probability of failure is (1+6N)/7

For Low Dependence the probability of failure is (1+19N)/20

For Zero Dependence the probability of failure is N

(1 + (___*_____))/___ = _____ Task Failure Probability With Formal Dependence

Figure 3. ASP Human Error Probability for Sequence Worksheet.

ASP HUMAN ERROR PROBABILITY FOR SEQUENCE WORKSHEET

Plant:_____ **Scenario:**_____ **Sequence Number:**_____

First Error in Sequence_____ Human Error Probability:_____

Subsequent Error 1_____ Human Error Probability:_____

Subsequent Error 2_____ Human Error Probability:_____

Subsequent Error 3_____ Human Error Probability:_____

Subsequent Error 4_____ Human Error Probability:_____

Subsequent Error 5_____ Human Error Probability:_____

Subsequent Error 6_____ Human Error Probability:_____

Subsequent Error 7_____ Human Error Probability:_____

Subsequent Error 8_____ Human Error Probability:_____

Subsequent Error 9_____ Human Error Probability:_____

Subsequent Error 10_____ Human Error Probability:_____

Multiply the probability for the first error by the probabilities for each subsequent error to obtain the human error probability for the sequence.

Human Error Probability for the Sequence:_____

predominately decision-making activities on the part of the operator. These are tasks which require the operator to read, collate, calculate or otherwise process information to make a response (i.e., mental processing tasks are "thinking" tasks). Physical response refers to tasks (or portions of tasks) which predominately are composed of taking an action. For example, this refers to turning a switch, pushing a button, turning a wrench, flipping a breaker, etc. (i.e., physical response tasks are "doing" tasks). In these tasks the operator is not required to make any significant decisions that require substantial processing of information. As an example of how mental processing and physical response ratings might differ, consider the task: venting containment. This task might be rated high threat and stress with adequate time for mental processing, but for physical response might be rated high threat and stress with expansive time. The analyst must consider the task and decide which portions will be treated as mental processing tasks and which portions will be treated as physical response tasks. This separation of ratings is desirable because the base failure rate for mental processing tasks is higher than that for physical response tasks. At the bottom of the front side of the ASP Human Error Worksheet, the analyst's mental processing ratings are used to modify a base error rate of 1.0E-2, while the analyst's physical response ratings modify a base error rate of 1.0E-3. These calculations yield two separate error rates, the Processing Failure Probability and the Response Failure Probability. These probabilities are combined to give the Task Failure Probability Without Formal Dependence.

If the error described at the top of the front side (Page 1) of the ASP Human Error Worksheet is the first error in the sequence, the analysis of the error probability stops at this point and the Task Failure Probability Without Formal Dependence is used as the human error probability for the described error. On the other hand, if the error is not the first error in the sequence, the probability of the error needs to specifically include the effects of previous errors (i.e., the probability needs to account for dependency). Dependency is evaluated on the back side (Page 2) of the ASP Human Error Worksheet. The analyst chooses the single condition (out of the 24 conditions available) that matches the error of interest . This can be done by proceeding through the table left to right, evaluating the factors one-by-one. First the analyst decides whether the crew performing on the error of interest is the same crew as performed the previous error in the sequence. Then the analyst decides whether the error involves the same system as the previous error, whether it is the same location as the previous error, whether it is close in time to the previous error, and (if not close in time) whether additional cues are available since the previous error. After deciding on these five factors, a single condition is determined and an appropriate level of dependency is given for that condition in the dependency column of the table. This level of dependency is then adjusted if the error of interest is the third or higher error in the sequence. If the error is the third error in the sequence, dependency must be no less than moderate; if it is the fourth or higher error, the dependency must be no less than high.

Finally, the Task Failure Probability Without Formal Dependence, developed on the front side (Page 1) of the ASP Human Error Worksheet is plugged into the correct equation from THERP based on the dependency rating. This yields a Task Failure Probability With Formal Dependence that thoroughly accounts for dependent effects between and among tasks. Each error that is not the first error in a sequence will have a Task Failure Probability With Formal Dependence calculated for it.

Once each human error in a sequence has been analyzed using the ASP Human Error Worksheet, the human error probability for the sequence is calculated on the ASP Human Error Probability for Sequence Worksheet. At the top of the ASP Human Error Probability for Sequence Worksheet there is a space for recording the specific plant, the specific ASP scenario, and the number of the sequence being evaluated. The human error probabilities for each human error in the sequence are then listed. If the error is the first error in the sequence, the human error probability is the Task Failure Probability Without Formal Dependence, developed on the front side (Page 1) of the ASP Human Error Worksheet. For all subsequent errors in the sequence the human error probability is the Task Failure Probability With Formal Dependence developed on the back side (Page 2) of the ASP Human Error Worksheet. The Human Error Probability for the Sequence is calculated by multiplying together the human error probabilities for each human error in the sequence.

4. COMMON CAUSE FAILURE ANALYSIS

The CCF improvements work focuses on providing better basic parameter estimates while not increasing the complexity of the models. The current ASP logic models are straightforward for construction and review purposes and they generate a reasonable number of simple cutsets. Therefore, it was decided that no modifications be made to the current ASP logic structure developed for symmetric redundant systems which is represented by the independent component failure events ANDed together and then ORed with the CCF basic event(s). Since the ASP logic models will remain unchanged, the focus was placed on the CCF basic events values. Previously, the CCF basic events included only the global CCF mode of all redundant components that failed a system. It is determined that this remain unchanged.

4.1 Independent-Dependent Failure Combinations

Prior to initiating any changes in the CCF basic event values, an analysis was performed to determine the effects of adding independent-dependent combination failures to the CCF basic event probabilities. For example, in a three-train system with a one-out-of-three success criterion, the common cause failure contributors are:

$$CCF_3 + 3*CCF_2*IND$$

where CCF_3 = common cause failure of all three redundant trains, and
$3*CCF_2*IND$ = the three combinations of an independent train failure and a common cause failure of the other two trains.

CCF_3 is the global common cause failure term and $3*CCF_2*IND$ represents the independent-dependent failure combinations.

The analysis revealed that eliminating the independent-dependent failure combinations from the CCF calculations underestimated the CCF contribution by at most approximately 11%. This underestimation alone was not enough to justify inclusion of the independent-dependent

combination events, since the added complexity to the models would be substantial. Thus the ASP method will only model the global failure due to common cause.

4.2 CCF Term Quantification

The Alpha Factor approach, as opposed to the Multiple Greek Letter approach used currently, was selected to estimate the ASP CCF event data. This approach is consistent with the suggestions provided by an expert panel[4] established to review selected portions of the ASP improvements work. In addition, the Alpha Factor approach better supports future work in uncertainty analysis by providing a less rigorous numerical solution for estimating CCF uncertainties. The Alpha Factor approach estimates a ratio of the number of failures based on a specified number of redundant components to the total number of events. This value is represented by α_n where n represents the number of redundant components. In general

$$Q_n = (m\ \alpha_n / [{}^{m}_{n}]\ \alpha_T)\ Q_c$$

where Q_c is the independent failure rate, m is the number of components in the CCF group and $\alpha_T = \sum_{n=1}^{m} m\ \alpha_n$. For example, the fraction of the number of failures involving two and only two components (Q_2) in a system where two components are susceptible to CCF is equal to

$$(2\alpha_2 / (\alpha_1 + 2\alpha_2)) * Q_c.$$

In a three component system $\alpha_2 = 3Q_2/Q_T$, or in terms of the independent failure rate

$$Q_2 = (3\alpha_2 / (\alpha_1 + 2\alpha_2 + 3\alpha_3)) * Q_c$$

where $3Q_2$ is equal to three combinations of failures involving two and only two components due to common cause and Q_T represents the total number of events. In the ASP methodology, Q_c is obtained from generic sources (ASEP database) or plant-specific sources when available (previous PRAs, IPEs, etc.). The failure probability for n number of redundant components greater than one (α_n where $n > 1$) will be estimated from results generated by the CCF database[5] now under development and the CCF Analysis Software.[6]

4.3 Modeling CCF Components

In the current ASP models, CCF events have been included for heat exchangers, diesel generators, motor-driven pumps, motor-operated valves, air-operated valves, and turbine-driven pumps. CCFs for check valves, pressure-operated relief valves, safety relief valves have not been included but will be added as part of the ASP CCF improvement task.

4.4 CCF Modeling Changes for Event Evaluations

The primary purpose of developing the ASP models is to evaluate the risk significance of operational events. Many times these events involve a reduction in the redundancy of safety systems. The impact of modifying the number of redundant components or trains on the CCF terms requires a basic knowledge of the plant model. Modification of the independent basic

event(s) to a house event TRUE and revision of CCF basic event values is required prior to regeneration/requantification of the cutsets to estimate a conditional core damage probability.

To facilitate the use of the ASP models for the analytical purposes mentioned above, all possible CCF basic event values will be included in the basic event database. Choosing the appropriate CCF value depends upon the number of redundant components susceptible to common cause failure, the number of components unavailable and the success criteria of the system. When one or more components are unavailable, the possibility that additional components may fail due to independent CCF mechanisms requires that the equation describing the CCF probability contain all possible CCFs of n *or more* components that fail the train or system. These equations are currently being developed.

5. OTHER MODELING IMPROVEMENTS

The ASP models currently do not include a number of the features typically found in a full-scope PRA. The following areas are being investigated for possible inclusion or improvements.

- Support System Models. The current ASP models do not include failures of support systems except for some very cursory emergency power dependencies. The current methodology requires the analyst to interpret the plant dependency matrix and manually fail any front-line equipment that is unavailable due to a support system failure. However, potentially important dependencies among the operational equipment are not modeled. The support systems for four plants will be modeled and integrated into the ASP models. Comparisons will be made to determine the impact of support systems on the model results. Based on the results, a decision will be made whether to proceed with all the other plants.

- Testing and Maintenance Unavailabilities. The current ASP models do not include train or component unavailabilities due to testing or maintenance. These unavailabilities can be readily incorporated into the ASP models without adding much complexity to the models. The major effort would be spent in determining the proper frequencies and durations for the various tests and maintenance activities.

- Initiating Events. The ASP models include the most commonly encountered initiating events: transient, loss of offsite power (LOOP), small loss of coolant accident (SLOCA), and steam generator tube rupture (SGTR). It is recognized that this set of initiating events is incomplete and does not represent the entire risk spectrum for a plant. Work is underway to determine if any other initiating events would be significantly useful for the purposes of operational event evaluations and whether the modeling of such initiating events would be cost effective.

- External Events. One of the restrictions for event evaluation inherent in the current ASP models is the inability to evaluate the impact of external event related issues, degradations, and failures. Operational events such as those associated with improper

anchorage of equipment or failure of fire boundaries are very difficult to analyze without external event models. NRC's Office of Research (RES) is currently pursuing establishing a project to address this need.

- Containment Behavior. The ASP models do not address containment performance (Level 2 PRA issues). Ocassionally, operational events that could impact the ability of the containment to perform its safety function are reported. It may be possible to extend the ASP models to include a simple, yet effective capability to analyze this type of event.

- Shutdown and Low Power Risk. Again, this is an area where operational events are encountered and the current ASP models and methods do not provide for easy analysis. RES has recognized this and has included shutdown and low power modeling as an element of the same project addressing external events.

- Generic Versus Plant-Specific Data. For most of the ASP models, the Accident Sequence Evaluation Program (ASEP) database was used to develop the hardware basic event failure probabilities. In some cases, the data from an existing PRA or IPE was deemed appropriate, however, the resources were not available to properly assess what the best data source was for each model.

6. REFERENCES

1. K. D. Russell, et al, SAPHIRE Technical Reference Manual: IRRAS/SARA 4.0, NUREG/CR-5964, December 1992.

2. Science Applications International Corporation, Daily Events Evaluation Manual (Draft Report), 1-275-03-336-01, January 31, 1992.

3. A. D. Swain and H. E. Guttmann, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, 1983.

4. Meeting between INEL and NRC AEOD, June 2, 1994.

5. H.M. Stromberg, F.M. Marshall, A. Mosleh, Common Cause Failure System: Definition and Classification of Common Cause Failure Events, NUREG/CR EGG-2709 Vol 2, October 1993.

6. K.L. Kvarfordt, A. Mosleh, N.L. Skinner, Common Cause Failures Database and Analysis Software, NUREG/CR EGG-2709 Vol 4, Sept 1993.

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-0140
Vol. 1

2. TITLE AND SUBTITLE
Proceedings of the Twenty-Second Water Reactor Safety Information Meeting
Plenary Session, Advanced Instrumentation & Control Hardware & Software, Human Factors Research, IPE & PRA

3. DATE REPORT PUBLISHED
MONTH: April
YEAR: 1995

4. FIN OR GRANT NUMBER
A3988

5. AUTHOR(S)
Compiled by Susan Monteleone, BNL

6. TYPE OF REPORT
Conference Proceedings

7. PERIOD COVERED *(Inclusive Dates)*
October 24-26, 1994

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 papers presented at the Twenty-Second Water Reactor Safety Information Meeting held at the Bethesda Marriott Hotel, Bethesda, Maryland, during the week of October 24-26, 1994. 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 Finland, France, Italy, Japan, Russia 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, international organizations-meetings, PWR type reactors-reactor safety, water cooled reactors-proceedings, Human Factors, Leading Abstract, Reactor Control Systems, Reactor Instrumentation, Probabilistic Estimation, Risk Assessment

13. AVAILABILITY STATEMENT
Unlimited

14. SECURITY CLASSIFICATION
(This Page)
Unclassified
(This Report)
Unclassified

15. NUMBER OF PAGES

16. PRICE