NUREG/CP-0157
Vol. 3

Proceedings of the U.S. Nuclear Regulatory Commission

Twenty-Fourth Water Reactor Safety Information Meeting

Volume 3

- PRA and HRA
- Probabilistic Seismic Hazard Assessment and Seismic Siting Criteria

Held at
Bethesda Marriott Hotel
Bethesda, Maryland
October 21–23, 1996

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 NOTICE

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

NUREG/CP-0157
Vol. 3

Proceedings of the U.S. Nuclear Regulatory Commission

Twenty-Fourth Water Reactor Safety Information Meeting

Volume 3

- PRA and HRA
- Probabilistic Seismic Hazard Assessment and Seismic Siting Criteria

Held at
Bethesda Marriott Hotel
Bethesda, Maryland
October 21-23, 1996

Manuscript Completed: January 1996
Date Published: February 1997

Compiled by: Susan Monteleone

C. Bonsby, NRC Project Manager

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

Proceedings Prepared by
Brookhaven National Laboratory

NUREG/CP-0157, Vol. 3 has been reproduced from the best available copy.

ABSTRACT

This three-volume report contains papers presented at the Twenty-Fourth Water Reactor Safety Information Meeting held at the Bethesda Marriott Hotel, Bethesda, Maryland, October 21-23, 1996. 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 Czech Republic, Finland, France, Japan, Norway, 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
24TH WATER REACTOR SAFETY INFORMATION MEETING

OCTOBER 21-23, 1996

Published in Three Volumes

GENERAL INDEX

Volume 1

- Plenary Sessions
- High Burnup Fuel
- Containment and Structural Aging

Volume 2

- Reactor Pressure Vessel Embrittlement and Thermal Annealing
- Reactor Vessel Lower Head Integrity
- Evaluation and Projection of Steam Generator Tube Condition and Integrity

Volume 3

- PRA and HRA
- Probabilistic Seismic Hazard Assessment and Seismic Siting Criteria

REGISTERED ATTENDEES (NON-NRC)
24TH WATER REACTOR SAFETY INFORMATION MEETING

J. ALMBERGER
VATTENFALL FUEL
STOCKHOLM, S-16287 SWEDEN
46-8-7395444 FAX 46-8-178640
JAN@FUEL.VATTENFALL.SE

A. ALONSO
CONSEJO DE SEGURIDAD NUCLEAR
JUSTO DORADO, 11
MADRID, 28040 SPAIN
341-346-0334 FAX 341-346-0378
AAS@CSN.ES

L. ANDERMO
SWEDISH NUCLEAR POWER INSPECTORATE
KLARABERGSVIADUKTEN 90
STOCKHOLM, 10658 SWEDEN
46-8-6988484 FAX 46-8--6619086
LARSA@SKI.SE

R. ANDERSON
NORTHERN STATES POWER CO.
414 NICOLLET MALL, RSq 8
MINNEAPOLIS, MN 55401 USA
612-337-2050 FAX 612-337-2042

A. ANKRUM
PACIFIC NORTHWEST NATIONAL LABORATORY
PO BOX 999, MSIN: K8-28
RICHLAND, WA 99352 USA
509-372-4095 FAX 509-375-3970
AR_ANKRUM@PNL..GOV

E. ARAIZA
COMISION NACIONAL DE SEGURIDAD NUCLEAR
DR. BARRAGAN 779 COL. NARVARTE
MEXICO CITY, 03020 MEXICO
525 590-8113 FAX 525 590-6103

V. ASMOLOV
RRC KURCHATOV INSTITUTE, NSI
KURCHATOV SQ. 1
MOSCOW, 123182 RUSSIA
7-095-1969320 FAX 7-0951961702
ASMOLOV@OBAE.KIAE.SU

M. AZARM
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, PO BOX 5000
UPTON, NY 11973-5000 USA
516-344-4922 FAX 516-344-5730
AZARM@BNL.GOV

S. AZUMI
KANSAI ELECTRIC POWER CO., INC.
2001 L STREET, NW, SUITE 801
WASHINGTON, DC 20036 USA
202-658-1138 FAX 202-457-0272

J. BAILEY
ARIZONA PUBLIC SERVICE CO.
P.O. BOX 53999
PHOENIX, AZ 85072-3999 USA

S. BAKHTIARI
ARGONNE NATIONAL LABORATORY
9700 S. CASS AVE.
ARGONNE, IL 60439 USA
630-252-8962 FAX 630-252-3250
SASAN_BAKHTIARI@GMGATE.ANL.GOV

W. BALZ
COMMISSION OF THE EUROPEAN COMMUNITIES
200, RUE DE LA LOI
BRUSSELS, 1049 BELGIUM
32-2-2954164 FAX 32-2-2966883

Y. BANG
KOREA INSTITUTE OF NUCLEAR SAFETY
PO BOX 114 YUSONG
TAEJON, 305-600 KOREA
82-42-868-0140 FAX 82-42-861-2535
K164BYS@KINSWS.KINS.RE.KR

A. BARATTA
PENNSYLVANIA STATE UNIVERSITY, DNE
231 SACKETT BLDG.
UNIVERSITY PARK, PA 16802 USA
814-865-1341 FAX 814-865-8499
AB2@PSUVM.PSU.EDU

R. BARI
BROOKHAVEN NATIONAL LABORATORY
BLDG. 197C, PO BOX 5000
UPTON, NY 11973-5000 USA
516-344-2629 FAX 516-344-5266
BARI1@BNL.GOV

J.P. BERGER
EDF - SEPTEN
12 AV. DU DUTRIEVOZ
VILLEURBANNE, 69628 FRANCE
72-82-7599 FAX 72-82-7690

C. BEYER
BATTELLE PACIFIC NORTHWEST LABORATORY
PO BOX 999
RICHLAND, WA 99352 USA
509-372-4605 FAX 509-372-4439
CE_BEYER@PNL.GOV

D. BHARGAVA
VIRGINIA POWER
5000 DOMINION BLVD.
GLEN ALLEN, VA 23060 USA
804-273-3638 FAX 804-273-2188
DIVAKAR_BHARGAVA@VAPOWER.COM

J. BOCCIO
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, PO BOX 5000
UPTON, NY 11973-5000 USA
516-344-7690 FAX 516-344-5730
BOCCIO@BNL.GOV

R. BORSUM
FRAMATOME TECHNOLOGIES, INC.
1700 ROCKVILLE PIKE, SUITE 525
ROCKVILLE, MD 20852-1631 USA
301-230-2100 FAX 301-468-6246

G. BROWN
AEA TECHNOLOGY
RISLEY, WARRINGTON
CHESHIRE, ENGLAND UK
01925-254473 FAX 1925254576
GEOFF.BROWN@AEAT.CO.UK

M. BRUMOVSKY
NUCLEAR RESEARCH INSTITUTE REZ
REZ PLE
REZ, 25068 CZECH REPUBLIC
42-2-6857979 FAX 42-2-6857519

W. BRUNSON
FRAMATOME COGEMA FUELS
3315 OLD FOREST RD.
LYNCHBURG, VA 24506-0935 USA
804-832-2687 FAX 804-832-3663
WBRUNSON@FRAMATECH.COM

A. CAMP
SANDIA NATIONAL LABORATORIES
PO BOX 5800
ALBUQUERQUE, NM 87185-0747 USA
505-844-5960 FAX 505-844-3321
ALCAMP@SANDIA.GOV

G. CAPPONI
AGENZIA NAZ. PER LA PROT. DE'L' AMBIENTE
VIA V. BRANCATI, 48
ROMA, 00144 ITALY
39-6-50072198 FAX 39-6-50072044
CAPPG@ANPA.IT

M. CARLSSON
STUDSVIK NUCLEAR AB
NYKOPING, 61182 SWEDEN
46-155-221000 FAX 46-155-263070

W. PAUL CHEN
ENERGY TECHNOLOGY ENGINEERING CENTER
6633 CANOGA AVENUE
CANOGA PARK, CA 91304 USA
818-586-5285 FAX 818-586-5118

J. CHERRY
SANDIA NATIONAL LABORATORIES
PO BOX 5800, MS 0741
ALBUQUERQUE, NM 87185-0741 USA
505-844-0090 FAX 505-844-1648
JCHERR@SANDIA.GOV

F.B. CHEUNG
PENNSYLVANIA STATE UNIVERSITY
304 REBER BLDG.
UNIVERSITY PARK, PA 16802 USA
814-863-4261 FAX 814-863-8682
FXC4@PSU.EDU

D. CHO
KOREA INSTITUTE OF NUCLEAR SAFETY
PO BOX 114 YUSONG
TAEJON, 305-600 KOREA
82 042 868 0229

W. CHOE
TU ELECTRIC NUCLEAR SAFETY ANALYSIS
1601 BRYAN ST., EP 15
DALLAS , TX 75201-3411 USA
214-812-4371 FAX 214-812-8687

Y.J. CHOI
KOREA INSTITUTE OF NUCLEAR SAFETY
PO BOX 114 YUSONG
TAEJON, 305-600 KOREA
82-42-868-0139 FAX 82-42-861-2535
K149CYJ@KINSWS.KINS.RE.KR

T.Y. CHU
SANDIA NATIONAL LABORATORIES
PO BOX 5800, MS 1139
ALBUQUERQUE, NM 87185-1139 USA
505-845-3217 FAX 505-845-3117
TYCHU@SANDIA.GOV

H.M. CHUNG
ARGONNE NATIONAL LABORATORY
9700 SO. CASS AVE.
ARGONNE, IL 60439 USA
630-252-5111 FAX 630-252-3604
HEE_CHUNG@QMGATE.ANL.GOV

R. CLARK
GOLDER ASSOCIATES, INC.
4104 148TH AVE., NE
REDMOND, WA 98052 USA
206-883-0777 FAX 206-882-5474
RCLARK@GOLDER.COM

T. CLONINGER
HOUSTON LIGHTING & POWER COMPANY
P.O. BOX 289
WADSWORTH, TX 77483 USA

J. CONDE
CONSEJO DE SEGURIDAD NUCLEAR
JUSTO DORADO, 11
MADRID, 28040 SPAIN
34-1-3460-253 FAX 34-1-3460-588
JMCL@CSM.ES

R. COPELAND
SIEMENS POWER CO.
2101 HORN RAPIDS ROAD
RICHLAND, WA 99352 USA
509 375-8290

D. COPINGER
OAK RIDGE NATIONAL LABORATORY
PO BOX 2009, BLDG. 9201-3
OAK RIDGE, TN 37831 USA
423-574-3222 FAX 423-574-0382
D9C@ORNL.GOV

C. CORNELL
C. ALLEN CORNELL CO.
110 COQUITO WAY
PORTOLA VALLEY, CA 94028 USA
415-854-8053 FAX 415-854-8075
CORNELL@SURGE.STANFORD.EDU

B. CORWIN
OAK RIDGE NATIONAL LABORATORY
P.O. BOX 2008
OAK RIDGE, TN 37831 USA
423-574-4648 FAX 423-574-5118
CORWINWR@ORNL.GOV

D. COUCILL
BRITISH NUCLEAR FUELS
SPRINGFIELDS WORKS, SALWICK
PRESTON, UK
44 1772 762085 FAX 44 1772 763888

M. COURTAUD
COMMISSARIAT A L'ENERGIE ATOMIQUE
17, RUE DES MARTYRS
GRENOBLE, CEDEX 9, 38054 FRANCE
33 4 76 88 36 60 FAX 33 4 76 88 51 79
COURTAUDDRN.CEA.FR

K. COZENS
NUCLEAR ENERGY INSTITUTE
1776 I ST., NW, SUITE 400
WASHINGTON, DC 20006-3708 USA
202-739-8085 FAX 202-785-1898

M. CUNNINGHAM
PACIFIC NORTHWEST NATIONAL LABORATORY
PO BOX 999
RICHLAND, WA 99352 USA
509-372-4987 FAX 509-372-4989
ME_CUNNINGHAM@PNL.GOV

C. CZAJKOWSKI
BROOKHAVEN NATIONAL LABORATORY
PO BOX 5000, BLDG. 830
UPTON, NY 11973-5000 USA
516-344-4420 FAX 516-344-4486
CJC@BNL.GOV

B. DE BOECK
AVN
AVENUE DU ROI 157
BRUSSELS, B-1190 BELGIUM
32-2-5368335 FAX 32-2-5368585
BDB@AVN.BE

F. DE PASQUALE
ATOMIC ENERGY CONTROL BOARD
280 SLATER ST.
OTTAWA, ONTARIO K1P5S9 CANADA
613-947-4018 FAX 613-995-5086
DEPASQUALE.F@ATOMCO.GA.CA

J. DeBOR
3630 NO. 21 AVE.
ARLINGTON, VA 22207 USA
703-524-3222 FAX 703-524-2427

D. DIERCKS
ARGONNE NATIONAL LABORATORY
9700 S. CASS AVE.
ARGONNE, IL 60439 USA
630-252-5032 FAX 630-252-4798
DR_DIERCKS@OMGATE.ANL.GOV

S. DOROFEEV
RRC KURCHATOV INSTITUTE
KURCHATOV SQUARE 1
MOSCOW, 123182 RUSSIA
7 095 196 9840 FAX 7 095 882 5801
DOROFEEV@ACPI.MSK.SU

J. DUCO
INSTITUT DE PROT. ET DE SURETE NUC.
CEA/FAR - BP6
FONTENAY AUX ROSES, CEDEX 92265 FRANCE
33 1 46 54 7068 FAX 33 1 46 54 4437
DUCO@BASILIC.CEA.FR

M. DURIN
INSTITUT DE PROT. ET DE SURETE NUC.
CEA FAR, BP NO. 6
FONTENAY AUX ROSES, CEDEX 92265 FRANCE
33-1-46-54-81-83 FAX 33-1-46-54-32-64

Z. ELAWAR
PALO VERDE NUCLEAR GENERATING STATION
PO BOX 52034, STA. 7527
PHOENIX, AZ 85072-2034 USA
602-393-5328 FAX 602-393-5467
ZELAWAR@APSC.COM

J.M. EVRARD
INSTITUT DE PROT. ET DE SURETE NUC.
CEA FAR, BP NO. 6
FONTENAY AUX ROSES, CEDEX 92265 FRANCE

M. EVRE
PECO NUCLEAR, FUEL & SERVICES DIV.
965 CHESTERBROOK BLVD., 62a-5
WAYNE, PA 19087-5691 USA
610-640-6829 FAX 610-640-6797

J. FIGUERAS
CONSEJO SEGURIDAD NUCLEAR
JUSTO DORADO, 11
MADRID, 28040 SPAIN
34 1 3460204 FAX 34 1 3460588
JMFC@CSN.ES

K. FOLK
SOUTHERN NUCLEAR OPERATING CO.
PO BOX 1295
BIRMINGHAM, AL 35201 USA
205 992-7385 FAX 205 992-5536
KEN.F.FOLK@SNC.COM

W. FORD
OAK RIDGE NATIONAL LABORATORY
BLDG. 4500-N, MS 6238 PO BOX 2008
OAK RIDGE, TN 37831-6238 USA
423-574-5272 FAX 423-574-9676
WEC@ORNL.GOV

L. FUGELSO
SANDIA NATIONAL LABORATORIES
PO BOX 5800
ALBUQUERQUE, NM 87185-0742 USA
505-845-3228 FAX 505-844-0955
JFUGEL@SANDIA.GOV

T. FUKETA
JAPAN ATOMIC ENERGY RESEARCH INST.
TOKAI, IBARAKI 319-11 JAPAN
81 29 282-6386 FAX 81 29 282-6160
TOYO@NSRRSUNL.TOKAI.JAERI.GO.JP

W. GALYEAN
IDAHO NATIONAL ENGINEERING LABORATORY
PO BOX 1625
IDAHO FALLS, ID 83415-3850 USA
208 526-0627 FAX 208 526-2930
WGJ@INEL.GOV

G. GAUTHIER
COMM. A L'ENERGIE ATOMIQUE
60-68 AV. DU GENERAL LECLERK
FONTENAY AUX ROSES, 92265 FRANCE
33 1 46 549174 FAX 33 1 47461016

J. GESSLER
JAPAN ELECTRIC POWER INFORMATION CENTER
1120 CONNECTICUT AVE, NW, #1070
WASHINGTON, DC 20036 USA
202-955-5610 FAX 202-955-5612
JGESSLER@JEPIC.COM

L. GOLDSTEIN
THE S.M. STOLLER CORPORATION
485 WASHINGTON AVE.
PLEASANTVILLE, NY 10570 USA
914-741-1200 FAX 914-741-2093
STOLLERP@COMPUTER.NET

M. GOMOLINSKI
INSTITUT DE PROT. ET DE SURETE NUC.
CEA / FAR - BP 6
FONTENAY AUX ROSES, CEDEX 92265 FRANCE
33 1 46 54 8177 FAX 33 1 46 54 8925

J. GORMAN
DOMINION ENGINEERING, INC.
6862 ELM ST.
MC LEAN, VA 22101 USA
703 790-5544 FAX 703-790-0027
DEI@US.NET

C. GRANDJEAN
INSTITUT DE PROT. ET DE SURETE NUC.
CEA CADARACHE
ST PAUL LEZ DURANCE, 13108 FRANCE
33 04 42 25 4480 FAX 33 04 42 25 3555
GRANDJEAN@IPSNCAD.CEA.FR

G. HACHE
INSTITUT DE PROT. ET DE SURETE NUC.
CEA CADARACHE
ST PAUL LEZ DURANCE, 13108 FRANCE
33 42 25 2055 FAX 33 42 25 7679

R. HALL
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, PO BOX 5000
UPTON, NY 11973-5000 USA
516-344-2144 FAX 516-344-3957
REHALL@BNL.GOV

B. HALLBERT
OECD HALDEN REACTOR PROJECT
PO BOX 173, N-1751
HALDEN, NORWAY
47-69-18-31-00 FAX 47-69-18-71-09
BRUCE.HALLBERT@NRP.NO

N. HANUS
KNOLLS ATOMIC POWER LABORATORY
PO BOX 1072
SCHENECTADY, NY 12301 USA
518-395-7098 FAX 518-395-4422

O. HASCOET
EDF - SEPTEN
12 AV. DU DUTRIEVOZ
VILLEURBANNE, 69628 FRANCE
33-72-82-74-91 FAX 33-72-82-75-55
OLIVER.HASCOET@DE.EDFGDF.FR

P. HAYWARD
ATOMIC ENERGY OF CANADA LIMITED
WHITESHELL LABORATORIES
PINAWA, MANITOBA ROE 1LO CANADA
204-753-2311 ext. 2790 FAX 204-753-2455

J.Y. HENRY
COMM. A L'ENERGIE ATOMIQUE
60-68 AV. DU GENERAL LECLERK
FONTENAY AUX ROSES, 92265 FRANCE
33 1 46 54 8565 FAX 33 1 47 46 1014

R. HENRY
FAUSKE & ASSOCIATES, INC.
16W070 WEST 83RD ST.
BURR RIDGE, IL 60521 USA
630-323-8750 FAX 630-986-5481
HENRY@FAUSKE.COM

G. HEUSENER
FORSCHUNGSZENTRUM KARLSRUHE
WEBERSTRASSE 5
KARLSRUHE, 76133 GERMANY
0 7247 82 5510 FAX 0 7257 82 5508

J. HIGGINS
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, PO BOX 5000
UPTON, NY 11973-5000 USA
516-344-2432 FAX 516-344-4900
HIGGINS@BNL.GOV

K. HISAJIMA
NUCLEAR POWER ENGINEERING CORP.
2F 3-13, 4-CHOME, TORANOMON
MINATO-KU, TOKYO 105 JAPAN
03 3434-2450 FAX 03 3434-6786

R. HOBBINS
RRH CONSULTING
PO BOX 971
WILSON, WY 83014 USA
307-739-0604 FAX 307-739-0604
RHOBBINS@WYOMING.COM

P. HOFMANN
FORSCHUNGSZENTRUM, IMF-1
PO BOX 3640
KARLSRUHE, 76021 GERMANY
49 7247 82 2517 FAX 49 7247 82 4567
PETER.HOFMANN@IMF.FZK.DE

H. HOLMSTROM
VTT ENERGY, NUCLEAR
PO BOX 1604
ESPOO, 02044 FINLAND
358 9 456 5050 FAX 358 9 456 5000
HEIKKI.HOLMSTROM@VTT.FI

T. HSU
VIRGINIA POWER
5000 DOMINION BLVD.
GLEN ALLEN, VA 23060 USA
804-273-3095 FAX 804-273-2188
TOM_W._HSU@VAPOWER.COM

I. HWANG
SEOUL NATIONAL UNIVERSITY
SAN 56-1, RM 32-211, SHINLIM-DONG, GWANAK-KU
SEOUL, 151-742 KOREA
82 2 880-7215 FAX 82 2 889-2688
HWANGILS@ALLIANT.SNU.AC.KR

Y.D. HWANG
KOREA ATOMIC ENERGY RESEARCH INST.
KUKJIM 150, YOUSUNG
TAEJON, KOREA
82 42 868-8292 FAX 82 42 868-8990
YDHWANG@NANUM.KAERI.RE.KR

K. ISHIJIMA
JAPAN ATOMIC ENERGY RESEARCH INST.
TOKAI, IBARAKI 319-11
TOKAI, IBARAKI 319-11 JAPAN

J.J. JEONG
KOREA ATOMIC ENERGY RESEARCH INST.
KUKJIM 150, YOUSUNG
TAEJON, KOREA
82 42 868 2659 FAX 82 42 868 8362
JJJEONG@NANUM.KAERI.RE.KR

Y. JIN
KOREA ATOMIC ENERGY RESEARCH INST.
KUKJIM 150, YUSONG
TAEJON, KOREA
82 42 868 2756 FAX 82 42 868 8256
YHJIN@NANUM.KAERI.RE.KR

W. JOHNSON
UNIVERSITY OF VIRGINIA
115 FALCON DR.
CHARLOTTESVILLE, VA 22901 USA
804-982-5465 FAX 804-982-5473
WRJ@VIRGINIA.EDU

R. JONES
STRUCTURAL INTEGRITY, MAGNOX ELECTRIC
BERKELEY CENTRE
BERKELEY, GLOUCESTERSHIRE GL139PB UK
0-1-453-81-2479 FAX 0-1-453-81-2693

M. KAKAMI
JAPAN ELECTRIC POWER INFORMATION CENTER
1120 CONNECTICUT AVE, NW, #1070
WASHINGTON, DC 20036 USA
202-955-5610 FAX 202-955-5612
GENDER@JEPIC.COM

R. KARIMI
SCIENCE APPLICATIONS INT'L CORP.
20201 CENTURY BLVD.
GERMANTOWN, MD 20874 USA
301-353-8326 FAX 301-428-0145
ROY.KARMI@CPMX.SAIC.COM

E. KEE
HOUSTON LIGHTING & POWER
SO. TEXEX PROJ., FM 521
WADSWORTH, TX 77414 USA
512-972-8907 FAX 512-972-8081

M. KENJI
NUCLEAR POWER ENGINEERING CORP.
FUJITA KANKO TORANOMON BLDG. 8F 1
MINATO-KU, TOKYO 105 JAPAN
81-3-5470-5500 FAX 81-3-5470-5524

R. KENNEDY
RPK STRUCTURAL MECHANICS CONSULTING, INC.
18971 VILLA TERRACE
YORBA LINDA, CA 92886 USA
714-777-2163 FAX 714-777-8299

H.J. KIM
KOREA INSTITUTE OF NUCLEAR SAFETY
PO BOX 114 YUSONG
TAEJON, 305-600 KOREA
82 42 868 0230 FAX 82 42 861-1700

H.K. KIM
KOREA INSTITUTE OF NUCLEAR SAFETY
PO BOX 114 YUSONG
TAEJON, 305-600 KOREA
82-42-868-0224 FAX 82-42-861-0943
K113KHK@PINPOINT.KMS.RE.KR

K.T. KIM
KOREA INSTITUTE OF NUCLEAR SAFETY
PO BOX 114 YUSONG
TAEJON, 305-600 KOREA
82-42-868-0153 FAX 82-42-861-2535
K235KKT@PINPOINT.KINS.RE.KR

J. KNEELAND
CONSUMERS POWER COMPANY
27780 BLUE STAR MEMORIAL HWY.
COVERT, MI 49043 USA
616-764-2814 FAX 616-764-2060

J. KOHOPAA
IVO INTERNATIONAL LTD.
RAJATORPANTIE 8
VANTAA, 01019 FINLAND
358-9-8561-4420 FAX 358-9-563-0432
JYRKI.KOHOPAA@IVO.FI

S. KOMURA
TOSHIBA CORPORATION
8, SHINSUGITA-CHO, ISOGO-KU
YOKOHAMA, KANAGAWA-KEN 235 JAPAN
85-45-770-2032 FAX 85-45-770-2117
KOMURA@RDEF.IEC.TOSHIBA.CO.JP

D. KOSS
PENNSYLVANIA STATE UNIVERSITY
202A STEIDLE BLDG.
UNIVERSITY PARK, PA 16803 USA
814-865-5447 FAX 814-865-2917
KOSS@EMS.PSU.EDU

J. KRAMER
ARGONNE NATIONAL LABORATORY
9700 SO.CASS AVE, BLDG. 207
ARGONNE, IL 60439 USA
630-252-4583 FAX 630-252-3075
JMKRAMER@ANL.GOV

J. KUJAL
NUCLEAR RESEARCH INSTITUTE
REZ NEAR PRAGUE
, 250 68 CZECH REPUBLIC
422-685-79-60 FAX 422-688-20-29
KUJ@NRI.CZ

D. KUPPERMAN
ARGONNE NATIONAL LABORATORY
9700 S. CASS AVE.
ARGONNE, IL 60439 USA
630-252-5108 FAX 630-252-4798

K. KUSSMAUL
MPA UNIV. OF STUTTGART
PFAFFENWALDRING 32
STUTTGART, D-70569 GERMANY
49-711-685-3582 FAX 49-711-685-2635
KUSSMAUL@MPA.UNISTUTTGART.DE

P. LACY
UTILITY RESOURCE ASSOCIATES
SUITE 1600, 51 MONROE ST.
ROCKVILLE, MD 20854 USA
301-294-1940 FAX 301-294-7879

J. LAKE
IDAHO NATIONAL ENGINEERING LABORATORY
PO BOX 1625, MS 3860
IDAHO FALLS, ID 83415-3860 USA
208-526-7670 FAX 208-526-2930
JJL@INEL.GOV

J. LAMBERT
ARGONNE NATONAL LABORATORY
9700 S. CASS AVENUE
ARGONNE, IL 60187 USA
630 252-6695 FAX 630 252-4922
LAMBERT@FLICKER.FP.ANL.GOV

D. LAMPE
UTILITY RESOURCE ASSOCIATES
SUITE 1600, 51 MONROE ST.
ROCKVILLE, MD 20854 USA
301-294-1940 FAX 301-294-7879

P. LAROUERE
VIRGINIA POWER
5000 DOMINION BLVD.
GLEN ALLEN, VA 23060 USA
804-273-2269 FAX 804-273-3543
PAULA_J._LAROUERE@VAPOWER.COM

T. LEAX
WESTINGHOUSE BETTIS ATOMIC POWER LAB
PO BOX 79
WEST MIFFLIN, PA 15122 USA
412-476-6782 FAX 412-476-5151

J.H. LEE
KOREAN NUCLEAR FUEL COMPANY
150 DEOJIN-DONG, YUSUNG-CZY
TAEJON, 305-353 KOREA
82 42 868 1461 FAX 82 42 862 4790

S. LEE
KOREA INSTITUTE OF NUCLEAR SAFETY
PO BOX 114 YUSONG
TAEJON, 305-600 KOREA
82-42-868-0196 FAX 82-42-861-0943

Y. LEE
KOREA INSTITUTE OF NUCLEAR SAFETY
PO BOX 114 YUSONG
TAEJON, 305-600 KOREA
82-42-868-0007 FAX 82-42-861-2535

J. LEHNER
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, PO BOX 5000
UPTON, NY 11973-5000 USA
516-344-3921 FAX 516-344-5730
LEHNER@BNL.GOV

J. LEWI
INSTITUT DE PROT. ET DE SURETE NUC.
CEA CADARACHE
ST PAUL LEZ DURANCE, 13108 FRANCE
33-04-42-25-44-47 FAX 33-04-42-25-29-29

R. LIMON
COMISION FEDERAL DE ELECTRICIDAD
KM 43.5 CARRETERA CARDEL-NAUTLA
MUN. DE ALTO LUCERO, VERA CRUZ 91680 MEXICO
91 297 40700 EXT 4326 FAX 91 297 40109

C.J. LIN
ATOMIC ENERGY COUNCIL
67, LANE 144 KEELUNG RD., SEC. 4
TAIPEI, TAIWAN 106 ROC
886-2-363-4180 EXT 762 FAX 886-2-366-0535
CJLIN@CC22.AEC.GOV.TW

T. LINK
PENNSYLVANIA STATE UNIVERSITY
107 STEIDLE BLDG.
UNIVERSITY PARK, PA 16802 USA
814-863-3512
TML110@PSU.EDU

M. LIVOLANT
INSTITUT DE PROT. ET DE SURETE NUC.
CEA / FAR - BP 6
FONTENAY AUX ROSES, CEDEX 92265 FRANCE
1-46-54-71-79 FAX 1-42-53-89-90
COLLIN@LUCIGER.CEA.FR

R. LOFARO
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, PO BOX 5000
UPTON, NY 11973-5000 USA
516-344-7191 FAX 516-344-3957
LOFARO@BNL.GOV

P. LOPEZ
NATIONAL COMM. OF NUCLEAR SAFETY
DR. BARRAGAN NO. 779 COL. NARVARTE
MEXICO CITY, 03020 MEXICO
525 590 50 54 FAX 525 590 75 08

W. LUCKAS
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, PO BOX 5000
UPTON, NY 11973-5000 USA
516-344-7562 FAX 516-344-2613

S. MAJUMDAR
ARGONNE NATIONAL LABORATORY
9700 S. CASS AVE.
ARGONNE, IL 60439 USA
708-252-5136 FAX 708-252-4798
MAJUMDAR@ANL.GOV

T. MARGULIES
U.S. EPA
MAIL CODE 6602J
WASHINGTON, DC 20460 USA
202-233-9774

A. MARION
NUCLEAR ENERGY INSTITUTE
1776 I ST., N.W., SUITE 300
WASHINGTON, DC 20006-3708 USA
202 739 8081 FAX 202 785 1898
AM@NEI.ORG

C. MARUSKA
ONTARIO HYDRO
700 UNIVERSITY AVE.
TORONTO, ONTARIO M5G 1X6 CANADA
416-592-5688 FAX 416-592-4483
CMARUSKA@HYDRO.ON.CA

B. MAVKO
JOSEF STEFAN INSTITUTE
JAMOVA 39
LJUBLJANA, 1000 SLOVENIA
286-61-1885-330 FAX 386-61-374919
BORUT.MAVKO@IJS.SI

D. McDONALD
AEA TECHNOLOGY
RISLEY, WARRINGTON
CHESHIRE, ENGLAND
01925-254512 FAX 01925-254536
DAVE.MCDONALD@AEAT.CO.UK

D. McCABE
OAK RIDGE NATIONAL LABORATORY
PO BOX 2008
OAK RIDGE, TN 32831-6151 USA
423-574-8010 FAX 423-574-5118

I. McNAIR
HM NUCLEAR INSTALLATIONS INSPECTORATE
ST PETER'S HOUSE, BALLIOL RD
BOOTLE, MERSEYSIDE L20 3LZ UK
44-151-951-4242

T. McNULTY
HM NUCLEAR INSTALLATIONS INSPECTORATE
ST PETER'S HOUSE, BALLIOL RD
BOOTLE, MERSEYSIDE L20 3LZ UK
44-151-951-3624 FAX 44-151-951-4942

R. MILLER
WESTINGHOUSE CNFD
3968 SARDIS ROAD
MURRYSVILLE, PA 15668 USA
412 374 2291 FAX 412 374 2382

E. MONAHAN
WESTINGHOUSE/SMPD
881 FIFTH STREET
NORTH HUNTINGTON, PA 15642 USA
412 374 4576

S. MONTELEONE
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, PO BOX 5000
UPTON, NY 11973-5000 USA
516 344-7235 FAX 516 344-3957
SMONTELE@BNL.GOV

R. MONTGOMERY
ANATECH CORP.
5435 OBERLIN DR.
SAN DIEGO, CA 92121 USA
619-455-6350 FAX 619-455-1094
ROB@ANATECH.COM

K. MORIYAMA
JAPAN ATOMIC ENERGY RESEARCH INST.
2-4 SHIRAKATA-SHIRANE
TOKAI-MURA, IBARAKI-KEN 319-11 JAPAN
81-29-282-5871 FAX 81-29-282-5570
MORI@SUN2SARL.TAKAI.JAERI.GO.JP

A. MOTTA
PENNSYLVANIA STATE UNIVERSITY
DEPT OF NUCLEAR ENG, 231 SACKETT BLDG.
UNIVERSITY PARK, PA 16802 USA
814-865-0036 FAX 814-865-8499
ATM2@PSU.EDU

M. MUHLHEIM
OAK RIDGE NATIONAL LABORATORY
PO BOX 2009, BLDG. 9201-3
OAK RIDGE, TN 37831 USA
423-574-0386 FAX 423-574-0382
M8M@ORNL.GOV

D. MURTLAND
SCIENCE & ENGINEERING ASSOCIATES, INC.
7918 JONES BRANCH DR., SUITE 500
MCLEAN, VA 22102 USA
703-761-4100 FAX 703-761-4105
DMURTLAND@SEABASE.COM

R. NANSTAD
OAK RIDGE NATIONAL LABORATORY
PO BOX 2008, 4500 S, MS 6151
OAK RIDGE, TN 37831-6151 USA
423 574-4471 FAX 423 574-5118
NANSTADRK@ORNL.GOV

D. NAUS
OAK RIDGE NATIONAL LABORATORY
PO BOX 2009
OAK RIDGE, TN 37831-8056 USA
423 574-0657 FAX 423 574-0651
DJN@ORNL.GOV

U. NAYAK
WESTINGHOUSE COMMERCIAL NUC. FUEL DIV.
PO BOX 355
PITTSBURGH, PA 15230-0355 USA
412 374 2241 FAX 412 374 2452

H. NOURBAKHSH
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, PO BOX 5000
UPTON, NY 11973-5000 USA
516-344-5405 FAX 516-344-5730

D. O'HAIR
WESTINGHOUSE NSA
129 ALEXANDER DRIVE
IRWIN, PA 15642 USA
412 374-5994
OHAIRD@CECIL.PGH.WEC.COM

G. ODETTE
UC SANTA BARBARA
DEPT. OF MECHANICAL ENGINEERING
SANTA BARBARA, CA 93106 USA
805 893-3525 FAX 805 893-8651

A. OHTA
MITSUBISHI HEAVY INDUSTRIES
3-1, MINATOMIRAI 3-CHOME, NISHI-KU
YOKOHAMA, 220-84 JAPAN
81-45-224-9637 FAX 81-45-224-9970
OHTA@ATOM.HQ.MHI.CO.JP

N. ORTIZ
SANDIA NATIONAL LABORATORIES
PO BOX 5800
ALBUQUERQUE, NM 87185 USA
505-844-0577 FAX 505-844-0955
NRORTIZ@SANDIA.GOV

D. OSETEK
LOS ALAMOS TECHNICAL ASSOCS., INC.
BLDG. 1, SUITE 400, 2400 LOUISIANA BLVD, NE
ALBUQUERQUE, NM 87110 USA
505-880-3407 FAX 505-880-3560

K. OSHIMA
TOSHIBA CORPORATION
C/O GENE M/C 726, 175 CURTNER AVE.
SAN JOSE, CA 95125 USA
408-925-6592 FAX 408-925-4945
OSHIMA@RDES.IEC.TOSHIBA.CO.JP

O. OZER
ELECTRIC POWER RESEARCH INSTITUTE
PO BOX 10412
PALO ALTO, CA 94303 USA
415-855-2089 FAX 415-855-2774
OOZER@EPRINET.EPRI.COM

J. PAPIN
INSTITUT DE PROT. ET DE SURETE NUC.
CEA CADARACHE
ST PAUL LEZ DURANCE, 13108 FRANCE
33-42-25-3463 FAX 33-42-25-6143

M. PARKER
ILLINOIS DEPT. OF NUCLEAR SAFETY
1035 OUTER PARK DR
SPRINGFIELD, IL 62704 USA
217-785-9854 FAX 217-524-5671

S. PATI
ABB COMBUSTION ENGINEERING NUCLEAR OPERATIO
2000 DAY HILL RD.
WINDSOR, CT 06070 USA
860-687-8043 FAX 860-687-8051
SATYAV.PATI

J. PELTIER
INSTITUT DE PROT. ET DE SURETE NUC.
60-68 AV. DU GENERAL LECLERC, BP 6
FONTENAY AUX ROSES, 92265 FRANCE
33-1-46-54-84.45 FAX 33-1-46-54-10-43
PELTIER@LUCIFER.CEA.FR

B. PENN
BROOKHAVEN NATIONAL LABORATORY
BLDG. 197C, PO BOX 5000
UPTON, NY 11973-5000 USA
516-344-7213 FAX 516-344-3021
PENN@BNL.GOV

W. PENNELL
OAK RIDGE, LOCKHEED MARTIN ENERGY RESEARCH
ENG'G MECHANICS & THERMAL SYS
OAK RIDGE, TN 37831-8045 USA
423-576-8571 FAX 423-574-0651
PO5@ORNL.GOV

A. PEREZ-NAVARRO
UNESA/UNIV. ALFONSO X
VILLANUEVA DE LA CANADA
, 28691 SPAIN
34-1-8109150 FAX 34-1-8109101
NAVARRO@.UAX.ES

K. PETTERSSON
KTH
STOCKHOLM, S-10044 SWEDEN
46-8-790-9194 FAX 46-8-207681
KJELLP@MET.KTH.SE

S. POPE
SCIENTECH
11140 ROCKVILLE PIKE, SUITE 500
ROCKVILLE, MD 20852 USA
301-468-6425 FAX 301-468-0883
SPOPE@SCIENTECH.COM

G. POTTS
GENERAL ELECTRIC CO.
PO BOX 780, CASTLE HAYNE RD, M/C K12
WILMINGTON, NC 28402-0780 USA
910-675-5708 FAX 910-675-6966

W.T. PRATT
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, PO BOX 5000
UPTON, NY 11973-5000 USA
516-344-2630 FAX 516-344-5730
PRATT@BNL.GOV

J. PUGA
UNESA
FRANCISCO GERVAS, 3
MADRID, 28020 SPAIN
34 1 567 4807

C. PUGH
OAK RIDGE NATIONAL LABORATORY
P.O. BOX 2009, MS-8067
OAK RIDGE, TN 37831 USA
423 574 0422 FAX 423 241 5005
PUG@ORNL.GOV

J. RASHID
ANATECH CORP.
5435 OBERLIN DR.
SAN DIEGO, CA 92121 USA
619-455-6350 FAX 619-455-1094
JOE@ANATECH.COM

S. RAY
WESTINGHOUSE
ENERGY CENTER, NOTHERN PIKE
MONROEVILLE, PA 15146 USA
412 374 2101 FAX 412 374-2045

R. REDA
GE NUCLEAR ENERGY
PO BOX 780, M/C J26
WILMINGTON, NC 28402 USA
910-675-5889 FAX 910-675-5879
REDAR@WLMPOL.WILM.GE.COM

K. REIL
SANDIA NATIONAL LABORATORIES
PO BOX 5800, MS 1139
ALBUQUERQUE, NM 87185-1139 USA
505-845-3050 FAX 505-845-3117
KOREIL@SANDIA.GOV

J. REITER
KNOLLS ATOMIC POWER LABORATORY
PO BOX 1032
SCHENECTADY, NY 12306 USA
518-395-4818

I. REMEC
OAK RIDGE NATIONAL LABORATORY
PO BOX 2008, BLDG. 6025 MS 6363
OAK RIDGE, TN 37831-6363 USA
423-574-7076 FAX 423-574-9619
I7R@ORNL.GOV

P. RICHARD
COMMISSARIAT A L'ENERGIE ATOMIQUE
BATTMENT 211 CE CADARACHE
ST PAUL LEZ DURANCE, 13108 FRANCE
33-62-25-31-54 FAX 33-42-25-47-59

D. RISHER
WESTINGHOUSE
P.O. BOX 355
PITTSBURGH, PA 15230 USA
412 374-5774 FAX 412 374-4011

G. ROCHAU
SANDIA NATIONAL LABORATORIES
PO BOX 5800, MS 0741
ALBUQUERQUE, NM 87185-0741 USA
505-845-7543 FAX 505-844-0955
GEROCHA@SANDIA.GOV

A. ROMANO
BROOKHAVEN NATIONAL LABORATORY
BLDG. 197C, PO BOX 5000
UPTON, NY 11973-5000 USA
516-344-4024 FAX 516-344-5266
ROMANO1@BNL.GOV

S. ROSINSKI
ELECTRIC POWER RESEARCH INSTITUTE
1300 HARRIS BLVD.
CHARLOTTE, NC 28262 USA
704-547-6123 FAX 704-547-6035
STROSMS@CHARLOTT.EPRI.COM

J. ROTHWELL
NUCLEAR SAFETY DIRECTORATE
ST. PETER'S HOUSE, BALLIOL RD.
BOOTLE, MERSYSIDE L20 3LZ UK
44-151-951-3751 FAX 44-151-951-3942

J. ROYEN
OECD NUCLEAR ENERGY AGENCY
LE SEINE ST GERMAIN, 12 BLVD DES ILES
ISSY LES MOULINEAUX, F 91130 FRANCE
33-1-4524-1052 FAX 33-1-4524-1110
JAQUES.ROYEN@OECD.ORG

D. SACCOMANDO
COMMONWEALTH EDISON
1400 OPUS PL, SUITE 500
DOWNERS GROVE, IL 60515 USA
630-663-7283 FAX 630-663-7155

O. SANDERVAG
SWEDISH NUCLEAR POWER INSPECTORATE
KLARABERGSVIADUKTEN 90
STOCKHOLM, 10658 SWEDEN
46-8-698-8463 FAX 46-8-661-9086
ODDBJORN@SKI.SE

Y. SASAKI
NUCLEAR POWER ENGINEERING CORP.
2F 3-13, 4-CHOME, TORANOMON
MINATO-KU, TOKYO 105 JAPAN
03-3434-4551 FAX 03-3434-9487

M. SATTISON
LOCKHEED MARTIN IDAHO TECH. CO., INEL
PO BOX 1625
IDAHO FALLS, ID 83401 USA
208-526-9626 FAX 208-526-2930
SBM@INEL.GOV

C. SAVAGE
JUPITER CORP.
2730 UNIVERSITY BLVD. W., SUITE 900
WHEATON, MD 20902 USA
301-946-8088 FAX 301-946-6539
BUZZ_SAVAGE@JUPITERCORP.COM

F. SCHMITZ
INSTITUT DE PROT. ET DE SURETE NUC.
CEA CADARACHE
ST PAUL LEZ DURANCE, 13108 FRANCE
33-42-25-7035 FAX 33-42-25-7679

S. SCHULTZ
YANKEE ATOMIC ELECTRIC CO.
580 MAIN STREET
BOLTON, MA 01740 USA
508 568-2131 FAX 508 568-3703
SCHULTZ@YANKEE.COM

M. SCHWARZ
INSTITUT DE PROT. ET DE SURETE NUC.
CEA CADARACHE
ST PAUL LEZ DURANCE, 13108 FRANCE

W. SHA
ARGONNE NATIONAL LABORATORY
9700 S. CASS AVE., BLDG. 308
ARGONNE , IL 60439 USA
630-252-3910 FAX 630-252-3250

R. SIMARD
NUCLEAR ENERGY INSTITUTE
1776 I ST., NW, SUITE 400
WASHINGTON, DC 20007 USA
202-739-8128

A. SINGH
ELECTRIC POWER RESEARCH INSTITUTE
3412 HILLVIEW AVE.
PALO ALTO, CA 94304 USA
415-855-2384 FAX 415-855-1026
AVSINGH@MSM.EPRI.COM

L. SLEGERS
SIEMENS/KWU
POSTFACH 101063
D 63067 OFFENBACH, GERMANY
06-91-807-3224 FAX 06-91-807-4567

J. SMITH
SANDIA NATIONAL LABORATORIES
PO BOX 5800
ALBUQUERQUE, NM 87185-0741 USA
505-845-0299 FAX 505-844-1648
JASMITH@SANDIA.GOV

K. SODA
JAPAN ATOMIC ENERGY RESEARCH INST.
2-2-2 UCHISAIWAICHO
CHIYODAKU, TOKYO 100 JAPAN
81-3-3592-2100 FAX 81-3-3592-2119
SODA@HEMS.JAERI.GO.JP

S. SONG
KOREA INSTITUTE OF NUCLEAR SAFETY
PO BOX 114 YUSONG
TAEJON, 305-600 KOREA
82-42-868-0222 FAX 82-42-861-0943
K056SSH@PINPOINT.KINS.RE.KR

K. ST. JOHN
YANKEE ATOMIC ELECTRIC CO.
580 MAIN ST.
BOLTON, MA 01740 USA
508-568-2133 FAX 508-568-3700
STJOHN@YANKEE.COM

P. STOOP
NETHERLANDS ENERGY RESEARCH FOUNDATION
WESTERDUJMWEG 3
PETTEN, 17552G NETHERLANDS
31-224-56-4342 FAX 31-224-56-3490
STOOP@ECN.NL

V. STRIZHOV
NUC. SAFETY INST., RUSSIAN ACADEMY OF SCI.
B. TULSKAYA 52
MOSCOW, 113191 RUSSIA
095 9580873 FAX 095 2302029

J. TAYLOR
BROOKHAVEN NATIONAL LABORATORY
BLDG. 130, PO BOX 5000
UPTON, NY 11973-5000 USA
516-344-7005 FAX 516-344-3957

T. THEOFANOUS
UCSB
SANTA BARBARA, CA 93106 USA
805-893-4900 FAX 805-893-4927
THEO@THEO.UCSB.EDU

C. THIBAULT
WYLE LABORATORIES
7800 HIGHWAY 20 WEST
HUNTSVILLE, AL 35806 USA
205-837-4411 FAX 205-837-3363

G. THOMAS
LAWRENCE LIVERMORE NATIONAL LABORATORY
PO BOX 808, 7000 EAST AVE
LIVERMORE , CA 94550 USA
510-423-3511 FAX 510-422-5497
THOMAS7@LLNL.GOV

O. THOMSEN
SOUTHERN CALIFORNIA EDISON
PO BOX 128
SAN CLEMENTE, CA 92672 USA
714-368-8087 FAX 714-368-8188

H. THORNBURG
CONSULTANT
901 S. WARFIELD DR.
MT AIRY, MD 21771 USA
301-829-0874 FAX 301-829-0874

P. TIPPING
SWISS FEDERAL NUCLEAR SAFETY INSPECTORATE (H
HSK, CH-5232
VILLIGEN, SWITZERLAND
41-56-310-3926 FAX 41-56-310-3855
TIPPING@HSK.PSI.CH

R. TREGONING
NAVAL SERVICE WARFARE CENTER
CODE G14
BETHESDA, MD 20084-5000 USA
301-227-4145 FAX 301-227-5576

P. TROY
MORGAN, LEWIS & BOCKIUS
1800 M ST., NW
WASHINGTON, DC 20036 USA
202-346-7536 FAX 202-467-7176
TROY7536@MLB.COM

J. TULENKO
UNIVERSITY OF FLORIDA
202 NUCLEAR SCIENCE CENTER, PO BOX 118300
GAINESVILLE, FL 32611-8300 USA
352-392-1401 FAX 352-392-3380
TULENKO@UFL.EPU

H. TUOMISTO
IVO INTERNATIONAL LTD.
RAJATORPANTIE 8
VANTAA, FINLAND
358-9-8561-2464 FAX 358-9-8561-3403
HARRI.TUOMISTO@IRO.FI

A. TURNER
DOMINION ENGINEERING, INC.
6862 ELM ST.
MC LEAN, VA 22101 USA
703 790-5544 FAX 703 790-0027
DEI@US.NET

H. UCHIDA
NUCLEAR POWER ENGINEERING CORP.
FUJITA KANKO TRANOMON BLDG. 6F
MINATO-KU, TOKYO 105 JAPAN
81-3-3438-3066 FAX 81-3-5470-5544

R. VALENTIN
ARGONNE NATIONAL LABORATORY
9700 S. CASS AVE., BLDG. 308
ARGONNE , IL 60439 USA
630-252-4483 FAX 630-252-3250

K. VALTONEN
FINNISH CENTRA FOR RADIATION & NUC. SAFETY
PO BOX 14
HELSINKI, 00881 FINLAND
358-0-759-881 FAX 358-0-7598-8382
KEIJO.VALTONEN@STUK.FI

M. VESCHUNOV
NUC. SAFETY INST., RUSSIAN ACADEMY OF SCI.
B. TULSKAYA 52
MOSCOW, 113191 RUSSIA
095 9552618 FAX 095 2302029

J. VILLADONIGA
CONSEJO DE SEGURIDAD NUCLEAR
JUSTO DORADO, 11
MADRID, 28040 SPAIN
34-1-3460240 FAX 34-1-3460588
JIVT@CSN.ES

G. VINE
ELECTRIC POWER RESEARCH INSTITUTE
2000 L ST NW, SUITE 805
WASHINGTON, DC 20036 USA
202-293-6347 FAX 202-293-2697
GVINE@MSM.EPRI.COM

N. WAECKEL
ELECTRICITE DE FRANCE SEPTEN
12-14 AV. DUTRIEVOZ
VILLEURBANNE, 69450 FRANCE
33-4-72-82-7571 FAX 33-4-72-82-7713

C. WELTY
ELECTRIC POWER RESEARCH INSTITUTE
3412 HILLVIEW AVE.
PALO ALTO, CA 94062 USA
415 855-2821 FAX 415 855-2774
CWELTY@EPRINET.EPRI.COM

K. WHITT
SOUTHERN NUCLEAR OPERATING CO.
40 INVERNESS CENTER PKWY
BIRMINGHAM, AL 35201 USA
205-870-6396 FAX 205-870-6108
KERMILT.W.WHITT@SNC.COM

D. WILKINSON
EPRI/NPG
3412 HILLVIEW AVENUE
PALO ALTO, CA 94303 USA
415 855-2426 FAX 415 855 2774

R. WITT
UNIVERSITY OF WISCONSIN - MADISON
531 ERB, 1500 ENGINEERING DR.
MADISON, WI 53719 USA
608 263 2760 FAX 608 262-6707
WITT@ENGR.WISC.EDU

G. WROBEL
ROCHESTER GAS & ELECTRIC CO.
89 EAST AVE.
ROCHESTER, NY 14649 USA
716-724-8070 FAX 716-724-8405

R. YANG
ELECTRIC POWER RESEARCH INSTITUTE
3412 HILLVIEW AVE.
PALO ALTO, CA 94304 USA
415-855-2481 FAX 415-855-2774
RYANG@EPRINET.EPRI.COM

L. YEGOROVA
RRC KURCHATOV INSTITUTE, NSI
KURCHATOV SQ. 1
MOSCOW, 123182 RUSSIA
7-095-196-7283 FAX 7-095-196-1702
ASMOLOV@OBAE.KIAE.SU

K. YOON
FRAMATOME TECHNOLOGIES
3315 OLD FOREST RD.
LYNCHBURG, VA 24503 USA
804 832-3280 FAX 804 832 3663
KYOON@FRAMATECH.COM

W.H. YOON
KOREA INSTITUTE OF NUCLEAR SAFETY
PO BOX 114 YUSONG
TAJEON, KOREA
82-42-861-4040 FAX 82-42-861-9945

R. YOUNGBLOOD
SCIENTECH
11140 ROCKVILLE PIKE
ROCKVILLE, MD 20852 USA
301-468-6425 FAX 301-468-0883
RYOUNG@SCIENTECH.COM

T. ZAMA
TOKYO ELECTRIC POWER CO.
1901 L ST., NW, SUITE 720
WASHINGTON, DC 20036 USA
202-457-0790 FAX 202-457-0810
ZAMA@WASH.TEPCO.CO

PROCEEDINGS OF THE
24TH WATER REACTOR SAFETY INFORMATION MEETING
OCTOBER 21-23, 1996

Contents - Volume 3

OVERVIEW OF NRC PRA RESEARCH PROGRAM

Mark A. Cunningham, Mary T. Drouin
Ann M. Ramey-Smith, Harold J. VanderMolen

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research

ABSTRACT

The NRC's research program in probabilistic risk analysis includes a set of closely-related elements, from basic research to regulatory applications. The elements of this program are as follows:

- Development and demonstration of methods and advanced models and tools for use by the NRC staff and others performing risk assessments;
- Support to agency staff on risk analysis and statistics issues;
- Reviews of risk assessments submitted by licensees in support of regulatory applications, including the IPEs and IPEEEs.

Each of these elements is discussed in the paper, providing highlights of work within an element, and, where appropriate, describing important support and feedback mechanisms among elements.

I. INTRODUCTION

The NRC's research program in probabilistic risk analysis includes a set of closely-related elements, from basic research to regulatory applications. The elements of this program are as follows:

- Development and demonstration of methods which improve existing techniques or fill gaps in the state of PRA technology, as well as advanced models and tools for use by the NRC staff and others performing risk assessments;
- Support to agency staff on risk analysis and statistics issues, with the largest recent activity being the development of guidance for using PRA in regulatory applications;
- Reviews of risk assessments submitted by licensees in support of regulatory applications, including the IPEs and IPEEEs.

Each of these elements is discussed in more detail below, providing highlights of work within an element, and, where appropriate, describing important support and feedback mechanisms among elements.

II. DEVELOPMENT AND DEMONSTRATION OF METHODS, MODELS, AND TOOLS

NRC's methods development and demonstration activities cover a wide range of topics. Some examples of these activities are summarized below, covering the gamut from the development of basic methods to fill gaps in present PRA technology to the delivery of application-oriented tools and models to NRC staff.

Human Reliability Analysis Research

It has been accepted for some time that failures in human performance are one of the principal sources of risk. Although techniques have been used in the past to quantify both pre-accident and post-accident human error, one of the remaining questions is how to treat "errors of commission." The NRC and its contractors are developing methods for treating human errors of commission. The general process will be to:

- Identify potentially unsafe actions and reasons for human failure events,
- Identify potential significant error forcing contexts (those conditions that "conspire" to cause operators to take unsafe actions), and
- Estimate the likelihood of potentially significant error forcing contexts and unsafe actions.[1]

Standby and Demand Stress Analyses

In most PRA calculations, component hardware failures are used to estimate an average unavailability. This average unavailability is adequate for assessment of total plant risk, but may require further delineation for some risk-based regulatory applications. Thus, an attempt is being made to separate failure modes for a standby (safety system) component into modes that result in component failure during the period when the component is in standby, and failure modes attributable to demand testing or operation of the component. Such separation of component failures will allow effective use of probabilistic techniques in decisions relating to improvements in surveillance test intervals in technical specifications and in evaluating additional surveillance to control risk from multiple component outages (plant configurations).

Accident Sequence Precursors

The NRC routinely evaluates operational events for safety significance and generic implications. Since the late 1970s, probabilistic analysis techniques have been used in such evaluations. This provides quantitative evaluations and also enforces a disciplined, comprehensive approach to event analysis.

As PRA techniques have evolved and increased in sophistication, so have these evaluations. In 1993, the original models were loaded into the SAPHIRE code package,[2] which permitted these evaluations to be performed on a personal computer. Then, 75 new train-level models were developed. These new models, called Simplified Plant Analysis Risk (SPAR) models, represent virtually all plants in the country. The 75 SPAR models have been loaded into a new computer code package called the Graphical Evaluation Module. This new module is part of the SAPHIRE code package and uses the same calculational models as the other PRA programs in SAPHIRE, but has a simplified user interface.

The NRC plans to improve the SPAR models in a number of respects over the next several years:

- The 75 models will be modified to include plant-specific dependencies and other features based on a review of the Individual Plant Evaluations and on responses to the Station Blackout Rule.
- An independent quality assurance (QA) review of the improved SPAR models will be performed.
- The models will be revised to incorporate the findings of the QA review. In addition, the common cause failure analyses and human reliability analyses will be enhanced, and support system models and uncertainty analysis capability will be added.
- External event analyses (seismic, fire, flood) will be added to the SPAR models. (Some actual operational events involve fires and floods, and these cannot be assessed quantitatively with the current models.)
- The models will be extended to consider low power/shutdown conditions. (Many operational events happen under these conditions, some of which could be risk significant.)
- The models will be expanded to consider Level 3 (public health consequences and risk). This will be

done to more correctly evaluate events which could involve relatively high consequences (e.g., containment bypass scenarios).

III. GUIDANCE FOR USE OF PRA IN REGULATORY ACTIVITIES

The NRC is now engaged in the development of regulatory guidance for power reactor licensees and staff with respect to the use of probabilistic risk analysis in regulatory activities. The overall policy direction for this guidance development is provided by the NRC's policy statements on safety goals[3] and PRA,[4] with the conceptual approach for the work described in a staff paper to the Commission.[5] This work, as well as the other PRA-related activities being undertaken by the staff, is managed via the staff's "PRA Implementation Plan."[6] The principal products of the guidance development work include:

- Regulatory guides providing guidance to licensees on acceptable methods for requesting changes to their licenses which are justified, at least in part, on PRA;
- Standard Review Plan (SRP) sections providing guidance to NRC staff on acceptable approaches for reviewing licensee-proposed changes; and
- Trial uses of the guidance via "pilot plant" studies involving both industry and staff.

IV. REVIEWS

On August 8, 1985, NRC issued a Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants[7] 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. NRC's Generic Letter (GL) 88-20[8] requested 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. Supplement 4 requested licensees to perform an IPE of external events and also report these results to the Commission.[9]

As a result of GL 88-20, 75 IPE submittals were received from the licensees covering 108 units and 74 IPEEE submittals will be received from the licensees covering 107 units (some licensees elected not to perform an IPEEE). There is a wealth of information contained in these reports. That is, beyond determining whether each licensee met the intent of GL 88-20, the information provides perspectives on what the collective results from the IPEs imply about the safety of U.S. nuclear power plants. Consequently, four separate but integrated programs were established, each of which is discussed below.

Key activities within the staff's IPE and IPEEE review process include:

- Review program Each IPE and IPEEE submittal is reviewed with a focus on whether the licensee's method was capable of identifying vulnerabilities, and therefore meets the intent of GL 88-20. The review considers (1) the completeness of the information and (2) the reasonableness of the results given the plant design, operation, and history. The staff expects to complete essentially all IPE reviews by the end of December 1996. With respect to the review of the IPEEE submittals, the staff has received approximately half of the IPEEE submittals (as of October 1996); the staff's reviews of IPEEE submittal is scheduled to be completed in December 1998.
- IPE database Information from the IPE submittals has been retrieved and entered into a database. This data primarily include information about plant design (e.g., system dependencies), core damage frequency (CDF) (e.g., accident sequences and their associated CDF, success criteria), and containment performance (e.g., plant damage states). The database is menu driven allowing user friendly access; this data base is now publicly available.

- IPE regional coordination For each IPE submittal, briefings are provided at the region to both regional headquarters personnel and the resident inspectors. These briefings include providing insights on the risk and safety important systems, components and human actions. In addition, perspectives are also provided on (1) the reasonableness of the results given the current design and operation, and (2) the potential strengths and weaknesses of the analysis.
- Insights program This program collects and documents the significant safety insights, based on the IPEs (and, at a later time, for IPEEEs), for the different reactor and containment types and plant designs. There are five major objectives of this program that involve providing perspectives on the following:

    - Impact of the IPE Program on Reactor Safety: perspectives on the number and type of vulnerabilities or safety issues, impact of the safety enhancements, and the generic applicability of the vulnerabilities and safety enhancements.
    - Reactor and Containment Design Perspectives: perspectives on the important design and operational features, methods and assumptions, and significant plant improvements that affect the core damage frequency and containment performance for different reactor and containment types.
    - Importance of the Operator's Role: perspectives on operator actions either consistently found important across the IPEs or found important due to plant-specific characteristics, on the influence of modeling assumptions and different methodologies, and on the causes of the variability in CDF estimation and containment performance analysis.
    - IPEs with Respect to Risk-Informed Regulation: perspectives on standards for a state-of-the-art PRA, on the quality of the IPEs (given the limited scope of the staff's review) as compared to a state-of-the-art PRA, and the potential role of the IPEs in risk-informed regulation.
    - Perspectives On Some Additional Items: (a) perspectives on the IPE results relative to the Commission's Safety Goals; (b) perspectives on the improvements that have been identified as a result of the Station Blackout Rule and analyzed as part of the IPE and the impact of these improvements on reducing the likelihood of station blackout; and (c) perspectives of the IPEs as compared to the perspectives gained from NUREG-1150.[10]

The document discussing the results of this work (NUREG-1560) is planned to be published in October 1996 for public comment. A workshop is planned to be in April 1997 to discuss the public comments. Following the review of public comment and conduct of the workshop, the staff's report will be published in final form.

REFERENCES

1.. M.T. Barriere et al., "Multidisciplinary Framework for Human Reliability Analysis with an Application to Errors of Commission and Dependencies," Brookhaven National Laboratory, NUREG/CR-6265, BNL-NUREG-52431, August 1995.

2. K.D. Russell et al., "Systems Analysis Programs for Hand-On Integrated Reliability Evaluations (SAPHIRE) Version 5.0, Idaho National Engineering Laboratory, NUREG/CR-6116, July 1994.

3. United States Nuclear Regulatory Commission (USNRC), "Policy Statement on Safety Goals for the Operation of Nuclear Power Plants," Federal Register, Vol. 51, p. 28044, August 4, 1986.

4. USNRC, "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement," Federal Register, Vol. 60, p 42622, August 16, 1995.

5. USNRC, "Framework for Applying Probabilistic Risk Analysis in Reactor Regulation," SECY-95-280, November 27, 1995.

6. USNRC, "Status Update of the Agency-Wide Implementation Plan for Probabilistic Risk Assessment," SECY-95-079, March 30, 1995.

7. United States Nuclear Regulatory Commission, "Policy Statement on Severe Reactor Accidents Regarding Future Design and Existing Plants," Federal Register, Vol. 50, p. 32138, August 8, 1985.

8. USNRC, "Individual Plant Examination for Severe Accident Vulnerabilities," Generic Letter No. 88-20, November 23, 1988.

9. USNRC, "Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities - 10 CFR 50.54(f)," Generic Letter No. 88-20, Supplement 4, June 28, 1991.

10. USNRC, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, December 1990.

CORE DAMAGE FREQUENCY (REACTOR DESIGN) PERSPECTIVES BASED ON IPE RESULTS*

Allen L. Camp[1], Susan E. Dingman[1], John A. Forester[1], Jeffrey L. LaChance[2], Mary T. Drouin[3]

[1]Sandia National Laboratories
[2]Science Applications International, Corp.
[3]U.S. Nuclear Regulatory Commission

This paper provides perspectives gained from reviewing 75 Individual Plant Examination (IPE) submittals covering 108 nuclear power plant units. Variability both within and among reactor types is examined to provide perspectives regarding plant-specific design and operational features, and modeling assumptions that play a significant role in the estimates of core damage frequencies in the IPEs. Human actions found to be important in boiling water reactors (BWRs) and in pressurized water reactors (PWRs) are presented and the events most frequently found important are discussed.

I. INTRODUCTION

In November 1988, the U.S. Nuclear Regulatory Commission (NRC) issued Generic Letter 88-20 requesting that all licensees perform an Individual Plant Examination (IPE) "to identify any plant-specific vulnerabilities to severe accidents and 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 response, 75 IPE submittals covering 108 nuclear power plant units were received by the staff. These IPE submittals were examined to determine which factors are most influential for core damage frequencies (CDFs).

An important aspect of the IPE program is to identify human actions important to severe accident prevention and mitigation. In this context, the human reliability analysis (HRA) is expected to be a critical component of the probabilistic risk assessments (PRAs) 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. Thus the human actions important in the IPEs are summarized in this paper and the degree of variability in the results of the HRAs is addressed. Of particular concern is the degree of variability in the quantification of similar human actions across different plants.

Perspectives regarding factors that have the largest influence on the IPE results are provided in Sections II through IV. More specific perspectives for one of the key factors, HRA, are provided in Sections V through VIII.

---

*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 DE-AC04-94AL85000.

II. GENERAL CDF PERSPECTIVES

Consistent with the results of previous NRC and industry risk studies, the IPEs indicate that the plant CDF is determined by a collection of many different sequences, rather than being dominated by a single sequence or failure mechanism. The accident class that is the largest contributor to plant CDF and the dominant failures contributing to that accident class vary considerably among the plants (e.g., some are dominated by loss-of-coolant accidents (LOCAs) while others are dominated by station blackout). However, for most of the plants, support systems are important to the results because support system failures can result in failures of multiple front-line systems. The support system designs and the dependencies of front-line systems on support systems vary considerably among the plants, which explains much of the variability in the IPE results. This variability is consistent with the perspectives of the Severe Accident Policy Statement, that is, that plant-specific factors are important in determining the risk for the various light water reactor (LWR) plants.

The CDFs reported in the IPE submittals for each of the individual LWR units are indicated by the dots in Figure1. As shown, the CDFs are lower on average for the BWR plants than for the PWR plants. Although the BWR and PWR results are strongly affected by the support system considerations discussed above, there are a few key differences among the plant types that cause this tendency for lower BWR CDFs. BWRs have more injection systems and can depressurize more easily than PWRs to use low pressure injection systems. This results in a lower average contribution from LOCAs for BWRs. Most PWRs can remove decay heat during transients either through the steam generators or by using primary system feed and bleed, which gives considerable redundancy for coping with transient sequences.

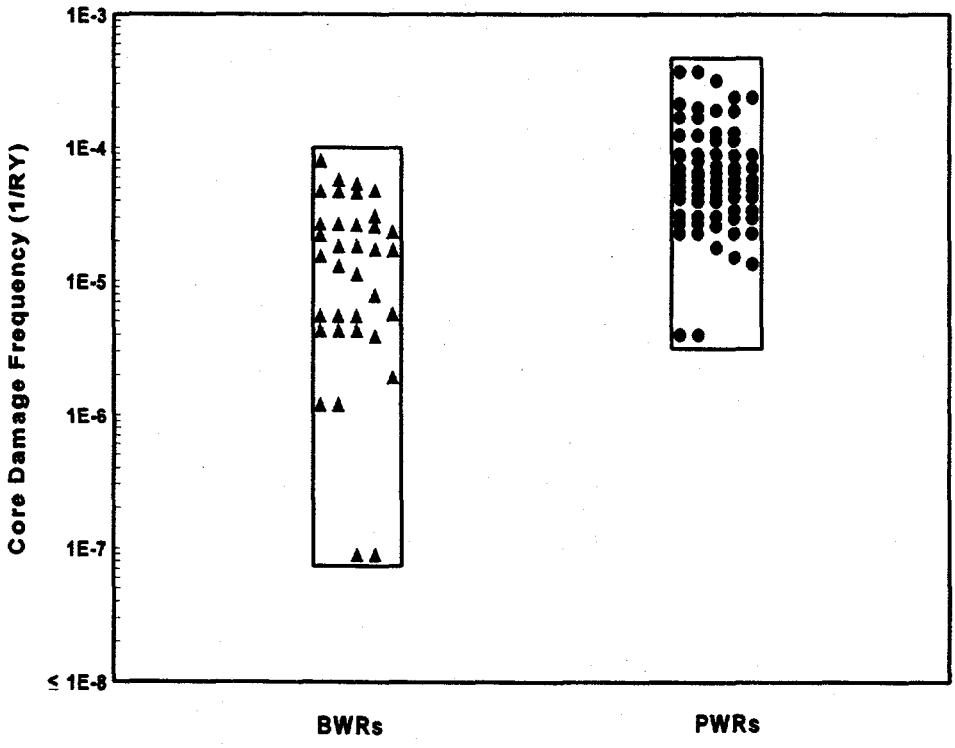


Figure 1 BWR and PWR CDFs as reported in the IPEs

However, if a LOCA is induced during a transient (e.g., reactor coolant pump (RCP) seal LOCA or stuck-open relief valve), injection is needed to maintain the reactor coolant system inventory. This is not as significant a problem for most BWRs because the normal means of decay heat removal is through injection systems, and as noted above, BWRs have more injection systems available than PWRs. However, many BWRs are more susceptible to transients with loss of containment heat removal because the sequence results in an adverse environment that fails emergency core coolant system (ECCS) pumps and other injection systems. This type of transient sequence is not generally important for PWRs. Station blackout sequences tend to be important contributors for both PWR and BWR plant groups because they result in the unavailability of numerous systems, leaving relatively few systems available to respond to the accident.

The results for some of the individual plants vary from the general trends noted above for some plants. As shown in Figure 1, there is considerable variability in CDFs within the BWR and PWR plant groups, which results in considerable overlap between the CDFs of the PWR and BWR plants. The variability is driven by a combination of factors, including plant design differences (primarily in support systems such as cooling water, electrical power, ventilation, and air systems), variability in modeling assumptions (including whether the models accounted for alternate accident mitigating systems), and differences in data values (including human error probabilities) used in quantifying the models. A summary of the key observations regarding the importance and variability of each accident sequence is provided in Table 1. Further details are provided in Sections III and IV for BWRs and PWRs, respectively.

III. BOILING WATER REACTOR PERSPECTIVES

The total CDFs for all operating BWRs in each of the BWR plant groups (grouped by design vintage) are shown in Figure 2. With the exception of a few outliers, the total CDFs for most BWRs fall within an order of magnitude range. The variability in the results is attributed to a combination of factors, including plant design differences, especially in support systems such as electrical power, cooling water, ventilation, and instrument air systems; modeling assumptions; and differences in data values, including human error probabilities. The largest variation exists in the BWR 3/4 group, which is the group with the largest number of plants. Variability in plant design and modeling assumptions results in several plants in the BWR3/4 group having CDFs below the remaining BWRs, and one plant (2 units) considerably below the others. Significantly smaller variability in the total plant CDFs was found for the other two BWR plant groups. A summary of the importance of the various accident classes to the BWR CDFs and the factors influencing the results is provided in Table 2.

A large variability exists for each BWR group in the contributions of the different accident classes to the total plant CDF. However, licensees in all three BWR groups generally found that three types of accidents are the major contributors to the total plant CDF: station blackouts, transients with loss of coolant injection, and transients with loss of decay heat removal (DHR). These three accident categories involve accident initiators and/or subsequent system failures that defeat the redundancy in systems available to mitigate potential accidents. Station blackouts involve a loss of both offsite and emergency onsite power sources (primarily diesel generators, but a few plants also have gas turbine generators) that fail most available mitigating systems except those that do not rely on AC power (the definition of station blackout for BWR 5/6s does not include failure of the diesel generator supplying the high pressure core spray (HPCS) system). Most of the accident sequences contributing to the transients with loss of coolant injection category involve the failure of high-pressure injection systems such as feedwater, RCIC, high pressure coolant injection (HPCI), and HPCS with a subsequent failure to depressurize the plant for injection by low-pressure injection systems. The failure to

depressurize effectively defeats a large part of the redundancy in the coolant injection systems. Support system failures (e.g., loss of cooling water systems, AC or DC buses, or instrument air) that impact many of the available accident mitigating systems contribute to the importance of this accident category and also to the transient with loss of DHR category. In all loss of DHR sequences involving transient or other initiators, redundancy in mitigating systems can be lost due to harsh environments in the containment prior to containment failure or in supporting structures following containment venting or failure.

Table 1 Overview of key IPE observations for LWRs

Accident Class	Key Observations
Transients	Important contributor for most plants because of reliance on support systems whose failure can defeat redundancy in front-line systems Both plant-specific design differences and IPE modeling assumptions contribute to variability in results. Major factors are: • capability to use alternate injection systems for BWRs • capability to use feed & bleed cooling and susceptibility to RCP seal LOCAs for PWRs
Station Blackouts	Significant contributor for most plants, with variability driven by: • number of emergency AC power sources • alternate offsite power sources • battery life • availability of firewater as injection sources for BWRs • susceptibility to reactor coolant pump seal LOCAs for PWRs
LOCAs	LOCAs are significant contributors for many PWRs BWRs generally have lower LOCA CDFs than PWRs • BWRs have more injection systems • BWRs can depressurize more readily to use low-pressure systems
Internal Floods	Small contributor for most plants, but significant for some because of plant-specific designs Largest contributors involve water system breaks that fail multiple mitigating systems (directly or through flooding effects)
Anticipated Transient Without Scram (ATWS)	Normally a low contributor to plant CDF because of reliable scram function and successful operator responses BWR variability mostly driven by modeling of human errors; PWR variability mostly driven by plant operating characteristics and IPE modeling assumptions
Bypass Sequences	Interfacing System LOCAs (ISLOCAs) are a small contributor to plant CDF for BWRs and PWRs because of low frequency of initiator Steam generator tube rupture normally a small contributor to CDF for PWRs because of opportunities for operator to isolate break and terminate accident

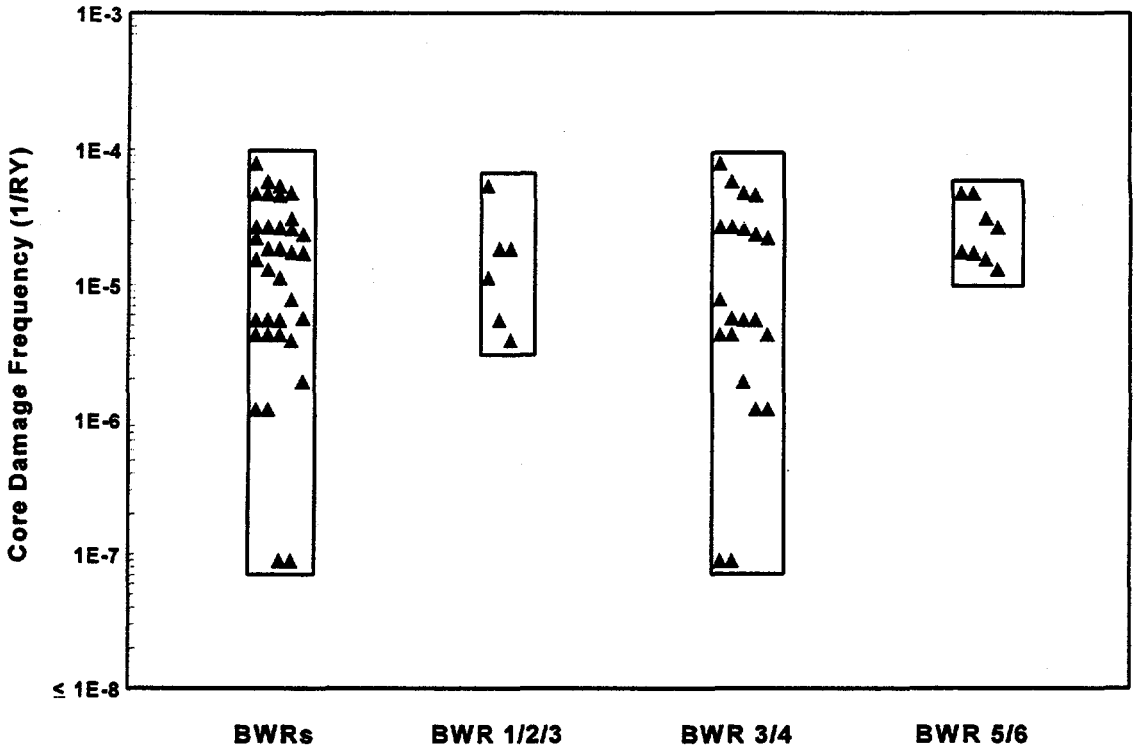


Figure 2 BWR plant group CDFs as reported in the IPEs

Lesser contributions from LOCAs, ATWS, and internal flooding are generally reported for all BWRs. These three accident categories are not important contributors primarily because they involve low frequency initiating events. However, there are a few BWRs that did report significant contributions from these accident categories. Although interfacing system LOCAs are potentially risk-significant contributors since the containment is bypassed, none of the licensees reported significant CDFs from this category of accident, again primarily because it involves low-frequency initiating events.

Many of the factors that impact the CDF contributions from these accident categories are the same for each plant group. However, there are factors worth highlighting that explain some of the differences across the BWR groups. For example, it was noted that some of the accident class frequencies for the BWR 1/2/3 plant group are generally lower than for the other two BWR plant groups, partially because isolation condensers appear to be more reliable than the RCIC systems that replaced them in the later BWR models. RCIC systems have more possible failure modes related to protective trip signals, ventilation failures, and pump operability requirements. Some of these failure modes are only prevalent in the BWR 5/6 IPEs and partially account for the higher station blackout CDFs for this group. However, it should be noted that some of the licensees with isolation condenser plants generally ignored the potential for recirculation pump seal failures, which would effectively defeat the use of the isolation condensers. Finally, the BWR 5/6 plants had lower contributions on average from sequences involving loss of high-pressure injection systems coupled with failure to depressurize the vessel for low-pressure injection than BWR 3/4s since the HPCS system in the BWR 5/6 plants tends to be more reliable than the HPCI system in the BWR 3/4 plants.

Table 2 Summary of CDF perspectives for BWRs

Accident Importance	Important Design Features, Operator Actions, and Model Assumptions
Station blackout accidents	
Important for most BWRs, regardless of plant group	Availability of AC-independent systems (i.e., high-pressure coolant injection system, diesel-driven firewater system, reactor core isolation cooling interface with suppression pool) Turbine bypass and isolation condenser capacity Battery life DC dependency for diesel generator startup Service water system design and heating, ventilating and air conditioning dependency AC power reliability (number of diesel generators, cross-tie capability between buses and units, diverse AC power sources)
Transients with loss of injection accidents	
Relatively unimportant at BWR 1/2/3 plants Important for most BWR 3/4 and 5/6 plants	Injection system dependencies on support systems, defeating redundancy Availability and redundancy of injection systems (e.g., control rod drive, motor-driven feedwater pumps, service cross-tie to residual heat removal, firewater system) Failure to depressurize influenced by operator direction to inhibit the automatic depressurization system
Transients with loss of decay heat removal accidents	
Important for most BWRs, regardless of plant group	Limited analysis to support success criteria — no credit for decay heat removal system (e.g., venting) Dependency of support systems for decay heat removal Net positive suction head problems with emergency core cooling systems on suppression pool Availability of injection system located outside containment and reactor building Capability of emergency core cooling systems to pump saturated water
Anticipated transient without scram accidents	
Relatively unimportant for most BWRs, regardless of plant group	Operator failure to initiate standby liquid control in timely manner, maintain main steam isolation valves open, control vessel level, and/or maintain pressure control Use of alternate means of injecting boron Availability of high-pressure core spray to mitigate
Loss-of-coolant accidents	
Relatively unimportant at all but one of the BWR plants	High redundancy and diversity in coolant injection systems
Interfacing systems LOCAs	
Not important for BWR plants	Compartmentalization and separation of equipment
Internal flood accidents	
Relatively unimportant at most BWRs, regardless of plant group	Plant layout: separation of mitigating system components and compartmentalization

IV. PRESSURIZED WATER REACTOR PERSPECTIVES

There is generally a larger variability in plant CDFs within the individual PWR plant groups than among plant groups. The Westinghouse (West) 3-loop plants generally have the highest CDFs, and the Babcock & Wilcox (B&W) plants generally have the lowest CDFs, with the CDFs for most of the B&W plants falling below the CDFs for the Westinghouse 3-loop plants. However, the difference in average CDFs between these two plant groups is about the same as the variability within either of the two plant groups. The variability in the PWR results is attributed to a combination of factors, including plant design differences (especially in support systems such as electrical power, cooling water, ventilation, and instrument air systems), modeling assumptions, and differences in data values (including human error probabilities). The largest variation exists in the Westinghouse 4-loop plant group, which is the group with the largest number of plants, but the other plant groups also show considerable variability. The Combustion Engineering (CE) plant group contains a 2-unit plant with a CDF well above the other plants in the group while the Westinghouse 4-loop plant group contains a 2-unit plant with a CDF considerably below the other plants in the Westinghouse 4-loop group. Figure 3 presents the CDFs for the different PWR plant groups.

A summary of the importance of the various accident classes for the PWR CDFs and the factors driving variability in the results is provided in Table 3. Considerable variability exists for each PWR group in the contributions of the different accident classes to the total plant CDF. However, licensees in all five PWR groups generally find that three types of accidents are the major contributors to the total plant CDF: transients, LOCAs, and station blackout. These three accident classes involve accident initiators and/or subsequent

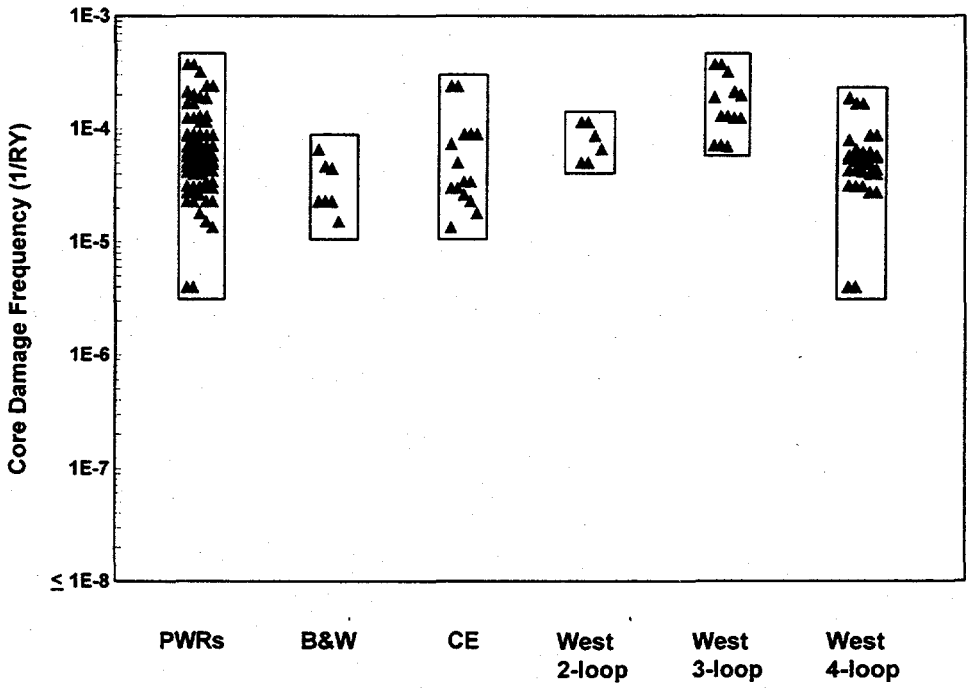


Figure 3 PWR plant group CDFs as reported in the IPEs

Table 3 Summary of CDF perspectives for PWRs

Accident Importance	Important Design Features, Operator Actions, and Model Assumptions
Station blackout accidents	
Important for most PWRs	Susceptibility to RCP seal LOCAs (o-ring design, alternate cooling, and seal LOCA model) Redundancy in emergency AC power sources (e.g., number of diesel generators) Battery life Use of plant operating data indicating low frequencies for loss of offsite power and high reliability of emergency diesel generators
Loss-of-coolant accidents	
Important for most PWRs	Whether manual action required for switchover to recirculation Alternate actions to mitigate LOCA (e.g., depressurizing the reactor coolant system using the steam generator atmospheric dump valves when high pressure injection fails during LOCA) Size of refueling water storage tank
Transient accidents	
Important for most PWRs	Susceptibility to RCP seal LOCAs (pump design, seal cooling capabilities, seal LOCA model) Capability for feed-and-bleed cooling Ability to cross-tie between systems/units Dependence on support systems (component cooling water and/or service water systems, heating, ventilation and air conditioning (HVAC) and instrument air) Ability to depressurize the steam generators and use condensate for heat removal Ability to supply long-term water to the suction for auxiliary feedwater/emergency feedwater (AFW/EFW)
Anticipated transients without scram accidents	
Relatively unimportant for most PWRs	Ability to mitigate by pressure control, boration, and heat removal
Interfacing system LOCAs	
Relatively unimportant for PWRs	Compartmentalization and separation of equipment
Steam generator tube rupture accidents	
Relatively unimportant to CDF for most PWRs	Credit for operator actions and equipment used to mitigate accidents
Internal flood accidents	
Important for some PWRs	Plant layout: separation of mitigating system components and compartmentalization

system failures that defeat the redundancy in systems available to mitigate potential accidents. Lesser contributions are generally reported for ATWS, steam generator tube ruptures, ISLOCAs, and internal flooding. However, a few PWRs do report significant contributions from these accident classes, and steam generator tube ruptures are found to be significant contributors for the Westinghouse 2-loop plants.

Some of the factors that have the largest influence on the CDF contributions reflect concerns that are more prevalent in a particular PWR plant group, but most reflect design differences or modeling assumptions that are applicable to all of the PWR plant groups. Differences that tend to reflect design differences among the PWR plant groups are summarized below.

One of the most important factors affecting PWR CDFs is the susceptibility to RCP seal LOCAs for transient and station blackout sequences. To prevent core damage in RCP seal LOCA sequences, inventory makeup is required in addition to core heat removal. Both the B&W and CE plant groups have less susceptibility to RCP seal LOCAs in the IPE models because most plants in these groups have a seal design that the industry believes to be less prone to seal damage. However, there is at least one plant in each group that has indicated a significant CDF contribution that involves RCP seal LOCAs. This lower susceptibility to RCP seal LOCAs in the B&W and CE IPEs tends to cause lower contributions from transient and station blackout sequences for the B&W and CE plants relative to the Westinghouse plants.

Because the probability of RCP seal LOCAs is generally lower in the B&W and CE IPEs, these plants tend to show more benefit than Westinghouse plants from plant characteristics that improve the reliability of heat removal through the steam generators (e.g., reliable or redundant feedwater pumps, sustained source of water for feedwater, or longer battery life for control of auxiliary feedwater during station blackout). The importance of these factors is less for many Westinghouse plants because RCP seal LOCAs lead to core damage despite the cooling provided through the steam generators.

Feed-and-bleed cooling is often an important backup for transient sequences with loss of steam generator heat removal. All but one of the B&W plants have high- pressure injection pumps with high shutoff heads that can provide adequate flow for feed-and-bleed cooling even at the safety relief valve setpoint. Some CE plants do not have power-operated relief valves (PORVs) or other means to depressurize. The inability to feed and bleed for these CE plants is generally compensated for by the ability to depressurize the steam generator and use condensate for cooling. Therefore, the lack of PORVs has less influence on the IPE results than might otherwise be expected.

The final factor that tends to show similarities within plant groups is the configuration for ECCS recirculation. Plants with a higher degree of automation in performing the switchover and plants that can achieve high-pressure recirculation with fewer components operating tend to have lower failure rates resulting from the switchover to recirculation. For the plants with manual switchover, variability in the assessment of operator performance in performing the action is also important. The B&W plants require manual actions for ECCS switchover from injection to recirculation, and the high-pressure injection pumps must draw suction from the low-pressure pumps to operate in the recirculation mode. The CE plants have automatic switchover, and the high-pressure pumps can draw water directly from the sump rather than drawing suction from the discharge of the low-pressure pumps. The Westinghouse plants are mixed on these factors. Some Westinghouse plants require operator actions to perform the switchover while other plants have automatic switchover. For some Westinghouse plants, the high-pressure pumps draw directly from the sump during recirculation, while at other plants the high-pressure pumps must be aligned to draw suction from the low-pressure pumps (which draw from the sump).

V. HUMAN ACTIONS GENERALLY IMPORTANT FOR BWRs

Table 4 lists the most important human actions identified in the staff's review of all 27 BWR IPE submittals (covering 35 units), along with the percentage of all BWR IPEs finding the action important, and the percentage of IPEs finding the action important as a function of BWR class. Of the 27 submittals reviewed, five are in the BWR 1/2/3 class (covering six units), 15 are in the BWR 3/4 class (covering 21 units), and seven are in the BWR 5/6 class (covering eight units).

Only a few specific human actions are regularly found to be important across all the BWR IPEs. That is, while many different events are indicated as being important, relatively few are important to most of the IPEs. Thus, the staff attempted to group the operator actions according to the function to be accomplished. For example, events related to aligning an alternative injection source during transients, LOCAs, and station blackouts (SBOs) are considered important to several licensees. Even though the alternative systems used ranged from firewater to suppression pool cleanup, the function accomplished by performing the action is similar. In order to help capture the general types of events that are important to BWRs, the staff grouped these actions with similar functions and presented them in Table 4 along with other important individual operator actions.

Manual depressurization of the vessel[1] so that low-pressure injection systems can be used after a loss or unavailability of high-pressure injection systems is important in most BWR IPE submittals. This action is particularly important in some plants for long-term SBO sequences where depressurization is required to allow injection from firewater systems, after loss of steam-driven systems such as reactor core isolation cooling (RCIC). This human action is important largely because of the fact that most plant operators are directed to inhibit automatic actuation of the ADS by the plant emergency operating procedures (EOPs). Thus, operators must manually depressurize the vessel when injection from low-pressure systems is required to cool the core. The percentage of total CDF accounted for by cutsets including this event ranged from 1 to 44%.

While human actions related to an ATWS are frequently found in the licensees' lists of the top ten important events, the contribution of ATWS events to overall CDF is usually relatively small. The human action to inhibit the ADS is important in the ATWS sequences of several submittals. In fact, some licensees assume that because of the instabilities created under low-pressure conditions during an ATWS, core damage will occur if the operators fail to inhibit the ADS. Given this position, it is somewhat surprising to find that only ~20% of the BWR licensees identify inhibition of the ADS as being important. The low percentage results in part from how licensees model ADS inhibition. Many licensees assume that failure to perform this action has a very low probability, or they do not model it at all. Other licensees model the failure to inhibit the ADS as resulting in core damage only if it occurs in conjunction with a second failure (e.g., failure of SLC or failure of low-pressure injection flow control). Such a model can reduce the importance of this type of accident sequence and thus the importance of the related human errors. The remaining licensees model the failure to inhibit the ADS during an ATWS as directly resulting in core damage. This human error is noted as being important for approximately 50% of the licensees that model ADS inhibition in any fashion.

---

[1]Section VII discusses the variability in HEPs for this event across the BWR IPEs.

Table 4 Important human actions and percentage of BWR IPEs finding the action important

Important human actions	Percentage of BWR IPEs finding the action important			
	All BWR IPEs	BWR 1/2/3s	BWR 3/4s	BWR 5/6s
Perform manual depressurization	~80%	~80%	~80%	~60%
Containment venting	~55%	~35%	~60%	~60%
Align containment or suppression pool cooling	~55%	~70%	~50%	~50%
Initiate standby liquid control (SLC)	~50%	~70%	~50%	~40%
Level control in ATWS	~25%	~50%	~30%	0%
Align/initiate alternative injection	~25%	~30%	~30%	~15%
Recover ultimate heat sink	~20%	~20%	~20%	~25%
Inhibit automatic depressurization system (ADS)	~20%	~20%	~20%	~25%
Miscalibrate pressure switches	~15%	~20%	~15%	~10%
Initiate isolation condenser	N/A	~85%	N/A	N/A
Control feedwater events (e.g., loss of instrument air)	~15%	~15%	~20%	~15%
Manually initiate core spray or other low-pressure system	~15%	~20%	~20%	0%
Miscalibrate low-pressure core spray permissive	~10%	~20%	~15%	0%
Provide alternative room cooling (in the event of a loss of HVAC)	~10%	0%	~5%	~25%
Recover injection systems	~10%	0%	~15%	~15%

Two other ATWS-related events are found to be important by several licensees. The operator action to initiate boron injection during an ATWS is important in ~50% of the BWRs, and ~25% identify level control as being important. As with ADS inhibition, the modeling of these events partially impacts their importance to core damage. For example, some licensees model early initiation of SLC, while others consider both early and late initiation times. The initiation times (important in calculating the HEPs) are based on avoiding adverse

conditions, such as high suppression pool temperatures, and are somewhat variable (ranging from one minute to 45 minutes). Some licensees take credit for alternative means of injecting boron, while others take credit for level control as a means of reducing core power to acceptable levels following SLC failure. All of these variables can contribute to the importance of the failure to manually initiate SLC. Modeling of level control is highly variable, with several different factors influencing the modeling. Whether these actions are important for particular licensees is, to some extent, a function of the contribution of the ATWS sequences to overall CDF. The contribution of these events to CDF is usually in the range of 1 to 3 %.

Many licensees identify human actions related to decay heat removal as being important. Two of the most frequently identified important actions in BWRs relate to decay heat removal (DHR) sequences in transients and LOCAs. With a loss of the power conversion system and safety relief valves (SRVs) open, containment temperature and pressure must be controlled. The actions to provide some form of containment or suppression pool cooling, or to vent containment when adequate cooling can not be provided, are important in more than 50% of the IPE submittals. Plant characteristics and modeling differences are important factors in determining the impact of these human actions.

Plants require DHR actuation before adverse conditions are reached. These conditions can range from reaching a high suppression pool temperature that results in a loss of emergency core coolant system (ECCS) pumps, to reaching a high containment pressure that results in closure of SRVs that are required to remain open to maintain the vessel at low-pressure (for coolant injection from low-pressure systems). However, some licensees did not model the failure of DHR as leading to a failure in the ability to inject water into the vessel from the ECCS or from alternative injection systems. In addition, some licensees identified the steam released following containment failure as having a negative impact on the operability of injection systems. In addition, some licensees do not model venting at all. They either do not have reliable venting systems, do not have a strong need to vent, or simply do not take credit for venting. The contribution from these events to CDF generally ranges from 1 to 5 %, with one licensee indicating a 12% contribution.

VI. HUMAN ACTIONS GENERALLY IMPORTANT FOR PWRs

Table 5 lists the most important human actions identified in the staff's review of all 48 PWR IPEs submittals, along with the percentage of all PWR submittals finding the action important, and the percentage of submittals finding the action important as a function of PWR class.

As with BWRs, only a few human actions are regularly found to be important across all PWR submittals. The human action most consistently important for PWRs is the switchover to recirculation during LOCAs. Other human actions frequently important include feed and bleed, and actions associated with depressurization and cooldown. Only these three actions are important in more than 50% of the submittals. They are discussed in more detail below, along with several other actions frequently found to be important by the licensees.

Switchover to recirculation on low ECCS level is important for LOCA sequences in most submittals for plants with semi-automatic or manual switchover. All ten CE plants (15 units) have an automatic switchover, as do four of the other plants. For the 35 plants (58 units) that require operator actions (either completely manual

Table 5 Important human actions and percentage of PWR submittals finding action important

Important human actions	Percentage of IPEs finding event important					
	All PWRs	B&W	CE	West 2-loop	West 3-loop	West 4-loop
Switchover to recirculation (plants with manual or semi-automatic switchover)	~80%	~85%	N/A	100%	~55%	~90%
Feed-and-bleed	~60%	~45%	~60%	~70%	~45%	~70%
Depressurization and cooldown	~50%	~60%	~30%	100%	~70%	~50%
Use of backup cooling water systems	~40%	~45%	~30%	~35%	~60%	~30%
Makeup to tanks for water supply	~35%	~30%	~20%	~35%	~40%	~40%
Restoration of room cooling (HVAC)	~30%	~15%	~50%	~35%	~30%	~30%
Restoration of main feedwater (MFW) or condensate to steam generators (SGs)	~30%	~30%	~35%	~35%	~50%	~30%
Proper control of AFW or EFW	~25%	~30%	~40%	~35%	0%	~30%
RCP Trips	~25%	~45%	~35%	~35%	~15%	~20%
Pre-initiators	~25%	0%	~50%	0%	~25%	~20%
ATWS reactivity control	~20%	0%	~20%	0%	~10%	~35%
Water supply for AFW or EFW	~15%	0%	~40%	~35%	~10%	~5%
Initiation of AFW or EFW	~15%	0%	~50%	0%	~10%	~10%

or semi-automatic) to complete the switchover, ~80% of the submittals find this action to be important. One possible reason some licensees fail to find this action important may be the fact that the sizes of refueling water storage tanks (RWSTs) vary from plant to plant. Licensees with plants that have larger RWST capacities may model the small LOCA and long-term transient sequences as not requiring the switchover to recirculation cooling, thereby lessening the importance of the recirculation function and hence human actions related to

recirculation cooling. Additionally, some licensees model RWST refill as the action preferred over recirculation cooling, particularly in small LOCA and long-term transient cooling situations. This again lessens the overall importance of recirculation cooling and the corresponding related human actions. For licensees that find the switchover to recirculation to be an important operation (and report the related contribution to total CDF), the contribution to CDF ranges from less than 1% in several cases to as much as ~16%, with an average contribution of ~6%.

Many licensees identify the initiation of the feed-and-bleed operation as being important. This event is important in transient and steam generator tube rupture (SGTR) sequences when all feedwater has failed. In addition, a few licensees find the establishment of an reactor coolant system (RCS) bleed path with one power operated relief valve (PORV) to be important in small LOCAs. In all, about 60% of the submittals indicate that feed-and-bleed is one of the more important events. Some licensees may fail to find feed-and-bleed important for a variety of reasons that are interrelated and not easily discernible. For instance, the relative reliability of each plant's AFW or EFW system is a factor since it is only in sequences where AFW or EFW has failed that feed-and-bleed becomes another important action in the in-depth defense to provide core cooling. Thus, accident sequences involving AFW/EFW failure (and thus the need to use the feed-and-bleed function) can vary considerably in frequency, thereby affecting the overall importance of the feed-and-bleed function. Specific support system dependencies can also be important to the overall feed-and-bleed reliability and hence the importance of this human action. For plants with a higher susceptibility of failing feed-and-bleed because of support system failures, this mode of cooling is less reliable, and the human action of feed-and-bleed operation can be less important.

Additionally, many licensees spent considerable effort to model the ability to depressurize the plant and use condensate as yet another way to achieve core cooling. Taking credit for such action further lessens the overall importance of feed-and-bleed function and the related human action. Other factors related to the success criteria for feed-and-bleed, as well as the HEPs themselves, can contribute to the relative importance of this mode of cooling and the related human action. The CDF contribution for this event ranges from less than 1% to 11%, with most submittals showing relatively small contributions from this event, resulting in an average total CDF contribution of about 4%.

The depressurization and cooldown operation, in order to use available sources of core cooling (and in many cases to lessen SGTR leakage), is found to be important by more than half of the licensees. This action usually (but not always) involves depressurizing the steam generators to cool the RCS and is found to be important in all types of sequences except ATWS. It is most frequently deemed important in SGTR sequences. As a result, 52% of the licensees find this human action important. As discussed above regarding the feed-and-bleed function, licensees may neglect to find depressurization and cooldown important for numerous interrelated reasons (including those described for the feed-and-bleed event). Additionally, not all of the plants model this mode of cooling, in some cases because of the relatively low capacity to depressurize the SGs in some scenarios (depending on PORV, atmospheric dump valve, or other equipment sizes). The CDF contribution for this event ranges from less than 1% to ~7%, and is similar to feed-and-bleed. Most submittals show relatively small contributions from this event, resulting in an average total CDF contribution of approximately 4%.

None of the remaining human actions are important in more than 40% of the submittals, and none of them consistently contributes significantly to CDF. As shown in Table 5, the remaining human actions are not important in a large percentage of the submittals. Recovering and using backup cooling systems, supplying makeup for injection sources, and recovering loss of room cooling are important for accident sequences in

approximately one-third of the submittals. Several actions related to restoration and appropriate use of MFW and AFW systems are found to be important in several submittals, and RCP trips upon loss of seal cooling is important in about 25% of the submittals. Similar to the BWRs, pre-initiator events, including both miscalibration and restoration errors, are found important in some submittals. The miscalibration errors tend to involve the traditional instruments such as level, pressure, and temperature sensors and transmitters, but the restoration errors tend to vary across submittals. Examples of important restoration errors include those associated with AFW and EFW systems, diesel generators, and several unique events such as leaving a nitrogen station manual valve closed and removing a jumper in the reactor protection system after refueling.

VII. VARIABILITY IN HUMAN ERROR PROBABILITIES

Numerous factors can influence the quantification of HEPs and introduce significant variability in the resulting HEPs, even for essentially identical actions. General categories of such factors include plant characteristics, modeling details, sequence-specific attributes (e.g., patterns of successes and failures in a given sequence), dependencies, HRA method and associated performance shaping factors (PSFs) modeled, application of HRA method (correctness and thoroughness), and the biases of both the analysts performing the HRA and the plant personnel from whom selected information and judgments are obtained. Although most of these factors introduce appropriate variability in results (i.e., the derived HEPs reflect "real" differences such as time availability and scenario-specific factors), several have the potential to cause invalid variability. A discussion of both appropriate and inappropriate influences is presented below, followed by a discussion of the variability in the HEPs for a specific event.

In order to examine the variability in HRA results from the IPEs and to assess the extent to which variability in results is caused by real versus artifactual differences, the staff examined HEPs from several of the more important human actions appearing in the submittals across plants. However, since the staff reached the same general conclusion after examining several important human actions for the BWRs and PWRs, this summary report presents the results from the examination of a single important human action. Discussions of the variability in HEPs for several other human actions from BWRs and PWRs are presented in the body of the main report.

Figure 4 presents the HEPs used in various BWR submittals for failure to depressurize the vessel during transients. As shown in the figure, a relatively large variability exists across the submittals for this event. However, there appears to be reasonable explanations for much of the variability in the HEPs. For values on the high end of the continuum, the events modeled appear to be special cases of depressurization. For example, the high value for Nine Mile Point 1 (N-1) involves depressurization using main steam isolation valves and the condenser, which is apparently not typically modeled. The high value for Peach Bottom 2&3 (PB) and the next to the highest value for Limerick 1&2 (LIM) pertain to the case in which a controlled depressurization is needed to allow use of the condensate system. The highest value for Limerick 1&2 (LIM) pertains to a recovery of a failed automatic depressurization. While the justification for the high values for Big Rock Point (BRP) is not apparent, it is unique relative to the other BWRs in that the plant has some characteristics similar to PWRs. The reason for the high value for Cooper (COP) is also not obvious, but the large range of values for that plant apparently relates to the number of SRVs to be used for depressurization.

The explanations for the large difference (approximately one and one-half to two orders of magnitude) between the HEP values in the middle range appear to be related, at least in part, to dependencies and initiator- and sequence-specific factors. Several licensees, such as Nine Mile Point 1 (N-1), Dresden 2&3 (DRE), Fermi 2 (FER), and Limerick 1&2 (LIM), conducted relatively detailed analyses and apparently derived

multiple values in order to account for specific conditions. These specific conditions include LOOPs, SBOs, loss of DC power, use of turbine bypass valves for depressurization, and loss of feedwater and standby feedwater. Nevertheless, while much of the variability in the middle range of values is clearly explainable, some differences are less clear. For example, the generally lower values for Fermi 2 (FER) and Limerick 1&2 (LIM) relative to those from Nine Mile Point 1 (N-1) and Dresden 2&3 (DRE) are not explainable in a straightforward manner, but may very well result from valid, plant-specific characteristics.

Finally, the reasons for the relatively low HEP values at Cooper (COP), Duane Arnold (DA), Fitzpatrick (FIT), Vermont Yankee (VY), and Susquehanna 1&2 (SUS) are not clear. It can be argued that at least the top three or four values from these submittals fall within an acceptable range. It may also very well be the case that plant-specific characteristics support the HEPs on the lower end of the continuum. For example, the relatively low value for Cooper (COP) is for a long-term DHR sequence in which operators have up to 4 hours to depressurize. The lowest value, from Susquehanna (SUS), is clearly an outlier, but this value is consistent with many of that plant's HEP values and is a direct function of the HRA methodology used in the Susquehanna IPE.

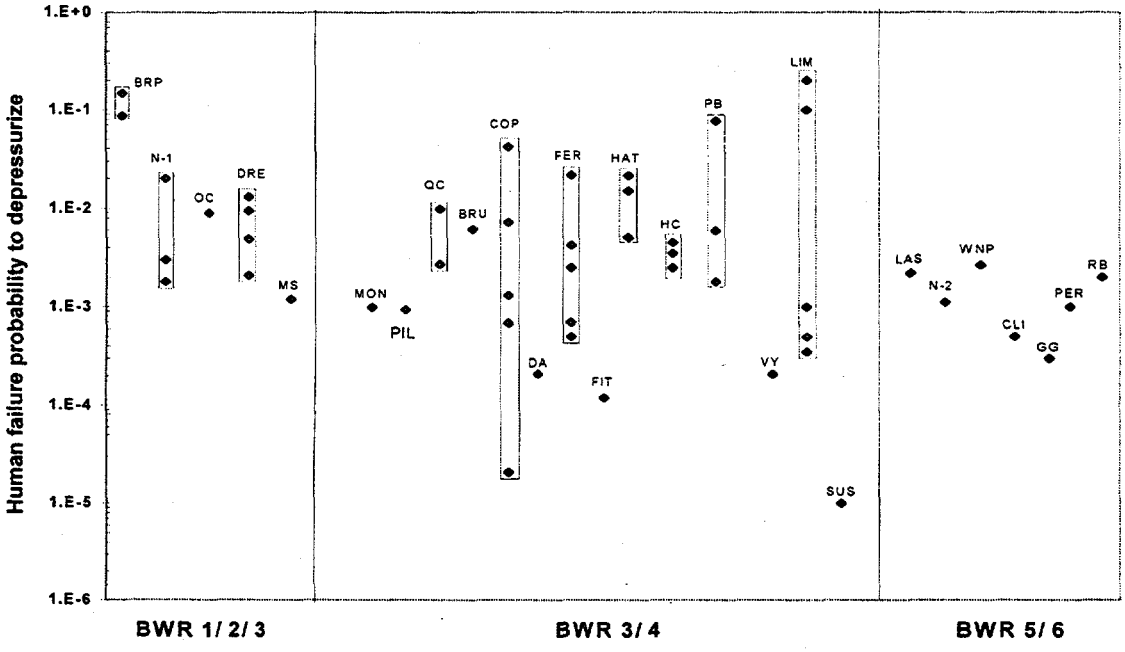


Figure 4 HEPs for depressurization failure by BWR class.[2]

[2] HEPs shown on figure are on a submittal basis, and not necessarily a plant-unit basis.

At least some of the variability in HEP values can arise as an artifact of the way in which HRA methods are applied. Nonetheless, the main point to be derived from examining the HEPs for specific actions across plants, is that, in most cases, it also appears that there are reasonable explanations for much of the variability in HEPs and in the results of the HRAs across the different IPEs. However, such an assertion does not necessarily imply that the HEP values are generally valid. Reasonable consistency can be obtained in HRA without necessarily producing valid HEPs. An HEP is only valid to the extent that a correct and thorough application of HRA principles has occurred. For example, if a licensee simply assumes (without adequate analysis) that their plant is "average" in terms of many of the relevant PSFs for a given event, but appropriately considers the time available for the event in a given context, the value obtained for that event may be similar to those obtained for other plants. Yet, the resulting value may be optimistic or pessimistic relative to the value that would have been obtained if the licensee had conducted a detailed examination of the relevant plant-specific factors. Thus, to reiterate, consistency does not necessarily imply validity. In addition, because many of the licensees failed to perform high-quality HRAs, it is possible that the licensees obtained HEP values that are not appropriate for their plants.

VIII. SIMILARITIES AND DIFFERENCES IN HUMAN ACTION OBSERVATIONS ACROSS BWRs AND PWRs

Given the basic differences between BWRs and PWRs, the preceding discussion has for the most part provided separate observations regarding the submittals for the two different plant types. Nevertheless, the obvious commonalities across the plant types, prompt an examination of potential similarities or differences in the operational and HRA-related observations:

- Neither BWR nor PWR submittals show a broad consistency in terms of which human actions are found to be important. Given the numerous factors that can influence the IPE results, and the fact that functional redundancy creates the opportunity for quite a few operator actions to be taken to mitigate an accident scenario in both BWRs and PWRs, there is no reason to expect more consistency in what is found to be important for one type of plant as opposed to the other.

- Of the events frequently found to be important in BWRs and PWRs, the only similar actions are those related to depressurization and cool down.

- Events related to aligning or recovering backup cooling water systems (e.g., service water) are found to be important in approximately one-third of both BWRs and PWRs.

- In both BWRs and PWRs, no individual human action appears to account for a large percentage of the total CDF across multiple submittals. Taken together, however, human actions are clearly important contributors to operational safety.

- With the exception of the licensees using the IPE Partnership (IPEP) methodology, there is no indication that particular HRA methods are applied more frequently to one type of plant than another. Thus, except for the IPEP plants, there is no reason to expect that any general differences in the results of the PRAs for the two different plant types is related to HRA method (or to any of the more general influencing factors). The IPEP methods are primarily applied to PWRs.

In summary, it seems that most of the differences in the HRA results from the BWR and PWR submittals relate (not surprisingly) to the differences in the systems used in the two types of plants. In terms of more

methodological aspects, general patterns of results, and the overall importance of humans in operating the plants, BWRs and PWRs are reasonably similar.

Containment Performance Perspectives Based on IPE Results*

J. R. Lehner, C. C. Lin, W.T. Pratt
Brookhaven National Laboratory
Building 130, P.O. Box 5000, Upton, NY 11973-5000

M. Drouin
U.S. Nuclear Regulatory Commission
Two White Flint North, 11545 Rockville Pike, North Bethesda, MD 20852

ABSTRACT

Perspectives on Containment Performance were obtained from the accident progression analyses, i.e. level 2 PRA analyses, found in the IPE submittals. Insights related to the containment failure modes, the releases associated with those failure modes, and the factors responsible for the types of containment failures and release sizes reported were gathered. The results summarized here are discussed in detail in volumes 1 and 2 of NUREG 1560.

1. BACKGROUND

Containment Performance perspectives were gathered from the level 2 analyses described in the Individual Plant Examination (IPE) submittals. Insights related to the containment failure modes, the releases associated with those failure modes, and the factors responsible for the types of containment failures and release sizes reported were obtained. Complete results are discussed in NUREG-1560[1] and summarized here.

The accident progression analyses methods and results reported in the IPE submittals were inspected to gain insights and perspectives with respect to: (1) the important design and operational features that affect containment performance for different reactor and containment types, (2) the influence of methods and assumptions on the results reported for different containments, and (3) what plant improvements for increasing containment performance were suggested by the licensees and their contractors performing the IPEs.

For purposes of presenting the perspectives obtained, the containments are divided up into five classes, i.e, the three boiling water reactor (BWR) containment types, Mark I, Mark II and Mark III, and the two pressurized water reactors (PWR) types, large dry containments (including those at subatmospheric pressures), and ice condenser containments.

The importance of early fission product releases to all risk measures (i.e., acute and latent health effects including land contamination) has been established in past PRAs which included consequence calculations. In keeping with the significance of such early releases, the level 2 analysis descriptions found in the IPE submittals emphasized the phenomena, mechanisms, and accident scenarios which could lead to early releases. These involve early structural failure of the containment, containment bypass, containment isolation failure, and for some BWRs deliberate venting of the containment.

2. GENERAL PERSPECTIVES

When the accident progression analyses in the IPEs are viewed globally, they are, for the most part, consistent with level 2 Probabilistic Risk Analyses (PRA) performed previously. Failure mechanisms identified in the past as being important are shown to be important in the IPEs also. The significance of individual containment failure mechanisms is often determined by particular features of a containment class.

*Work performed under the auspices of the U.S. Nuclear Regulatory Commission.

As a group the PWR large dry containments analyzed in the IPEs have discernibly smaller conditional probabilities of early structural failure than the BWR pressure suppression containments analyzed, as indicated in Figure 1. (Conditional containment failure probability is defined as the probability of containment failtre conditional on core damage having occurred). On the other hand, containment bypass, as well as isolation failures, are, in general, more significant for the PWR containments. However, because of the considerable range in the results, these general trends are often not true for individual IPEs.

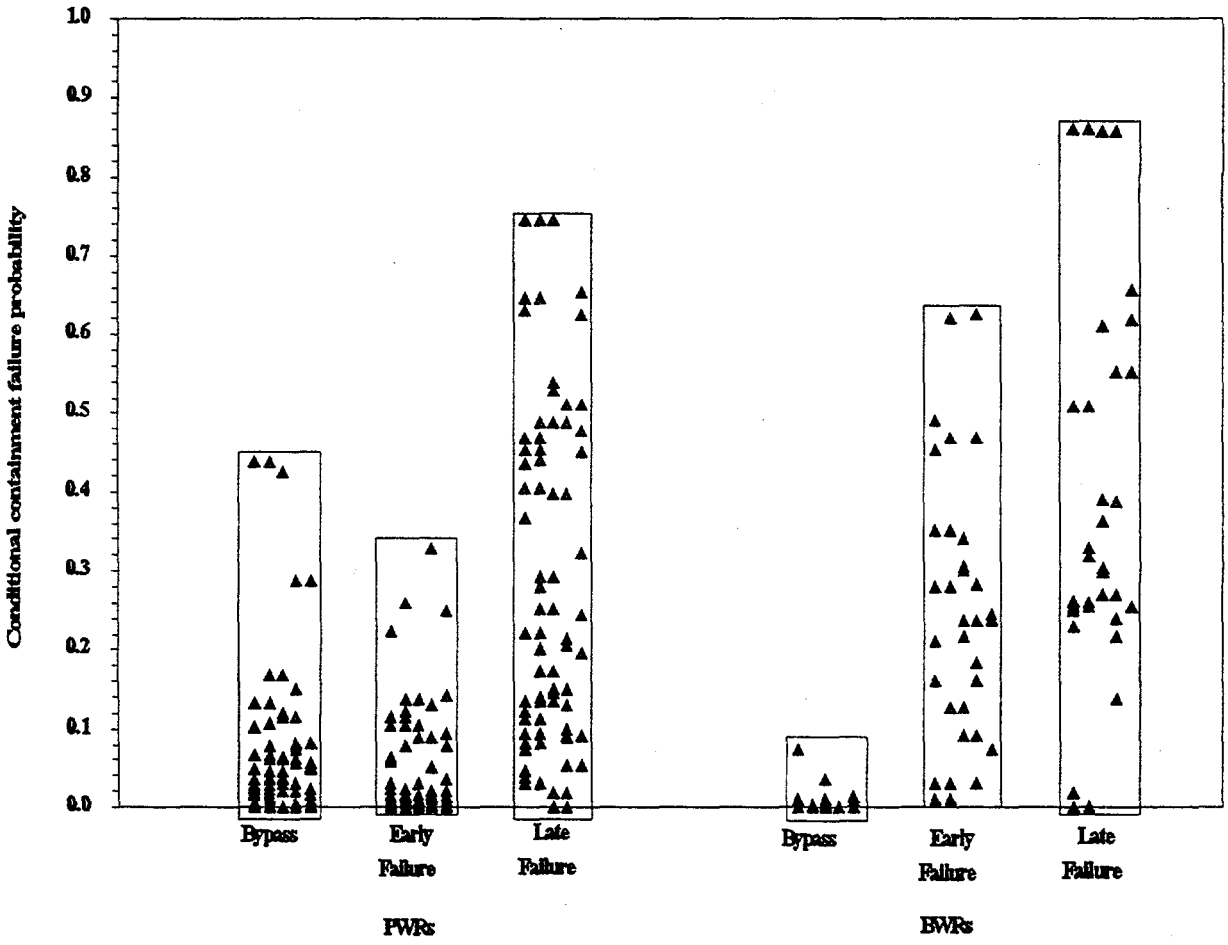


Figure 1 Reported IPE conditional containment failure probabilities (given core melt) for all plants.

Differences in containment designs account for much of the differences in failure probabilities indicated in Figure 1. This is true for the variations between containment classes but also for differences between individual plants in the same containment class. In a significant number of cases unique, plant specific containment features were identified in the analyses as leading to important failure mechanisms. However, differing assumptions in the accident progression modeling also play a ma or role in explaining the significant range in the results obtained.

3. BWR CONTAINMENT PERSPECTIVES

The reported BWR containment results follow expected trends and indicate that the early Mark I containments are, in general, more likely to fail during a severe accident than the later Mark II and Mark III designs. However, the ranges of predicted failure probabilities are quite large for all containment designs and there is significant overlapping of the results. The variability in the results is attributable to a combination of factors including plant design differences such

as the reactor pedestal and drywell floor configuration, drywell flooding, containment construction (steel versus concrete), and combustible gas control; modeling assumptions; and differences in recovery actions that could be taken during a severe accident. However, IPEs for plants in all three containment groups reported a significant probability of early or late structural failure conditional on core damage occurring. These results are expected because smaller pressure suppression containments have been found to have relatively high containment failure probabilities in past PRAs. The probabilities of the various failure modes are shown for each BWR pressure suppression containment group in Figure 2. In general, the factors that influence the failure modes are not the same for each group.

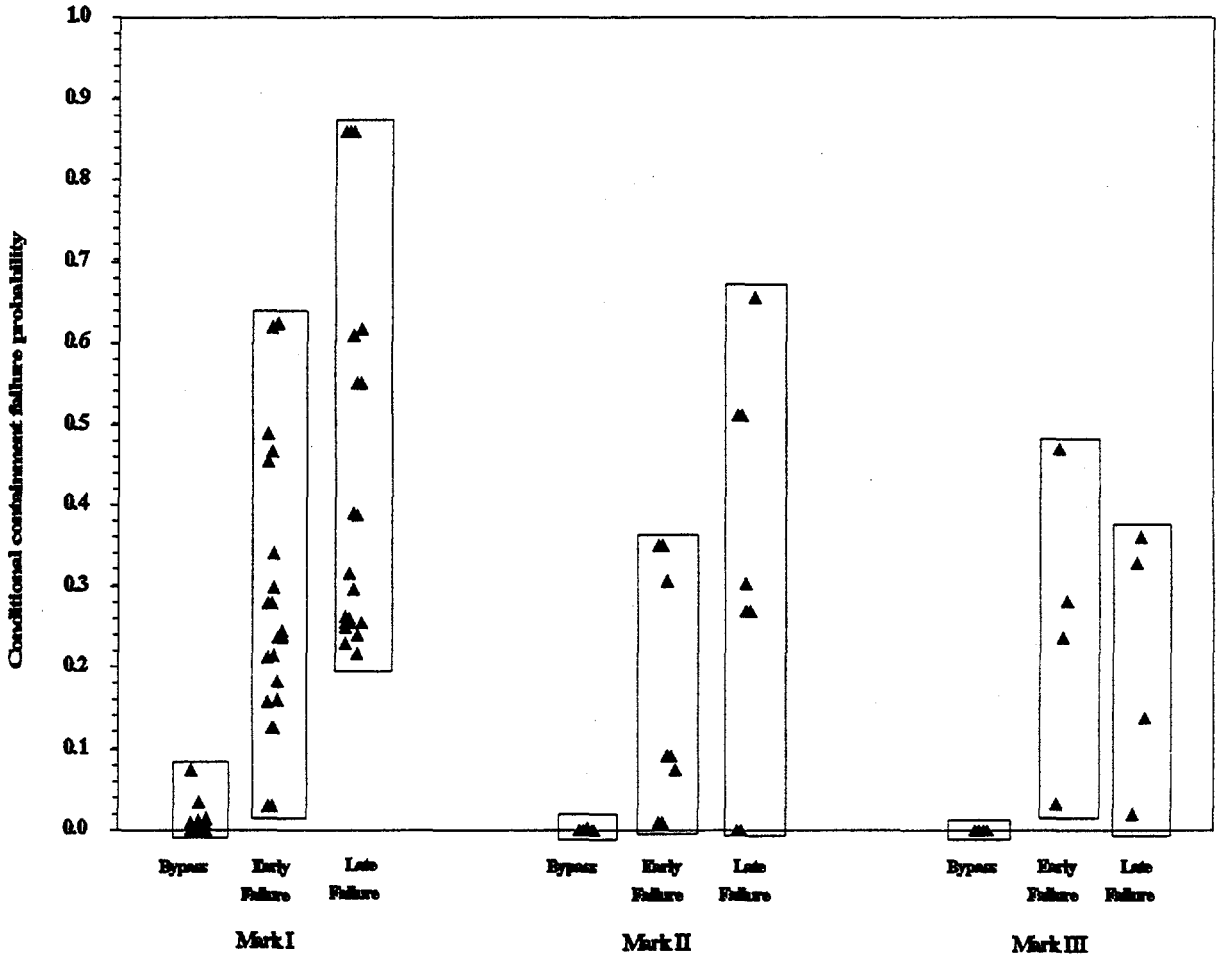


Figure 2 Reported IPE conditional containment failure probabilities (given core melt) for BWR plants.

Accidents that bypass containment are found to be not important for the BWR containments, according to the IPEs. Interfacing systems loss-of-cooling-accidents (LOCA) are found to be not important because of their relatively low frequency compared with the frequency of accidents that dominate the core damage frequency (CDF) and which can lead to early structural failure. Accidents that involve failure to isolate containment are also found not important for BWR containments in the IPEs because of their relatively low frequencies.

Twenty-two BWR units (17 IPE submittals) are housed in Mark I containments. All of the plants in the BWR 2/3 group and most of the plants in the BWR 3/4 group have Mark I containments. These containments have relatively high strength but small volumes and rely on pressure suppression pools to condense steam released from the reactor pressure

vessel during an accident. The IPE results indicate a significant probability of early and/or late containment failure for most of the Mark I containments.

Shell melt-through is found to be the most important contributor to early containment failure for Mark I containments, given core melt. This failure mechanism has a relatively high likelihood of occurring because, for most Mark I containments, the reactor pedestal and the drywell floor are at the same level and openings exist between the pedestal region and the floor. This design allows the core debris to flow across the drywell floor and fail the steel drywell shell either by direct melt-through or via creep rupture. The capability to flood the drywell floor, the design configuration of the drywell, and assumptions regarding core debris dispersal on the drywell floor determine, on a plant-specific basis, how significant shell melt-through is as a containment failure mechanism. In this regard the presence of a water pool on the drywell floor is found to mitigate shell melt-through in all of the submittals, while the design of the drywell sump and drywell floor can prevent or mitigate shell melt-through in some Mark I containments. For example, containment sumps in one plant are large enough to contain the molten core material and thus prevent it from reaching the containment boundary. Finally, the amount of core debris released to the drywell and the fluidity of the core debris assumed in the IPEs also determine whether or not shell melt-through occurs. A number of utilities are being proactive and are identifying minor hardware modifications and changes in procedures to ensure a flooded drywell floor prior to reactor vessel melt-through. Several IPEs also discuss the possibility of relaxing the restrictions on drywell spray initiation in the current Emergency Operating Procedures (EOPs), thus providing greater assurance that there would be water on the drywell floor.

High pressure and temperature loads at the time the core debris melts through the reactor vessel are also a significant contributor to early containment failure for Mark I containments. This failure mechanism occurs in Mark I containments because of their relatively small volumes. The reactor coolant system (RCS) pressure at vessel melt-through, the containment failure location, and modeling assumptions regarding the rate of RCS depressurization and amount of core debris dispersed determine whether this failure mechanism is a significant contributor to early containment failure for individual Mark I containments.

Containment challenges from anticipated-transient-without-scram (ATWS) sequences are important in a number of IPEs for plants with Mark I containments. These sequences belong to an accident class in which containment heat removal and containment venting are inadequate. In ATWS events the energy deposited to the containment can overwhelm the normal containment heat removal mechanisms as well as the available vent paths, leading to early core damage and containment failure. The inability to remove heat from the containment causes containment failure to occur before core damage. The containment failure in turn can lead to the loss of emergency core cooling systems (due to a loss of net positive suction head for pumps drawing from the suppression pool, for instance) with resulting core damage and vessel failure. Depending on the accident progression, core damage could occur first, but containment failure follows quickly. These accidents have been found risk significant in past PRAs since core damage, vessel failure and containment failure can occur within a short time interval, thus producing conditions for significant release to the environment. However, many IPE submittals report that, by proper reactor pressure vessel (RPV) level control and by opening the maximum number of vent paths, many ATWS scenarios can be controlled. The significance of ATWS events in the different IPEs depends on some plant specific features, such as the ability of pumps to work with saturated water, as well as on assumptions regarding power level, point in the fuel cycle, and rapidity of operator response.

Accidents with successful reactor scram but loss of containment heat removal are found to be relatively unimportant in all the Mark I IPEs. The ability to vent the containment is sometimes a ma or factor in reducing the importance of this class of accident. In general, venting is used in the Mark I IPE analyses to reduce releases and is sometimes credited for preventing core damage in accidents involving loss of containment heat removal. However, a few utilities state in their IPEs that their analyses indicate that the installation of a hardened vent does not significantly impact risk and therefore is only of marginal benefit. The pressure at which venting should be started is also examined in detail by several utilities. The impact of high temperatures on the structural capability of the drywell is also noted. For example, one IPE reports that at 400°F the containment could fail at pressures below the current venting pressure in the EOPs. Further analysis is recommended that could refine the vent actuation pressure.

High pressure and temperature loads caused by core/concrete interactions are a significant contributor to late containment failure for Mark I containments. Gradual pressurization at high temperatures caused by non-condensible gases and steam

released from the drywell floor during core/concrete interactions can fail Mark I containments several hours after vessel melt-through. The significance of this failure mechanism to late containment failure is determined by whether or not the drywell is flooded, the design configuration of the drywell, the availability of sprays or venting, and modeling assumptions regarding the quantity and temperature of core debris dispersed across the drywell floor.

Eight BWR units (five IPE submittals) are housed in Mark II containments. Four units are of the BWR 4 type, while the other four units are BWR 5 designs. Mark II containments retain many of the features of the older Mark I containments from which they evolved: They also are characterized by relatively high strength but small volume, and in the event of an accident they depend on a pressure suppression pool to condense the steam released to the containment from the reactor coolant system. However, unlike the Mark I group, most of the Mark II containments are of concrete construction. The exception is one plant (one unit) where the containment consists of a steel shell.

As Figure 2 shows, the conditional probability of early failures varies considerably among the Mark II containments. To a large extent this variation can be attributed to variations in plant-specific containment features, specific plant features play an important role in accident progression in Mark II containments, but modeling assumptions play a role as well. Failure mechanisms found to lead to early failure of Mark II containments include:

- Containment over-pressure failure due to loss of containment heat removal or inadequate containment heat removal.
- Fuel-coolant interaction and direct impingement of core debris on the containment boundary.
- Rapid pressure and temperature rise at the time of reactor vessel failure (important in only a few Mark II IPE analyses).

With the exception of one plant, containment venting does not play a significant role in the accident progression in the Mark II plants.

As with the Mark I IPEs, high pressure and temperature loads caused by core/concrete interactions are significant contributors to late containment failure for Mark II containments, according to these IPEs. In addition, some Mark II IPEs report that late containment failure also results when significant discharge from safety relief valves (SRV) into a hot suppression pool occurs. This assumption is based on the fact that only very limited data exists to support containment integrity at a high SRV discharge rate and elevated containment pressure and temperature.

Four single unit BWRs, described in four separate IPE submittals, are housed in Mark III containments. All four plants are a BWR 6 design. The total free volume of a Mark III containment is significantly greater than that of a Mark I or Mark II. The containment volume to thermal power ratio is about four times that of Mark Is or Mark IIs while the containment design pressure and the estimated failure pressure are significantly lower than those of Mark Is and Mark IIs. Because of their relatively larger volume Mark III containments are not inerted but rely on glow plug igniters to burn off accumulating hydrogen during a severe accident and prevent energetic hydrogen events.

Since the drywell is completely enclosed by the primary containment in the Mark III design, a release to the environment will be scrubbed by the suppression pool if the containment fails but the drywell remains intact. Early drywell failure is therefore an important consideration in the accident progression, and radionuclide release is highest when both the containment and the drywell fail. Since the drywell has a much higher design pressure than the containment, such a failure would most likely be caused by energetic events such as hydrogen combustion and the phenomena associated with vessel breach. These considerations are reflected by the IPE results.

While the causes for early containment failures are not discussed in detail in most of the IPE submittals for Mark III plants, early containment failure seems to be primarily caused by energetic events, such as fuel-coolant interactions or hydrogen burns. The wide spread in the conditional early failure probability among the four Mark III plants shown in Figure 2 is mainly due to the small failure probability assigned to one plant, where ATWS loads are identified in the IPE as the only mechanism capable of causing an early containment failure. While the dismissal of other failure mechanisms may be partly attributable to design differences between this plant and other Mark IIIs, modeling assumptions of this IPE analysis play a significant role as well.

A venting scheme considered in one Mark III plant produces a significant contribution to the frequency of radionuclide release. Venting of the primary system using the Main Steam Isolation Valves (MSIVs) results in an early release and is the most severe release mode in this IPE. According to the analysis, MSIV venting is directed by the BWR emergency procedure guidelines for containment flooding in response to loss of RPV level indication. The procedure requires that a vent path to the RPV be established as containment flooding proceeds beyond the top of the drywell weir wall. This vent path is realized by bypassing the containment interlocks and, regardless of potential releases, opening the MSIVs. This results in a release that bypasses the containment. The licensee suggest in the IPE submittal that this procedure be revisited.

Principal contributors to late failures in Mark III containments are late combustible gas burns and phenomena associated with core/concrete interaction.

4. PWR CONTAINMENT PERSPECTIVES

Containment performance results for all the PWRs in the two groups (large dry including subatmospheric, and ice condensers) are shown in Figure 3. The results indicate that in both PWR groups most of the containments have relatively low conditional probabilities of early failure.

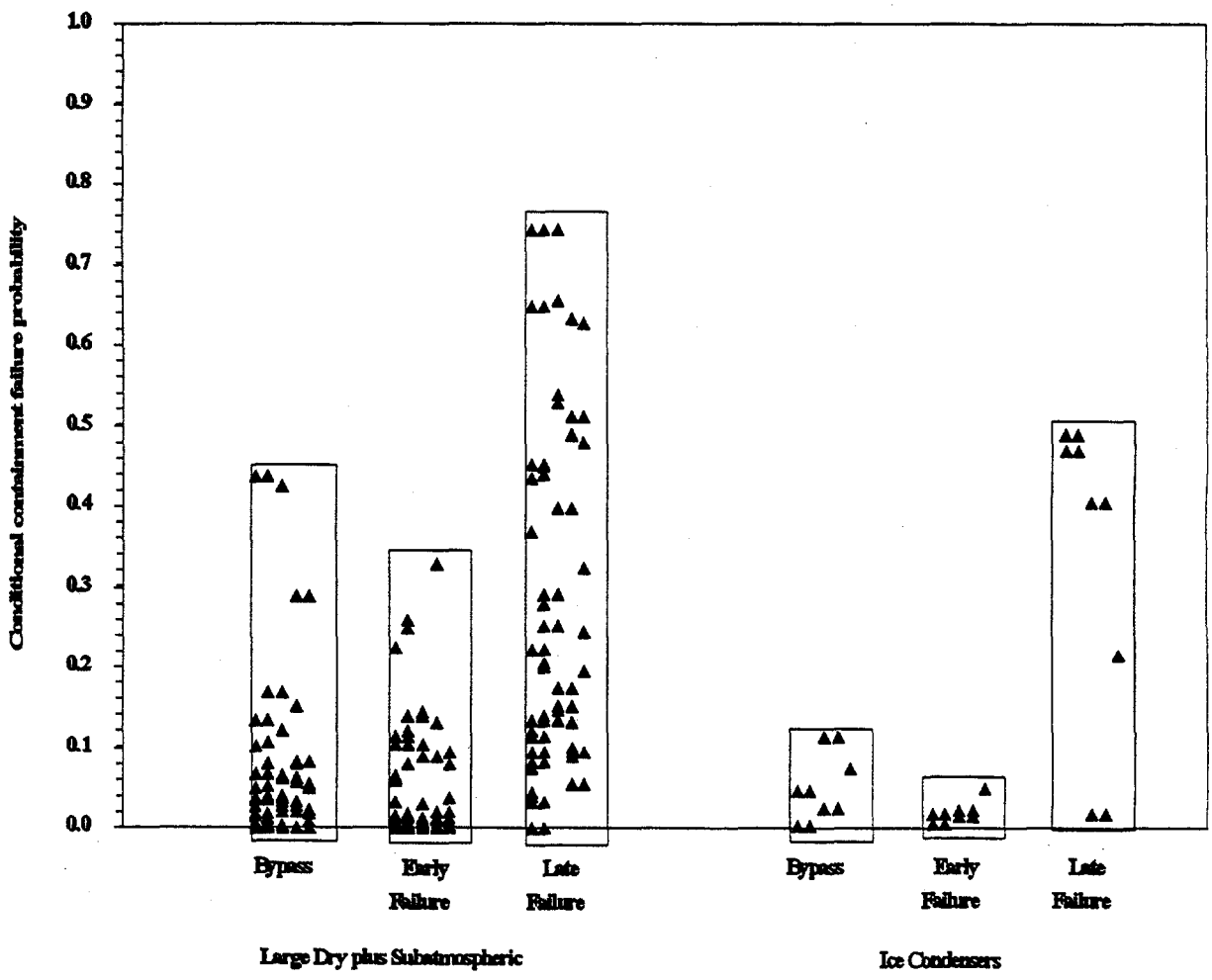


Figure 3 Reported IPE conditional containment failure probabilities (given core melt) for PWR plants.

A large variability exists for both containment groups in the contributions of the different failure modes. This variability is due to plant specific design features, but also due to the modeling assumptions made in the different IPE analyses. The uncertainty of the phenomena associated with high pressure melt e ection (HPME) from the reactor vessel, for instance, is reflected in the variation in likelihood and in magnitude for HPME loads found in the IPEs. Differences in assigning credit for recovery of the core in-vessel after core damage also plays a role in broadening the range of the containment failure results reported.

Sixty-four PWR reactor units and one BWR unit (Big Rock Point), described in forty-three submittals, are housed in large dry containments. For seven of the PWR units (four submittals) the containments are kept at an internal pressure that is a somewhat below atmospheric pressure. All of these containments rely on structural strength and large internal volume to maintain containment integrity during an accident.

In general, only very severe and rapid pressure loads will fail these containments early, and, with a few notable exceptions, the probability of early containment failure for plants in this group is quite small. Important factors for early containment failure are found to be the following:

- Phenomena associated with HPME.
- In a few cases, specific design features leading to unique and significant failure modes.
- Containment bypass, especially steam generator tube rupture, an important source of significant early release.

The most important challenges to containment integrity before or at vessel breach are those associated with high pressure melt e ection (HPME). The containment loads associated with HPME are generated by the addition of mass and energy to the containment atmosphere from a number of sources. This combined load is referred to as the direct containment heating (DCH) load in some IPEs. There are significant uncertainties related to the containment pressure loads that can be produced from the energetic events associated with HPME. The pressure of the reactor coolant system at vessel breach is obviously a factor, as is the geometry of the reactor cavity and the presence or absence of water in the cavity. These parameters, plus some additional assumptions, will determine what the estimated pressure rise at vessel breach will be. However, the estimated containment pressure load before vessel breach also plays an important role in determining the early failure probability. The containment pressure capability curve, particularly the shape of the distribution assumed at the lower pressure end of the curve, is also important. Since a point estimate (rather than a distribution) is used in most of the IPEs, a single pressure load estimate is usually obtained and compared with the containment pressure capability to determine the failure probability.

In some IPEs the probability of early containment structural failure is determined to be not credible. In one group of PWR IPE submittals, which use similar analysis methods, the estimated early containment pressure loads are less than the containment pressure capability, and therefore early containment structural failure is assumed not to occur. It is argued in these IPEs that early containment failure modes, such as those discussed above, are not expected to challenge the containment.

The predicted containment pressure loads are higher in those IPEs that reported relatively higher early containment failure probabilities (i.e., from 0.05 to 0.10) than the IPEs that predict no early containment failure. Usually in these analyses the containment failure pressure is reached when the pressure prior to vessel breach, the "base" pressure, is combined with the pressure rise at vessel breach. Depending on the individual submittal, the higher pressure loads may be due to a high containment base pressure before vessel breach, or a bigger pressure rise due to HPME, or both.

In a number of IPEs specific containment features lead to unique and significant failure modes. For instance, the large probability value of early containment failure in one IPE (0.32) arises from the location of the engineered safeguards (ESF) sump. The IPE postulates a flow of molten core debris from the reactor cavity into the ESF sump and subsequently into the ESF recirculation piping. In the IPE analysis the debris is assumed to melt through the pipe wall eventually and enter the Auxiliary Building.

Containment bypass, especially steam generator tube rupture (SGTR), is an important source of early release in many IPEs for plants with large dry containments. Containment bypass failures include those from interfacing-system LOCA, SGTR, or temperature-induced SGTR. Temperature-induced SGTR is calculated as part of the accident progression

analysis. It occurs if one or more steam generator tubes have a creep rupture due to the flow of high temperature hot gases from the core when the RCS is at system pressure.

Isolation failure is assumed to be negligible in some PWR IPEs for plants with large dry containments, and assumed to have a large conditional probability in others. A large probability of isolation failure is most likely in those IPEs which assume a lack of operator actions to locally or remotely close the isolation valves if no containment isolation signal is provided.

The IPE results for large dry containments show that the dominant late containment failure mode is containment over pressurization, which occurs when containment heat removal capability is lost.

Nine PWR units, described in five IPE submittals, are housed in ice condenser containments. All of these plants utilize a Westinghouse four loop reactor system design. Ice condenser containments have smaller volumes as well as smaller volume to thermal power ratios than other PWR containments. Their containment strength is also less than that of other types. To avoid excessive containment pressure these pressure suppression containments rely on the capability of the ice condenser system to absorb energy released accidentally from the reactor coolant system. Similar to BWR Mark III containments, ice condenser containments rely on glow plug igniters to burn off accumulating hydrogen during a severe accident and thus prevent energetic hydrogen events. Seven of the nine ice condenser units have a cylindrical steel containment surrounded by a concrete secondary containment. The remaining two units feature reinforced concrete containments with steel liners, and lack secondary containments.

Figure 3 shows the containment failure probabilities for this group. Among the five ice condenser IPE analyses the most important causes of early containment failure are:

- Direct impingement of core debris on the containment in the seal table room.
- Rapid steam generation, DCH, and hydrogen burns.
- Over pressurization when containment heat removal is not available.

Although the ma ority of the ice condenser IPEs used data from the NUREG-1150 [2] Sequoyah analysis in their accident progression models, additional plant specific models result in lower failure probabilities than found in NUREG-1150. The primary cause of late containment failure for these containments is found to be overpressure failure in the IPEs. Draining of the refueling water storage tank into the failed vessel, and therefore the reactor cavity, with subsequent boil-off and ice melt contributes to this failure mode. Containment bypass is dominated by interfacing-systems LOCA and SGTR initiators, but one IPE finds induced SGTR to be dominant due to the restart of the reactor coolant pumps (RCPs) when inadequate core cooling conditions exist.

The conditional probabilities of early failure (including isolation failure) found in the IPEs for the ice condenser containments are, on average, smaller than the values obtained from the IPEs for plants with large dry and subatmospheric containments. This smaller failure probability for ice condenser containments as a group is somewhat surprising. The containment volume to reactor thermal power ratios for ice condenser containments are a factor of two to three less than those for large dry containments and subatmospheric containments. The ultimate containment pressure capabilities for ice condenser containments are also smaller than those for large dry and subatmospheric containments (e.g., 80 psig versus 130 psig). No single reason for the lower (on average) ice condenser failure probabilities is apparent from the IPE submittals. Modeling assumptions such as the availability of the ice condenser and its availability to absorb the energy produced by phenomena like DCH play a role. However, it must also be remembered that there are only five IPEs for ice condenser plants, a relatively small sample, while there are forty-five IPEs for plants with either a large dry or subatmospheric containment. Therefore, much greater variation in the likelihood of early failure can be found in this larger group.

5. RADIONUCLIDE RELEASE PERSPECTIVES

It is useful to review the results presented in the IPE submittals regarding radionuclide release, especially early release.

Following the usual convention, the source term which defines the severity of radionuclide release is expressed in the IPEs in terms of the fractions of the radionuclides released to the environment to their total inventories initially in the

reactor system. These release fractions are predicted in the ma ority of IPEs using either the MAAP [3] computer code or the parametric source term prediction code developed in NUREG-1150. In some IPEs, results from the calculations of both codes (i.e., MAAP or parametric source term) are presented. Early release is of particular concern because of the potential for severe consequences due to the short time allowed for radioactivity decay and natural deposition, as well as for accident response actions such as evacuation of the population in the vicinity of the plant.

The containment failure modes that result in an early release of radionuclides to the environment are containment bypass, isolation failure, and early containment structural failure. In BWR pressure suppression containments early containment venting could also lead to an early release. Not all early failures lead to a significant release, since the amount of the release depends on the failure size as well as the removal or "scrubbing" (if any) of some of the radionuclides within the containment that is assumed to take place. What is considered to be a significant release varies among the IPEs. In many IPEs significant releases includes those release cases that involve a release fraction of volatile radionuclides equal to or greater than 0.10 (i.e., the release fraction of either the iodine and or cesium group is greater than 0.10 of core inventory). This definition can be used to screen the results reported in most of the IPE submittals, and is used for purposes of this discussion. However, in some IPEs release fractions are predicted to be below 0.10 for all containment failure modes. Since there are considerable uncertainties in source term predictions, it seems inappropriate to characterize these IPEs as having zero significant early release. Instead, for these IPEs the frequency of containment bypass and the part of early failure that involves a large failure size is used as the frequency of early release in the discussion below. Figure 4 shows the frequency for significant early release of radionuclides by containment type as reported in the IPEs. The reporting of release results in the IPEs varied in the type and detail of the information provided so that in some cases the results discussed below have had to be inferred or estimated.

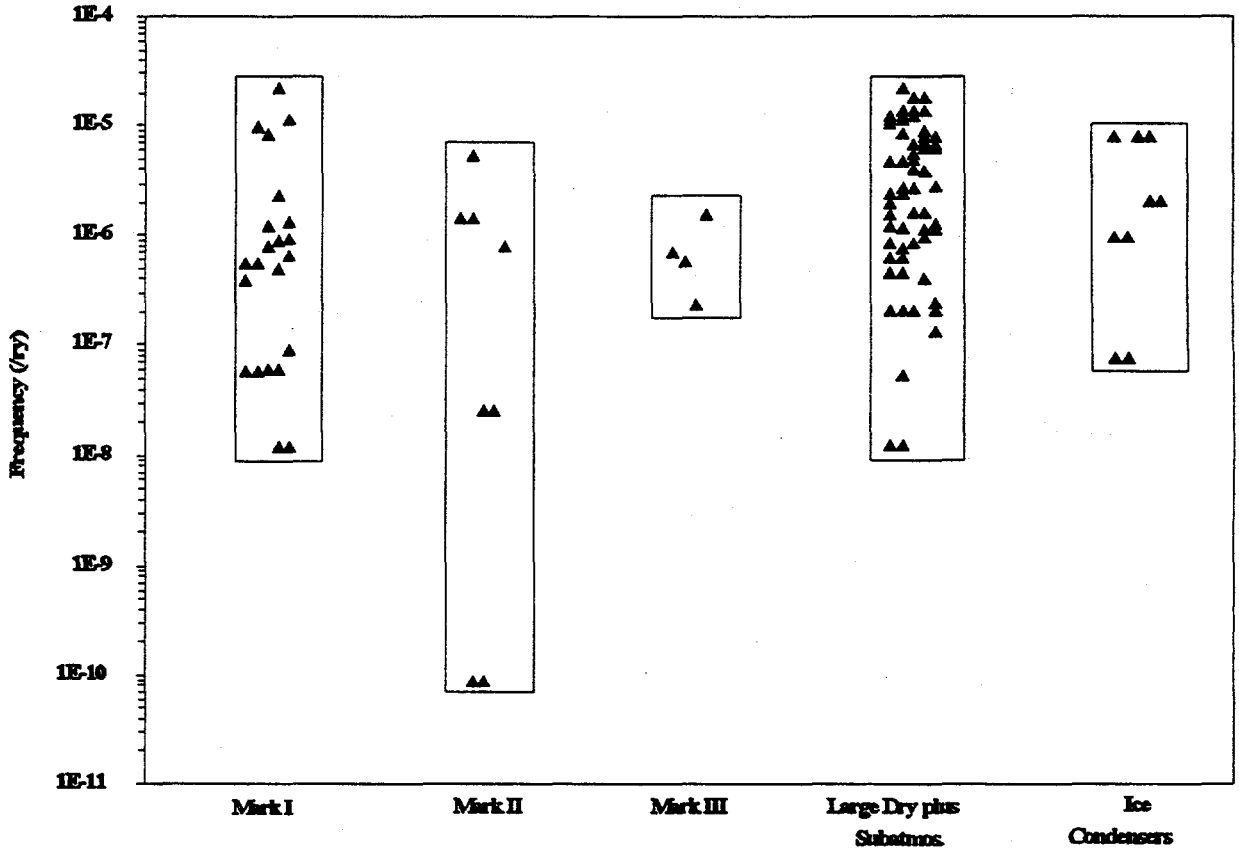


Figure 4 Reported IPE frequencies of significant early release by containment type.

Among the BWR plants with pressure suppression containments, those with Mark I containments show the largest variation in the probability and frequency of significant early release reported in the IPEs. As indicated in Figure 4, the frequency of significant early release reported for Mark I plants varies from less than 1E-8/ry to 2E-5/ry. With the exception of one Mark I plant, the frequency of significant early release reported for BWR plants is less than 1E-5/ry.

For Mark II containments Figure 4 shows that the frequencies of significant early release vary from less than 3E-8/ry to about 5E-6/ry, if the very low (<E-10/ry) value reported by one analysis, which used some unusual assumptions, is disregarded.

The frequencies of significant early release for Mark III containments vary from about 2E-7/ry to about 1.5E-6/ry.

The IPE results show that for PWR plants, containment bypass sequences, usually dominated by SGTR sequences, are important contributors to total early as well as significant early radionuclide release. As discussed above, not all early failures involve significant releases. Isolation failure for some of the IPEs involves only a small leak area, and consequently, results in only small releases and consequences. Even for some of the bypass cases reported in the IPEs, the release point may be submerged under water and the release is thus scrubbed. In SGTR sequences, radionuclide release is more significant if the safety valves or the atmospheric dump valves in the steam line of the faulted steam generator are stuck open rather than cycling. Furthermore, the operation of containment sprays will attenuate radionuclides released to the containment atmosphere and greatly reduce the source term.

Since containment bypass usually causes high releases, the IPEs that have relatively high frequencies of significant early release are those that have relatively high frequencies of containment bypass. As indicated in Figure 4, frequencies of significant early release reported in the IPEs for large dry and subatmospheric containments vary from 1E-8/ry to about 2E-5/ry.

Figure 4 also shows the frequencies reported for significant early release in the IPEs for the plants with ice condenser containments vary from less than 1E-7/yr to 8E-6/yr for the five IPEs.

REFERENCES

1. NUREG-1560, "Individual Plant Examination Program: Perspective on Reactor Safety and Plant Performance," Draft for Comment, USNRC, published October 1996.

2. NUREG-1150, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," Final Summary Report, USNRC, December 1990.

3. Fauske and Associates, Inc., "MAAP 3.0B Modular Accident Analysis Program User's Manual," Vol. 1 & 2, March 1990.

PRELIMINARY PERSPECTIVES GAINED FROM INDIVIDUAL PLANT EXAMINATION OF EXTERNAL EVENTS (IPEEE) SEISMIC AND FIRE SUBMITTAL REVIEW

J. T. Chen*, E. Connell*, N. Chokshi*, G. Bagchi*, M. Drouin*
R. Sewell#, M. Kazarians#, J. Lambright#, A. Kuritzky#, M. Bohn+, S. Nowlen+

SUMMARY

As a result of the U.S. Nuclear Regulatory Commission (USNRC) initiated Individual Plant Examination of External Events (IPEEE) program, every operating nuclear power reactor in the United States has performed an assessment of severe accident due to external events. This paper provides a summary of the preliminary insights gained through the review of 24 IPEEE submittals.

INTRODUCTION

On June 28, 1991, NRC issued Generic Letter 88-20, Supplement 4, "Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities, 10 CFR 50.54(f),"[1] and NUREG-1407, "Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities: Final Report."[2] The generic letter requested all licensees to perform an IPEEE to identify plant-specific vulnerabilities to severe accidents caused by external events and report the results to NRC. A comparable program, requesting all licensees to conduct an individual plant examination (IPE) for internally initiated events, GL 88-20[3], was issued in 1988.

Supplement 5[4] to GL 88-20, "Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities," based on the assessment of the impact of the revised seismic hazard results on seismic IPEEE, was subsequently issued to provide modified guidance for performing seismic evaluations.

The objectives of the IPEEE are for each licensee:

1. to develop an appreciation of severe accident behavior,

2. to understand the most likely severe accident sequences that could occur at it's plant under full power operating conditions,

3. to gain a qualitative understanding of the overall likelihood of core damage and fission product releases, and

*USNRC, Washington, D. C. 20555; #ERI, Rockville, MD 20847; +SNL, Albuquerque, NM 87185

4. if necessary, to reduce the overall likelihood of core damage and radioactive material releases by modifying, where appropriate, hardware and procedures that would help prevent or mitigate severe accidents.

To date, the staff has received 51 IPEEE submittals, and will receive an additional 23 submittals by the end of 1997. The NRC will perform a limited review of licensee's IPEEE submittals to obtain reasonable assurance that each licensee has adequately analyzed the plant design and operations to discover instances of particular vulnerability to core damage or unusually poor containment performance given a core damage accident. Currently, twenty-four submittals are under various stages of review. The staff plans to complete the IPEEE submittal reviews by the end of calendar year 1998. This paper provides some preliminary perspectives on seismic and fire risks from the review of those 24 IPEEE submittals.

PROCESS FOR IPEEE SUBMITTAL REVIEW

The process for the current 24 IPEEE submittal reviews consists of two steps. Under Step 1, each IPEEE submittal is examined. This examination involves (1) reviewing the information for completeness against what was requested in Supplement 4 to GL 88-20 and NUREG-1407, and (2) reviewing the results, findings, and conclusions in the submittal for reasonableness. Under Step 2, selected IPEEE submittals (based on the results of Step 1 review) receive a more in-depth review, involving a site audit. At the completion of the review, a staff evaluation report (SER) is prepared and transmitted to the licensees. The SER provides the review findings and the staff position regarding whether the licensee met the intent of the GL.

The goal of the staff review is to ascertain whether the licensee's IPEEE process is capable of identifying external events-induced severe accident vulnerabilities and cost-effective safety improvements to either eliminate or reduce the impact of these vulnerabilities. Therefore, the review does not attempt to validate or verify the results of the licensee's IPEEE.

Currently, twenty-four IPEEE submittals are under various stages of review; five reviews were initially conducted by the staff and nineteen are being conducted primarily with contractor support. A panel, called the Senior Review Board, which consists of the NRC staff and contractors expert in probabilistic risk assessment (PRA), fire, and seismic margins analyses, assessed the completeness, reasonableness, and quality of the contractor reviews.

PRELIMINARY PERSPECTIVES GAINED

The seismic and fire risk evaluations are two major aspects of the IPEEE and licensees have typically expended considerable effort on the evaluations and have conducted extensive plant walkdowns. No licensees have reported a vulnerability due to either seismic or fire event. However, some licensees have implemented plant modifications or procedural changes as a result of the analysis.

SEISMIC PERSPECTIVES

On the basis of relative ranking of seismic hazards, the staff has designated nuclear power plant sites into following seismic evaluation categories in Supplement 4 to Generic Letter 88-20 and NUREG-1407:

Eastern United States (East of the Rocky Mountains) Plant Sites

1. Reduced-scope
2. 0.3g Focused-scope
3. 0.3g Full-scope
4. Seismic PRA (Licensees committed to perform a seismic PRA)

Western United States Plant Sites

5. Seismic margin methods (0.3g Full-scope and 0.5g)
6. Seismic PRA

As described in NUREG-1407, a seismic PRA methodology is acceptable for plants in all evaluation categories; however, a seismic margin assessment (SMA) is also acceptable for plants in evaluation categories 1, 2, 3, and 5. About one-half of the 24 seismic IPEEEs were implemented with a seismic PRA (SPRA), and about one-half were implemented with a seismic margin assessment. Among those SPRAs, a limited number of submittals have used a hybrid approach in which the initial SMA screening procedures were used in conjunction with the risk quantification.

Plant seismic core damage frequency (CDF). Table 1 summarizes the seismic CDF results obtained from the 14 reviewed SPRA IPEEE submittals. Seismic CDFs are observed to range from less than 1×10^{-7} per reactor year (ry) to 2.3×10^{-4}/ry. This broad variation cannot be attributed to the use of different seismic hazard curves (e.g., Lawrence Livermore National Laboratory [LLNL] versus Electric Power Research Institute [EPRI]), since some higher seismic CDF values are based on the EPRI seismic hazard curves. Rather, the broad variation is mainly due to the significant differences in seismic hazards among the plant sites in combination with the designed seismic capacities. In addition, the assumptions and modeling used for the SPRA quantification also contribute to the broader range of variation.

Plant seismic capacity. For plant sites east of the Rocky Mountains, the plant high confidence, low probability of failure (HCLPF) results derived from seismic PRAs have ranged in values of peak ground acceleration (PGA) from less than 0.05g to 0.50g. For the only Western U.S. plant reviewed to date, a PGA HCLPF value of 0.67g was estimated.

In addition to a value of PGA (or other parameter), a spectral shape is also needed to define a plant HCLPF capacity. As Table 1 indicates, seismic capacity results developed from seismic

PRAs are most often associated with a site-specific spectral shape, usually derived from a uniform hazard spectrum. In some cases, the NUREG/CR-0098 spectral shape has been used for evaluating seismic capacity.

Table 2 presents a list of plant-level HCLPF results reported in the licensees' SMA IPEEEs included in this study. All plants in this list are located east of the Rocky Mountains. The plant HCLPF capacities for these full-scope and focused-scope plants are noted to vary from 0.21g to 0.50g. All HCLPF values presented in Table 2 have been derived based on a NUREG/CR-0098 median spectral shape for rock or soil (depending on the site conditions at the plant).

Walkdown insights. Most SPRA and SMA IPEEEs assessed to date have stated that EPRI NP-6041[5] procedures were used for performing seismic screening and walkdowns. For Unsolved Safety Issue (USI) A-46 plants, the walkdown procedures and criteria described in the generic implementation procedure (GIP)[6] were used in all seismic IPEEEs.

In general, anomalous conditions for plants, revealed from a thorough walkdown effort, are related to the following items:

- adequacy of equipment anchorage
- quality of installation
- physical interactions
- seismic maintenance and housekeeping

Relay evaluation. NUREG-1407 describes the recommended procedures for relay evaluation, depending on the scope of seismic evaluation and on whether or not the plant is a USI A-46 plant. Relay evaluations for USI A-46 plants have revealed low ruggedness (bad actor) relays at a number of plants. However, beyond the selected USI A-46 safe shutdown paths, only a few of these plants assessed to date have encountered bad actor relays in other safe shutdown paths selected for IPEEE. For non-USI A-46 plants assessed to date, relay evaluations have revealed a few bad actor relays at a number of plants.

When bad actor relays have been encountered, they have often been found to exist in alarm circuitry, they have been assessed as having negligible consequences resulted from the effect of relay chatter, or they have been determined to be functional upon operator action, i.e., that operator actions will be able to reset the function of these relays. Consequently, only in a few isolated instances, licensees have proposed to replace these bad actor relays.

Soils evaluation. Most licensees, whose plants are not in the reduced-scope seismic category and are identified as soil sites, have provided information addressing the issue of soil failure effects in their IPEEE submittals. A few licensees, who made use of the modified seismic IPEEE guidelines described in Supplement 5 to GL 88-20, have not provided a soils evaluation in their IPEEEs.

In two cases, the soils evaluation has indicated that liquefaction is likely to occur at the review level earthquake (RLE) as defined in NUREG-1407. Also, seismic slope instability is likely to occur at the RLE for two plants; however, the magnitude of slope deformations has been assessed as being minor. Impacts of seismic-induced soil settlements and soil deformations have also generally been assessed as being minor.

The insight from the IPEEEs assessed to date is that soil failures might be a significant concern at some plants; but, the effects of such potential failures might be difficult to rectify in a cost-effective manner.

Non-seismic failures and human actions. All IPEEEs assessed to date have provided some discussion of non-seismic failures and human actions. For SPRA IPEEEs, these effects have been introduced in seismic event-tree and fault-tree models which have been based on plant logic constructed for internal events. It is important to note, though, that seismic impacts on operator error rates have been modeled in a wide variety of fashions among the IPEEE submittals assessed to date. In some seismic PRAs, simplified operator error fragilities have been developed. In other instances, debatable scaling factors on internal event error rates have been applied based on the importance of the human action or on other factors. A notable insight is that, when operator error fragilities have been applied, they often acted to mask the seismic failures that dominate seismic CDF. Because operator fragilities are highly uncertain, it is important to identify the specific operator actions and undertake, as a minimum, a sensitivity study to reveal the relative significance of seismic failures and their impact on operator actions.

In only a few cases have screening criteria been actually applied with respect to random failure rates and human error rates. Most frequently, the SMA IPEEE submittals assessed to date have simply reported an attempt to rely on those seismic success paths that are most familiar to plant operators and that utilize the most reliable equipment.

Seismic-fire evaluation. All IPEEEs assessed to date have attempted to evaluate the following seismic-fire interaction issues:

- seismic initiated fires
- seismic actuation of fire suppression systems

However, the treatment on these issues are rather diversified; some submittals have evaluated them thoroughly in certain areas while other submittals are less thorough. Perhaps most consistently, however, the following are noticed:

- the locations of fire sources have often not been clearly identified
- seismic-induced flooding due to sources other than fire water piping (e.g., tank failures and non-fire-water piping) has often been neglected

The most consistent strong points of the seismic-fire evaluations appear to be the treatment of inadvertent actuation of fire suppression systems and the identification of potential interaction concerns. A number of the IPEEE submittals have produced some significant findings and have resulted in some plant-specific improvements.

Dominant risk contributors. In most instances, dominant risk contributors (seismic failures, random failures, and operator errors), that may lead to core damage, are identified in these SPRA IPEEEs. The following dominant contributors have been reported to be of most significance to seismic CDF:

- Seismic failures:

  Most frequently reported: offsite power, electrical control panels, block walls, and interactions between buildings or systems

  Frequently reported: major building structures, switchgear, cable trays, fuel oil tanks, transformers, and pumps

  Also reported: switchgear chatter, ice condenser, AFW pipe, MFW heaters, containment fans, battery racks, inverters, battery chargers, accumulators, bus under voltage relays, motor control centers, electrical buses, surge tanks, control rod drive, and load centers

- Random failures:

  Most frequently reported: diesel generators

  Frequently reported: relief valves and AFW pumps

- Operator failures:

  Most frequently reported: alignments and other actions to maintain AFW flow

  Frequently reported: actions to initiate cooling or recirculation

  Also reported: actions to reduce CCW heat loads, to cross-tie units, to shut down from the remote panel, to implement diesel procedures, and to reset relays

It is of interest to note that the SPRA IPEEEs assessed to date have indicated that the list of dominant contributors is not significantly altered as a result of using different seismic hazard curves for seismic CDF quantification. That is, the dominant contributors are substantially the same regardless of whether LLNL or EPRI hazard results[7,8] are used, and only minor changes in the ranking of dominant risk contributors have been observed.

Containment performance insights. Most containment performance insights were obtained based on qualitative assessments. However, a few of the IPEEEs assessed to date have employed a quantitative assessment of seismic containment performance. In some instances, the quantitative results are presented as frequencies of small and large radioactive releases, whereas, in other cases, they are presented in the form of frequencies of small and large containment failures. Some seismic PRA IPEEEs have also reported containment HCLPF capacities.

SMA IPEEEs assessed to date have generally implemented a qualitative, deterministic assessment of containment performance. Typically, the assessments have involved screening or walkdown examination of the following items:

- containment structural integrity
- containment penetrations, hatches, and seals
- containment cooling systems

No anomalous conditions have been reported with respect to containment structural integrity. In a few instances, outliers pertaining to containment penetrations and containment cooling have been identified.

Outliers, plant improvements, and vulnerabilities. A number of maintenance and minor improvements have been implemented as a result of the seismic IPEEEs. Some more significant plant changes have been made, based on analyses and resolution strategies implemented by the licensee. Some of the reported plant improvements would reduce seismic CDF, whereas others are simply undertaken to ensure proper plant maintenance.

Licensees have presented a variety of ways in assessing the plant vulnerability in the IPEEE submittals assessed to date. In a few IPEEE submittals, the licensees have employed the guidelines proposed by NUMARC for vulnerability assessment[9]. In other instances, the submittal refers to a significant number of plant anomalies as being vulnerabilities. However, in most instances, no definition of vulnerability is proposed in the IPEEE submittals, and the submittal simply states that no vulnerabilities were found.

Implication of Different Methodologies

Implications of different PRA methodologies. All of the seismic PRA IPEEEs assessed to date have generally followed the conventional seismic PRA methodology, such as described in NUREG/CR-2300[10] and NUREG-1150. However, a hybrid variation on this methodology - the use of a surrogate element - has been employed in many seismic PRA IPEEEs. Table 1 indicates those IPEEEs for which the surrogate element has been employed.

The basis and approach for surrogate element modeling is discussed by Reed and Kennedy[11]. The overall concept of the surrogate element is to account, albeit approximately, for the effects of components that are screened out during the walkdown and screening phase of a SPRA.

Hence, the potential failures of several components (that might normally be excluded from an SPRA model) are represented by the failure of a single surrogate element. Use of the surrogate element helps to ensure that a potentially significant portion of the seismic CDF is not eliminated.

Based on the review findings reported in several IPEEE submittals assessed to date, it appears that the use of the surrogate elements in a SPRA may represent a reasonable alternate SPRA practice. However, the screening should be performed at a sufficiently high threshold, the capacity of the surrogate element should be assessed to be consistent with the screening threshold, and the surrogate element should be appropriately included in the plant logic model. Otherwise, the usefulness of this approach, and the validity of seismic PRA findings, may be compromised. This is revealed in some of the seismic PRA IPEEEs using the surrogate element approach, in that the screening threshold was not chosen sufficiently high, the surrogate element was found to be a dominant risk contributor, and thus masking the true dominant contributors.

Implications of different SMA methodologies. The two different approaches to seismic margin assessment include the NRC methodology (NUREG/CR-4334) and the EPRI methodology (EPRI NP-6041). The principal insight from a comparison of application of these two seismic margin methodologies is that they provided substantially similar findings. It should be noted, though, that HCLPF capacities based on the EPRI method pertain to an 84th percentile non-exceedance probability (NEP), whereas those capacities based on a fragility approach are typically determined with respect to a 50th percentile NEP. Hence, if an NRC SMA is based on fragility calculations, the plant HCLPF should be adjusted to an 84th percentile NEP before making comparisons with HCLPF determinations from an EPRI SMA.

Generic Findings

For the purposes of this paper, generic findings are defined as those frequently observed among plants, whereas plant-unique findings are those that are limited to perhaps just a single plant. Clearly, both plant-unique and generic insights have been revealed from the seismic IPEEE submittals assessed to date.

The dominant risk contributors, presented previously as being reported most frequently or frequently, appear to elucidate some generic concerns. Many of these concerns have been reported previously.

Due to the fact that bad actor relays have been found in several seismic IPEEEs, the existence of bad actor relays in certain plants is also being considered as a generic insight. However, it is an insight that IPEEE submittals assessed to date have generally indicated that the consequences of relay chatter may often be benign, sometimes may need a reset, and may even need to be replaced.

From seismic-fire interaction evaluations, the common finding that suppression equipment (e.g., tanks, bottles, extinguishers) need to be better anchored or restrained, and that the operation

of fire pumps may be compromised due to failure of fuel oil supply or relay chatter effects, can also be classified as additional generic findings.

Plant-Unique Findings

Following are listed some plant-unique findings that have not been fully revealed from past seismic evaluation studies of U.S. commercial nuclear power plants:

- A few eastern U.S. plants present significant core damage frequencies from seismic events, exhibiting seismic CDF values near or higher than 1×10^{-4}/ry, regardless of whether the EPRI or LLNL seismic hazard results are used for seismic CDF quantification.

- Estimates of seismic capacities (HCLPF values) for certain plants can be extremely low.

- Cable trays have been reported as outliers or dominant risk contributors at a number of plants. This is contrary to past pre-IPEEE PRA findings.

- Soil failures might be a significant concern at some plants; however, it may be difficult to impose any cost-effective plant-specific improvements in order to rectify the effects of such failures.

FIRE PERSPECTIVES

In many cases, licensees have collected, generated, and analyzed plant data bases, fire modeling of plant areas, and other important plant information. Licensees have, in general, considered spurious actuation of equipment in the evaluation of equipment failure modes. Most licensees have addressed all plant areas as requested by GL 88-20, Supplement 4, and have conducted extensive plant walkdowns.

Licensees' submittals assessed to date have utilized either the Fire Induced Vulnerability Evaluation (FIVE) methodology,[12] a fire PRA, or a combination of the two methods to perform the analysis. Licensees have, in general, utilized generic industry data for the determination of fire ignition frequencies, and have not updated the generic information with plant-specific experience data. To identify the critical equipment in a specific area, the licensees have typically used their existing fire safe shutdown analysis. For fire impact analysis, the licensees have used the internal events model developed for the IPE effort in almost all cases.

Fire scenarios are identified in varying levels of detail. The most common level of detail is based on the assumption that given a fire in a compartment, the entire contents of that compartment are lost. Less conservative scenarios include suppression of the fire before critical damage and localized fire limited to an electrical panel, motor, or control panel.

To establish the contents of a compartment (in terms of cables and equipment critical to plant safety), the cable routing information collected for the plant post-fire safe shutdown analysis have been used in almost all submittals examined to date. For fire impact analysis (i.e., the frequency of core damage from a fire event), the internal events model developed for the IPE submittal has been used in almost all cases.

Plant Fire CDF. Table 3 summarizes a few key elements from the submittals. For plants that reported a fire induced core damage frequency (CDF), the range varies from less than 1.0E-9 to 2.2E-4/RY. The assumptions and the methodology employed by the risk analysts seem to dominate the results of the fire IPEEE in most cases reviewed to date, not the actual plant configuration.

Walkdown Insights The importance of the walkdowns to the fire portion of the IPEEE has been specifically emphasized in Generic Letter 88-20, Supplement 4, and NUREG 1407. Although the initial IPEEE submittals, in general, are brief in the discussion of the walkdown findings and the methodology utilized, based on licensees' response to NRC's follow up requests for additional information, it appears that most licensees' efforts in the walkdown were adequate. Walkdown information was used by most licensees to address some of the Sandia Fire Risk Scoping Study Issues,[13] such as seismic/fire interactions, spurious operation of fire suppression equipment, fire barrier effectiveness and manual fire fighting effectiveness. Smoke effects on plant equipment and the potential for fire spread between fire areas was also addressed by some licensees during the walkdown. The insights for seismic/fire interactions, spurious operation of fire suppression equipment are discussed in the seismic perspective previously.

Cable Routing Information Cable routing information is perhaps the most important element of a nuclear power plant fire risk analysis. Errors in this part of the analysis can jeopardize the validity of the entire study. The routing of only a select set, albeit a large number, of cables is necessary for IPEEE analysis.

Almost invariably, the submittals state that the cable routing information established as part of the safe shutdown analysis effort has been used in the IPEEE analysis. This practice is acceptable, but two issues must be taken into consideration:

- How does the post-fire safe shutdown model of the Appendix R compliance effort compare with the IPE internal events model?

- In addition to fire-induced reactor trip sequence, has any other fire-induced initiating event sequences been considered in the IPEEE model?

The fire safe shutdown analysis required by 10 CFR 50.48 assumes that a loss of offsite power has occurred for those plant areas where an alternative shutdown procedure is utilized, such as that described in Section III.G.3 and III.L of Appendix R, and that the plant operators have successfully initiated a reactor trip. The reactor trip assumption is reasonable because given the

design features of the reactor protection systems for nuclear power plants, the probability of an ATWS event as a direct consequence of a fire is very low.

The main goal of the post-fire safe shutdown analysis is to deterministically demonstrate that the plant has available paths for safe shutdown the plant. However, the probability of occurrence of a chain of events (especially those that may include high failure probability of human actions), and its effect on containment related functions, was not addressed. This could lead to some differences between the results obtained from using the IPE model and post-fire safe shutdown systems and components.

Almost all IPEEE submittals assessed to date have not addressed how the above differences have been identified and resolved. From the submittals, it is unclear whether those components for which cable routing information is not available were assumed to be in the failed position. If such an assumption was not made, the core damage frequency results can be optimistic.

The probability of fire-induced initiating events other than reactor trip is explicitly addressed in only a few of the submittals examined to date. For example, for PWRs, the possibilities of PORV failure in the open position or loss of offsite power often have not been discussed. Often the fire safe shutdown analysis does not address the cables associated with such initiating events. The lack of a separate discussion of these potential initiating events can lead to the conclusion that the spectrum of accident sequences considered by the licensee may be incomplete, and thus the overall results may be optimistic.

Threshold Value for Screening All fire IPEEE submittals examined to date have included at least one screening step to reduce the number of compartments and fire scenarios requiring detailed analysis. Different methodologies have been used for this purpose. The most common methodology is based on a comparison with a threshold value of initiating event frequency. The threshold value, typically employed by a large number of licensees, and recommended by FIVE, is an initiating event frequency of 1E-6 per reactor year. A few licensees have used 1E-7 or even as low as 1E-8 per reactor year as the threshold value.

The effect on the final results of using a low threshold value cannot be assessed at this time. In the majority of the cases where a low threshold value (i.e., 1E-7 or 1E-8 per reactor year) is employed, the review of these submittals has questioned the adequacy of some parts of the fire analysis methodology. For example, in one case the licensee has assumed that all fire scenarios lead to the same internal events initiating event, without properly justifying this assumption. These types of concerns may overshadow the screening results.

Fire Detection and Suppression Many of the IPEEE submittals have not modeled manual suppression of fires (except in the case of control room fires). While this is understandable under circumstances where the brigade cannot respond before critical damage to safety-related equipment occurs, the limitation resulting from the lack of fire brigade modeling is unclear. Furthermore, not modeling fire brigade actions is functionally equivalent to assuming that there is a negligibly

low conditional probability that the brigade will cause collateral damage during suppression activities to equipment which has not been damaged by a fire.

In conjunction with this analysis, consideration of potential human errors in manual fire suppression is important. The potential exists for inadvertent application of fire suppressant agents to equipment that has been undamaged by fire. Such inadvertent application can result in the failure of the otherwise undamaged equipment.

In general, most submittals have assumed a reliability of automatic suppression in the range of 0.95-0.98, consistent with the information provided in the FIVE methodology. This data is based on the performance of automatic suppression systems that have been designed, installed, and maintained in accordance with applicable National Fire Protection Association (NFPA) codes and standards. For systems that are not designed in accordance with the applicable codes and standards, the reliability data provided in the FIVE methodology cannot be used without additional justification.

It is important to note that, in many IPEEEs reviewed to date, simplified modeling has been used for the fire suppression (automatic features and manual actions combined) aspect of a fire scenario. The fire occurrence frequency is simply multiplied by the failure probability of the suppression system. The failure probability is often gleaned from either FIVE or other industry sources. It is assumed (as a first step) that upon fire occurrence, the entire compartment is affected, and all the cables and equipment within are failed. Multiplication by a suppression failure probability implies the additional assumption that no critical damage may occur if fire suppression is successful. This may be an optimistic assumption without knowledge of the layout of cables and equipment in the compartment. If critical cables and equipment are in close proximity to each other, and on top of a likely ignition source, this multiplication process is clearly optimistic.

Analytical Assumptions In many of the fire IPEEE submittals assessed to date, a variety of optimistic assumptions have been used in the analysis. Assumptions that were found by the staff to be unacceptable included: optimistic actuation times of automatic suppression and detection equipment, manual suppression times based solely on fire brigade response times during drills, consideration of unprotected conduit as equivalent to a rated fire barrier, optimistic cable and equipment damage thresholds, inappropriate heat release rate data for plant materials, partitioning of fire ignition frequencies based on floor area, and assumed 100% reliability of active components of fire barriers, such as doors and dampers. Additional detail on some of these areas is provided below.

Fire Propagation Modeling: NUREG-1407 specifically requests a discussion of the treatment of fire growth and spread, as well as the spread of hot gases and smoke. Issues that were found to be questionable included such items as: use of inappropriate heat loss factors; omission of fire sources; use of inappropriate heat release rates; and ignoring the existence of open pathways between compartments. Most FIVE-based assessments reviewed to date have failed to extend the analysis for cases in which fire spread may be predicted.

Electrical Cabinet Fire Propagation: A number of the fire IPEEE submittals have made optimistic assumptions concerning electrical cabinet fires which have acted to artificially reduce the impact of such fires on the results of the studies. Some of the optimistic assumptions appear to derive from the treatment of electrical cabinet fires in the NSAC/181 report[14]. For example, the heat release rates associated with such fires were significantly understated and the chimney effect in switchgear cabinet fires and fires involving highly energetic switchgear or breaker faults was not considered. Plant-specific details of electrical cabinets are potentially very important to fire risk, yet the initial IPEEE fire submittals have most frequently not reported such details.

Control Room Fire Modeling: A few IPEEE submittals have reported very low core damage frequencies for control room fires; this seems to be the result of using the data presented in the NSAC/181 report. Conditional non-suppression probabilities in the range of 1 to 3% were noted in the IPEEE submittal reviews. Other submittals provided so few details concerning the control room fire analysis that it was not possible to ascertain how this matter was modeled. The use of optimistic assumptions regarding the time available to suppress control room fires before the smoke and heat would force abandonment of the control room in some submittals, and the lack of details concerning control room fire modeling in other submittals, raise questions about the contribution of control room fires to fire-initiated core damage frequency.

Inter-Compartment Fire Propagation: The possibility of inter-compartmental fire propagation has been treated in the IPEEE submittals with varying degrees of detail and sophistication. Many submittals have quoted the Fire Compartment Interaction Analysis (FCIA) of FIVE as the methodology employed for inter-compartmental fire analysis, and simply do not provide additional information. The IPEEE submittals, in almost all cases, have ignored the potential failure of an active fire barrier (e.g., self closing doors and fire dampers), even though a fire damper may have an unreliability level as high as 0.2 per demand (e.g., for curtain-type fire dampers).

Human Error Analysis Human errors, typically those involving recovery actions, can be a significant aspect of the plant's fire vulnerability. However, due to insufficient data regarding human performance during a fire incident, most IPEEE submittals assessed to date provide little or no discussion on how human intervention was treated and how fire-induced and non-fire-induced failures were combined. Although fires in the control room are generally significant contributors to the CDF, the effects of fire and smoke on operator performance reliability was addressed in only two of 24 submittals. Considering the emergency nature of a fire in the control room, the adverse environmental conditions associated with the fire, and the reliance on alternative or remote shutdown procedures and equipment, it is reasonable to expect some degradation in operator reliability that is unique to this event.

The performance of the fire brigade is usually addressed by assuming a plant wide reliability factor for manual suppression based on response times recorded during drills and the level of fire

brigade training. This approach does not consider the type or expected severity of the fire and its impact on brigade effectiveness, or the potential adverse effects on plant equipment of manual suppression activities. Response times during drills do not correlate to the time required to control or extinguish a fire.

Due to the uncertainties in method and lack of rigor associated with the treatment of human intervention in fire scenarios, it appears that the modeling of human performance should be considered as a weak area.

Vulnerabilities and Plant Improvements A few licensees have used NUMARC 91-04, "Severe Accident Issue Closure Guidelines," to define plant vulnerabilities. However, most other licensees have not provided a specific definition for identifying vulnerabilities. No licensees have reported a vulnerability due to fire. However, some licensees have implemented plant modifications or procedural changes as a result of the analysis. A few licensees have indicated the need for additional analyses.

Implication of Different Methodologies

The methodologies used for fire IPEEEs have been: FIVE, PRA (i.e., NUREG/CR-2300[6] and Kazarians et al.[15]), and an aggregate of FIVE and PRA (see Table 3). The majority of licensees have taken some advantage of various features of the FIVE methodology.

It is interesting to note that a few plants, that have used FIVE as the primary methodology for screening, report a larger total core damage frequency than those plants using PRA. The submittals did not contain sufficient detail to identify the underlying reasons for the difference.

The screening phases are practically the same for these methodologies. Quantitative screening is used in FIVE prior to the use of PRA models to augment with the independent events to estimate the core damage frequency. For fire propagation modeling, FIVE methodology provides a set of pre-formulated worksheets and look-up tables. The PRA users have generally used the updated COMPBRN[16] for this purpose. In both cases, similar fire phenomenology is considered and similar formulations are employed.

FIVE also provides generic fire occurrence data, fire protection system failure data and procedures for using and partitioning such data. The procedures and data are consistent with those used in fire PRA. In fact, many PRA users have used data and procedures that are similar to those provided in the FIVE handbook.

Generic Findings

Licensees generally have stated that the reported fire CDF should not be compared with other core damage contributors due to the uncertainties associated with fire risk assessment. This statement notwithstanding, one can still draw the following:

- The fire core damage frequencies for certain plants are relatively high as compared to CDFs associated with internal events.

- There is a large plant-to-plant variation in terms of overall fire CDF and especially when the specific contributors are considered.

The dominant CDF contributors are presented in terms of two important aspects of a fire event: (1) location of the fire, and (2) equipment/systems affected by the fire. Often, fire scenarios affecting the control room and cable spreading room are found to be the dominant contributors to fire CDF during power operation.

CONCLUSIONS

Seismic and fire IPEEEs assessed to date have revealed numerous valuable perspectives concerning the severe-accident behavior and the most likely accident sequences at these 24 operating nuclear power plants. The licensees have benefited from their seismic and fire IPEEE effort and have proposed or already implemented certain plant-specific improvements, which will reduce the overall frequency of core damage and enhance the safety of these nuclear power plants. Through the reviews of IPEEE submittals concerning the completeness, detail, and overall quality, the NRC has been able to gain important perspectives concerning the severe-accident behavior for these licensees' nuclear power plants. These valuable perspectives will enhance NRC's capability in focusing more closely on specific issues related to seismic and fire events when appropriate.

ACKNOWLEDGMENTS

This paper was based on the IPEEE submittal reviews performed by the NRC staff and Energy Research, Inc. The involvement of the following individuals in various facets of this project is acknowledged: M. Cunningham, A. Buslik, T. Y. Chang, R. Kornasiewicz, R. Rothman, R. J. Budnitz, M. V. Frank, M. Khatib-Rahbar, and S. C. Sholly.

REFERENCES

1. USNRC, Generic Letter 88-20, Supplement No. 4, "Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities, 10 CFR 50.54(f)," June 28, 1991.

2. NUREG-1407, "Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities, Final Report," J. Chen, et al., USNRC, June 1991

3. USNRC, Generic Letter 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities, 10 CFR 50.54(f)," November 23, 1988.

4. USNRC, Generic Letter 88-20, Supplement No. 5, "Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities," September 8, 1995.

5. EPRI NP-6041-SL, "A Methodology for Assessment of Nuclear Power Plant Seismic Margin," Rev. 1, August 1991.

6. Seismic Qualification Utility Group (SQUG), "Generic Implementation Procedure (GIP) for Seismic Verification of Nuclear Plant Equipment," Revision 2, February 14, 1992.

7. EPRI NP-6395-D, "Probabilistic Seismic Hazard Evaluation at Nuclear Plant Sites in the Central and Eastern United States: Resolution of the Charleston Issue," April 1989.

8. NUREG/CR-5250, "Seismic Hazard Characterization of 69 Nuclear Power Plant Sites East of Rocky Mountains," Vols. 1-8, Jan. 1989.

9. NUMARC Report 91-04, "Severe Accident Issue Closure Guideline," January 1992

10. NUREG/CR-2300, "PRA Procedures Guide," American Nuclear Society, Institute of Electrical and Electronic Engineers, and U.S. Nuclear Regulatory Commission, January 1983.

11. EPRI TR-103959, "Methodology for Developing Seismic Fragilities," J.W. Reed and R.P. Kennedy. EPRI, June 1994.

12. EPRI TR-100370, "Fire Induced Vulnerability Evaluation (FIVE)", Electric Power Research Institute (EPRI), April 1992.

13. NUREG/CR-5088, "Fire Risk Scoping Study: Investigation of Nuclear Power Plant Fire Risk, Including Previously Unaddressed Issues," J. Lambright, et al., Sandia National Laboratories, January 1989.

14. NSAC/181, "Fire PRA Requantification Studies," W. Parkinson, et al., Electric Power Research Institute, Nuclear Safety Analysis Center, March 1993.

15. Kazarians, M., N.O. Siu, and G. Apostolakis, "Risk Analysis for Nuclear Power Plants: Methodological Developments and Applications," Risk Analysis, Vol. 5 No. 1, March 1985.

16. UCLA-ENG 9016, "COMPBRN IIIe: An Interactive Computer Code fore Fire Risk Analysis", Vincent Ho, S. Chien and G. Apostolakis, EPRI, UCLA School of Engineering and Applied Science, October 1990.

Table 1. Seismic CDF and HCLPF Results from SPRAs

Plant Name	Seismic CDF (per ry) EPRI[8]/Other	Seismic CDF (per ry) LLNL[9]	HCLPF (g)	Spectral Shape	Surrogate Element?
Catawba	1.6×10^{-5}	--	--	Site-Spec. (Sequoyah)	No
Cook	3.2×10^{-6}	1.0×10^{-5}	0.25	1989 LLNL	No
Diablo	4.2×10^{-5}	--	0.67	Site-Spec. (LTSP)	No
Haddam	2.3×10^{-4}	1.5×10^{-4}	<0.05	1989 EPRI	Yes
Kewaunee	1.1×10^{-5}	1.3×10^{-5}	0.23	1989 LLNL	Yes
LaSalle	7.6×10^{-7}	--	--		No
McGuire	1.1×10^{-5}	--	--	NUREG/CR-0098	No
Millstone	9.1×10^{-6}				No
NMP-2	2.5×10^{-7}	1.2×10^{-6}	0.50	NUREG/CR-0098	Yes
Palisades	--	8.9×10^{-6}	0.22	1993 LLNL	Yes
Pilgrim	5.8×10^{-5}	9.4×10^{-5}	0.25	1989 LLNL	Yes
Pt. Beach	1.4×10^{-5}	1.3×10^{-5}	0.16	1989 LLNL	Yes
Seabrook	1.2×10^{-5}				No
S. Texas	$<1\times10^{-7}$				No

Table 2. HCLPF Results from Seismic Margin Assessments

Plant Name	Selected Method	Seismic Category	HCLPF (g)	Spectral Shape
Brunswick	EPRI	Focused-scope	>0.3	NUREG/CR-0098 Soil
Callaway	EPRI	Focused-scope	>0.3	NUREG/CR-0098 Soil
Comanche Pk	EPRI	Reduced-scope	--	SSE, 0.12g, Rock
Ft. Calhoun	NRC	Focused-scope	0.25	NUREG/CR-0098 Soil
Limerick	EPRI	Focused-scope	--	SSE, 0.15g, Rock
NMP-2	EPRI	Focused-scope	0.50	NUREG/CR-0098 Rock
Robinson	EPRI	Full-scope	0.28	NUREG/CR-0098 Soil
St. Lucie	Site-specific	Reduced-scope	--	SSE, 0.10g, Fill
Sequoyah	EPRI	Full-scope	0.27	NUREG/CR-0098
Susquehanna	EPRI	Focused-scope	0.21	NUREG/CR-0098 Rock, Soil
Turkey Point	Site-specific	Reduced-scope	--	SSE, 0.15g, Rock

Table 3 List of Plants and their Core Damage Frequencies From Fire Events

Plant	CDF	Method	Plant Improvements	Significant Fire Areas
Brunswick	3.4E-5	PRA+FIVE	TBD for CDF>1E-6	Control room (CR) and cable spreading room (CSR)
Callaway	8.9E-6	FIVE	None	CR and 2 ESF switchgear rooms (SGRs)
Catawba	4.7E-6	PRA	None	CR, CSR, and component cooling room (CCR)
Comanche Peak	2.1E-5	PRA+FIVE	None	CR
Cook	3.8E-6	PRA	None	CR, diesel generator room (DGR), ESW R, SGR, MCC R, battery (BatR), aux bldg (AuxB), & turbine bldg (TB).
Diablo Canyon	2.7E-5	PRA	None	CR and CSR
Ft. Calhoun	2.7E-5	PRA	Proc mod (ISLOCA & SAMG)	CR, east basement of AuxB, & TB
Haddam Neck	6.1E-5	PRA+FIVE	Dev proc, Inst spr head, & Reroute cables for pumps	
Kewaunee	9.8E-5	PRA+FIVE	None	Aux feedwater pump (AFW PuR), CSR, DGR
LaSalle	3.2E-5	PRA	None	CR, TB, CSB, electrical equipment room (EER), AuxR, cable shaft area
Limerick	<1E-6	FIVE	Red Tran Comb, Imp Proc	SGR, static convertor (S-CvR), remote shutdown room (RSDR)
McGuire	2.3E-7	PRA	None	CR, CSB, I&C area, Aux SD panel
Millstone #3	4.8E-6	PRA	None	CSR, CR, charging and component cooling pump zone
Nine Mile Pt #2	1.0E-6	PRA+FIVE	None	CR
Palisades	2.0E-4	PRA+FIVE	Upgrade F Prog & Re-Ana	CR, CSR, TB, spent fule pool (SFPR), AuxB
Pilgrim	2.2E-5	PRA+FIVE	None	CR, SGB, RBCCW-TBCCW PuR, TB, main transformer (MnTr)
Pt. Beach	5.1E-5	FIVE	Add 2 DGs, AuFWS, CR	CR, CSR, AFW PuR, gas turbine (GTR), vital & non-vital (V/NV) SGR, DGR
Robinson	2.2E-4	PRA+FIVE	Impl SAMG	CR, BatR, SGR, yard transformer (YTr)
St. Lucie #1	1.9E-4	FIVE	X-tie, door closed, SGRB CDF	CR, CSR, SGR
St. Lucie #2	1.2E-5	FIVE		CR, CSR, & SGR
Seabrook	1.2E-5	PRA	Mod. resp proc., Exp. supp. in TB, inst det'n in TB relay R	CR, CSB, AuxB, TB, service water pumphouse (SWPH)
Sequoyah	1.6E-5	FIVE	None	AuxB, HVAC R, BatR, SGR, TB
S Texas #1&2	5.1E-7	PRA	None	CR, AuxB
Susquehanna	<1E-9	PRA	Splash guard on cabs, prov'ns for draining water from CSB	
Turkey Pt		FIVE	H_2O proof CSR cabs & install dry pipe, preactive system	CR, CSR, ICWS

ATHEANA: "A Technique for Human Error Analysis" Entering the Implementation Phase

J. Taylor, J. O'Hara, W. Luckas
Brookhaven National Laboratory

D. Bley, J. Wreathall
Wreathall Group

E. Roth
Westinghouse Electric Corp.

G. Parry, A. Ramey-Smith, M. Drouin, C. Thompson
U.S. Nuclear Regulatory Commission

Introduction

Probabilistic Risk Assessment (PRA) has become an increasingly important tool in the nuclear power industry, both for the Nuclear Regulatory Commission (NRC) and the operating utilities. The NRC recently published a final policy statement, SECY-95-126, encouraging the use of PRA in regulatory activities. Human reliability analysis (HRA), while a critical element of PRA, has limitations in the analysis of human actions in PRAs that have long been recognized as a constraint when using PRA. In fact, better integration of HRA into the PRA process has long been a NRC issue. Of particular concern, has been the omission of errors of commission - those errors that are associated with inappropriate interventions by operators with operating systems.

To address these concerns, the NRC identified the need to develop an improved HRA method, so that human reliability can be better represented and integrated into PRA modeling and quantification.

The purpose of the Brookhaven National Laboratory (BNL) project, entitled "Improved HRA Method Based on Operating Experience" is to develop a new method for HRA which is supported by the analysis of risk-significant operating experience. This approach will allow a more realistic assessment and representation of the human contribution to plant risk, and thereby increase the utility of PRA. The project's completed, ongoing, and future efforts fall into four phases:

1) Assessment Phase (FY 92/93, documented in NUREG/CR-6093)[1]
2) Analysis and Characterization Phase (FY 93/94, documented in NUREG/CR-6265)[2]
3) Development Phase (FY 95/96, documented in NUREG/CR-6350)[3]
4) Implementation Phase (FY96/97 ongoing)

The Analysis and Characterization Phase (documented in NUREG/CR-6265) developed a multi disciplinary HRA framework with the objective of providing a structured approach for analyzing operating experience and understanding nuclear power plant (NPP) safety, human error, and the underlying factors that affect them. The framework had to be multi disciplinary because the factors affecting human reliability and plant safety are based on many sciences. In the Development Phase, the concepts of the framework matured into a working HRA method, with identified process steps.[4] This working HRA method, albeit in preliminary form, was expanded by using trial applications.

The ATHEANA HRA Method

The new HRA method, called ATHEANA (A Technique for Human Error Analysis), improves the ability of PRAs to:

- identify and characterize important human-system interactions and their likely consequences under accident conditions;
- represent the most important severe accident sequences that could occur;
- provide recommendations for improving human performance based upon characterizations of the causes of human errors.

In order to achieve these goals in the development of the new HRA method, ATHEANA, it was necessary to establish a new basis for HRA modeling, starting with the development of a better understanding of human performance in serious nuclear power plant accidents and their precursors. ATHEANA is based on a multi disciplinary framework that considers both the human-centered factors (e.g., performance shaping factors such as human-machine interface design, procedures content and format, and training) and the conditions of the plant that give rise to the need for actions and create the operational causes for human-system interactions (e.g., misleading indications, equipment unavailabilities, and other unusual configurations or operational circumstances). The human-centered factors and the influence of plant conditions are not independent of each other; the combined effect of performance shaping factors (PSFs) and plant conditions that create a situation in which human error is likely to occur is an "error-forcing context."

Considerable research was conducted on the various HRA elements of the ATHEANA framework. The representation of human error encompasses both the underlying mechanisms of human error and the consequences of the error mechanism, which is the unsafe action, whose consequences on the system are represented in the PRA model by the human failure event (HFE). The error mechanisms are behavioral and cognitive mechanisms causing human errors, that can be triggered by particular plant conditions and PSFs. When applied in the wrong context, error mechanisms can lead to inappropriate actions that can have unsafe consequences that lie within

the PRA definition of accident scenarios. "Unsafe actions" are those actions inappropriately taken, or not taken when needed, by plant personnel that result in a degraded plant safety condition. Unsafe action does not necessarily imply that humans are a root cause; people are often set-up by circumstances and conditions to take actions that are unsafe.

In addition to the psychological developments discussed above, analyses of accidents and serious incidents have both confirmed the principles underlying ATHEANA and precipitated the identification and development of these principles. The results of these operational event analyses are formulated in a manner that supports use of ATHEANA. These results are captured in a database[5] which has been developed for this project.

ATHEANA has been developed with the goal of being used in traditional PRA models. In other words, application of ATHEANA will not require major changes to the mechanics of how PRA models are constructed. Furthermore, ATHEANA will be usable by a PRA analyst, using input from experts such as those knowledgeable of plant design and operations, but will not need to rely on having extensive experience in human factors or psychology.

A simulated trial application of ATHEANA was conducted for the purpose of validating the following process steps. (It should be noted that the quantification of a HFE based upon the likelihood of EFCs occurring represents a fundamental shift in the conduct of HRA.):

- identification of a human failure event (HFE)
- identification of an unsafe action associated with the HFE
- identification of an error-forcing context (EFCs) associated with the unsafe action
- estimation of probabilities for each EFCS
- quantification of the HFE using the estimated EFCS probabilities

For the purposes of the simulated trial application, a PWR small-break LOCA was selected. The specific PRA used in the trial application was the Surry Unit I NUREG-1 150 PRA. An existing PRA was used so that comparisons could be made between the original PRA and the trial application. As is typical, the sample PRA only modeled human errors of omission. However, to demonstrate the value of ATHEANA, the success of the high pressure injection function was examined and ways in which the operators can fail this function were identified, based upon knowledge gained on the project to date from human factors research and event analyses. As a result, the HFE identified in the trial demonstration was "operators inappropriately terminate HPI". The unsafe action, associated with the HFE, that was selected for the demonstration was described as "Operators turn off operating HPI pumps, given the mistaken belief that the safety injection (SI) termination criteria given in procedures have been satisfied."

Actual plant procedures were used to identify an error-forcing context (EFCS) that could induce the unsafe action and resulting HFE that were selected for the trial application. The EFCS selected was: a stuck open power operated relief valve causing pressurizer level indication to read incorrectly, coupled with PSFs and errors in information processing. A quantification demonstration resulted in an HFE probability of 7.5E-4 and a core damage frequency of 1.5E-5. These calculations demonstrate that HFEs can be significant contributors to plant risk when considered under an appropriate EFCS.

The trial application was a "proof of concept" for ATHEANA; it demonstrated that it is possible to identify and estimate the probabilities of HFEs (and associated EFCS) that have an observable impact on the frequency of core damage, and which are generally not included in current PRAs.

A general process was outlined that addresses the iterative steps of defining HFEs and estimating their probabilities using search schemes.

A knowledge-base was developed with the objective of describing the links between unsafe actions and error-forcing contexts, and is based on behavioral science theory and analysis of NPP events.

In the Implementation Phase, there are several activities that are required to complete the development of ATHEANA. The most important of these activities is the development of the ATHEANA application tools. These tools are 1) the implementation guidelines, which is to be a "how to" document, and 2) the frame-of-reference (FOR) manual, which is a technical basis document. The Frame-of-Reference manual has been completed in draft form,[6] and is discussed briefly in the following paragraph.

Tools of ATHEANA: The Frame-of-Reference Manual

The purpose of the Frame-of-Reference manual is to provide information to analysts using ATHEANA for human reliability analyses. The information given allows analysts to use "lessons learned" in developing ATHEANA without having to repeat the creation process.

The method is based on the following three principal sources of information:

- models of human errors and their causes,
- knowledge of power plant design, operations, behavior during upset conditions, and probabilistic risk assessments, and
- analyses of the course of operational events that have 'involved significant contributions of human failure.

The models of human errors and their causes that form one of the three bases of the method

emerged in the behavioral sciences in the late 1980s and early 1990s, partly as a result of the major industrial accidents such as Three Mile Island and Chernobyl in the nuclear industry, and others in the transportation, aerospace, and chemical industries. These models provide the basis for the judgements needed to apply the method. The analyses of operational events have confirmed the principles developed from the models and provide examples from the "real world" of the kinds of events that can occur. However, it is important to recognize that the events analyzed do not constitute a large enough database for modeling new events; there simply are not enough thoroughly documented events that have occurred to provide data.

These sources of information are used in ATHEANA to give: (1) a structure for searching for human failure events to be included in PRAS, and in particular, new events representing the results of inappropriate actions that have been missing from PRAs performed to date; (2) a basis for the estimation of the probabilities of the human failure events (HFEs); and (3) examples of events to support the expert judgment required in ATHEANA.

This Frame-of-Reference manual is complementary to the future Implementation Guidelines manual that has step-by-step instructions on applying ATHEANA.

As mentioned previously, the Frame-of-Reference manual was developed in preliminary form in FY 1996; it contains the following major parts:

Part I Principles and Concepts

This part explains the underlying principles that have led to the current form of the ATHEANA method, why the judgments inherent in the method are required and what kinds of bases exist for these judgments.

Part 2 Confirmation of Principles

This part describes the understanding of human error and the causes of unsafe actions derived from behavioral science models. It also describes the analyses of several actual events that have taken place at US. nuclear power plants in recent years that have involved human errors as major contributing factors. These analyses arc based on the concepts of ATHEANA and illustrate these concepts using operational experience.

Part 3 The ATHEANA Knowledge Base

This part describes how the ideas presented in this Frame-of-Reference manual are used to help make the judgments inherent in ATHEANA. It also presents the knowledge gained from the behavioral models and the analysis of operational events in a form that is compatible with the needs of the Implementation Guidelines. This section is the interface between the knowledge-base and the application process.

ATHEANA Search Aids

A significant part of the knowledge base mentioned above, ATHEANA search aids are provided to help the analyst structure the search for human failure events (HFEs), unsafe acts (UAs), and associated error-forcing contexts (EFCs). This tabular information is composed of generic insights from behavioral science and past operational experience as well as event-specific, illustrative examples. The ATHEANA Implementation Guidelines will provide guidance on how this information should be used and applied. Corresponding with the current structure and organization of ATHEANA search processes, preliminary information is given for identifying the following:

- Human Failure Events and Unsafe Actions
- "Reasons" for Unsafe Actions
- Error-Forcing Context Elements

Future

Future efforts will focus on:

- Finalizing the Frame-of-Reference Manual and developing/finding the Implementation Guidelines.

- Demonstrations will be conducted using internal as well as second party personnel.

- In addition to its intended use of providing more comprehensive HFEs and more accurate quantification, other valuable uses of the ATHEANA methodology should be examined, such as root cause analysis and a structured approach to incident analysis/investigation to identify and correct the underlying causes of human error.

References

1. NUREG/CR-6093, An Analysis of Operational Experience during LP&S and a Plan for Addressing Human Reliability Assessment Issues, M.T. Barriere, et al, Brookhaven National Laboratory, and Sandia National Laboratories, June 1994.

2. NUREG/CR-6265, Multidisciplinary Framework for Analyzing Errors of commission and Dependencies in Human Reliability Analysis, M.T. Barriere, et al., Brookhaven National Laboratory, August 1995.

3. NUREG/CR-6350, BNL-NUREG-52467, A Technique for Human Error Analysis (ATHEANA), S. Cooper, et al., Brookhaven National Laboratory, 1995.

4. Technical Report L-2415/95-2, Process Description for ATHEANA: A Technique for Human Error Analysis, G.W. Parry, et al., Brookhaven National Laboratory, December 1995.

5. Technical Report L-2415/95-1, Human-System Event Classification Scheme (HSECS) Database Description, S. Cooper, W. Luckas, J. Wreathall, Brookhaven National Laboratory, December 1995.

6. Draft Technical Report L-2415/96-1, Frame-of-Reference Manual for ATHEANA: A Technique for Human Error Analysis, J. Taylor, et al., Brookhaven National Laboratory, June 1996.

SAPHIRE MODELS AND SOFTWARE FOR ASP EVALUATIONS

Martin B. Sattison
Lockheed Martin Idaho Technologies Company
Idaho National Engineering Laboratory
P.O. Box 1625
Idaho Falls, Idaho 83415-3850

ABSTRACT

The Idaho National Engineering Laboratory (INEL) over the three years has created 75 plant-specific Accident Sequence Precursor (ASP) models using the SAPHIRE[1] 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 ASP evaluations. These models and software will be the next generation of risk tools for the evaluation of accident precursors by both the U.S. Nuclear Regulatory Commission's (NRC's) Office of Nuclear Reactor Regulation (NRR) and the Office for Analysis and Evaluation of Operational Data (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. Future plans for the ASP models is also presented.

I. 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 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 draft 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 team 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. These models were called "Revision 0" models.

The nine lead plant models plus the Grand Gulf model (a BWR 6 with High Pressure Core Spray) were subjected to a peer review by SAIC. The review comments were catergorized into several groups: 1) those that must be incorporated, 2) those that should be addressed at a later date, and 3) those that were invalid or impractical. Review comments in the first group were tagged as either generic to a group of plants or plant-specific and were incorporated into all 75 ASP models accordingly. The resulting models were called "Revision 1" models. The last of the Revision 1 models were delivered to the NRC in June 1995.

Work then began immediately to develop the next generation of models. With the availability of a simplified risk model for every commercial power plant in the U.S. interest in these models grew rapidly and in areas outside the Accident Sequence Precursor program. Therefore, the next generation of models were called Simplified Plant Analysis Risk (SPAR) Models, Revision 2. These models were changed in four ways: 1) the treatment of emergency ac power in the fault trees was expanded, 2) plant-specific features gleaned by NRR from the

utility Station Blackout Rule responses and the Individual Plant Examination submittals were added to the models, 3) the interdependencies among the feedwater, condensate, and power conversion systems in BWRs were modeled in more detail, and 4) the models were converted to SAPHIRE 5.0. The last of the Revision 2 models were delivered to the NRC in April 1996.

II. THE MODEL STRUCTURE

A. 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.

B. 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 supercomponent basic event may consist of the following components and failure modes:

HPI MDP 1A	Fails to start/run
Discharge check valve	Fails to open/plugs
Suction MOV	Fails to remain open
Discharge MOV	Fails to remain open

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 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 in the older versions of SAPHIRE, (2) the availability of sufficient information to accurately model support systems is limited without putting forth an effort larger than could be afforded in the early phases of this project, and 3) if support systems were deemed important to a particular ASP analysis, the impacts of any support system failures could be explicitly added to the model.

C. 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

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. 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, JCN E8257.

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.

III. MODEL QUANTIFICATION

The ASP models were originally 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.

With the conversion to SAPHIRE 5.0 for the Revision 2 models, a truncation of 1.0E-15/hour was used for sequence cutset generation. With the increased capabilities of the software, the analyst can rapidly regenerate accident sequence cutsets to whatever truncation desired. Thus, it is no longer desirable to have all possible sequence cutsets available to the user all the time.

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. Revision 3 models will address uncertainty.

IV. 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, GEM. 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 extremely 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 then requantified to determine the CCDP. The difference between the base case and the condition case is the event importance.

GEM 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 (CCDP) and the event importance.

V. CURRENT WORK AND FUTURE PLANS

All 75 Revision 2 models are currently undergoing a quality assurrance review at Sandia National Laboratories (SNL). The review comments are being resolved and incorporated into the models as deemed appropriate by the NRC/INEL/SNL team. The resulting models are called "Revision 2 QA" models. These models should be completed in the January/February 1997 timeframe.

Work is also currently underway to make large advances in the SPAR models. Based on the Revision 2 QA models, the following changes will be reflected in the Revision 3 models: 1) support system models will be added, 2) additions will be made to the event trees to allow assignement of plant damage states to the accident sequences for Level 2 and 3 ASP evaluations, 3) modifications will be made to the human error and recovery action models and methods to more accurately depict the dependencies that exist, 4) the quantification of common cause failure basic events will be converted from the Multiple Greek Letter method to the Alpha method, and 5) information will be added to allow uncertainty calculations. The Revision 3 models are scheduled to be completed in August 1998.

V. 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.

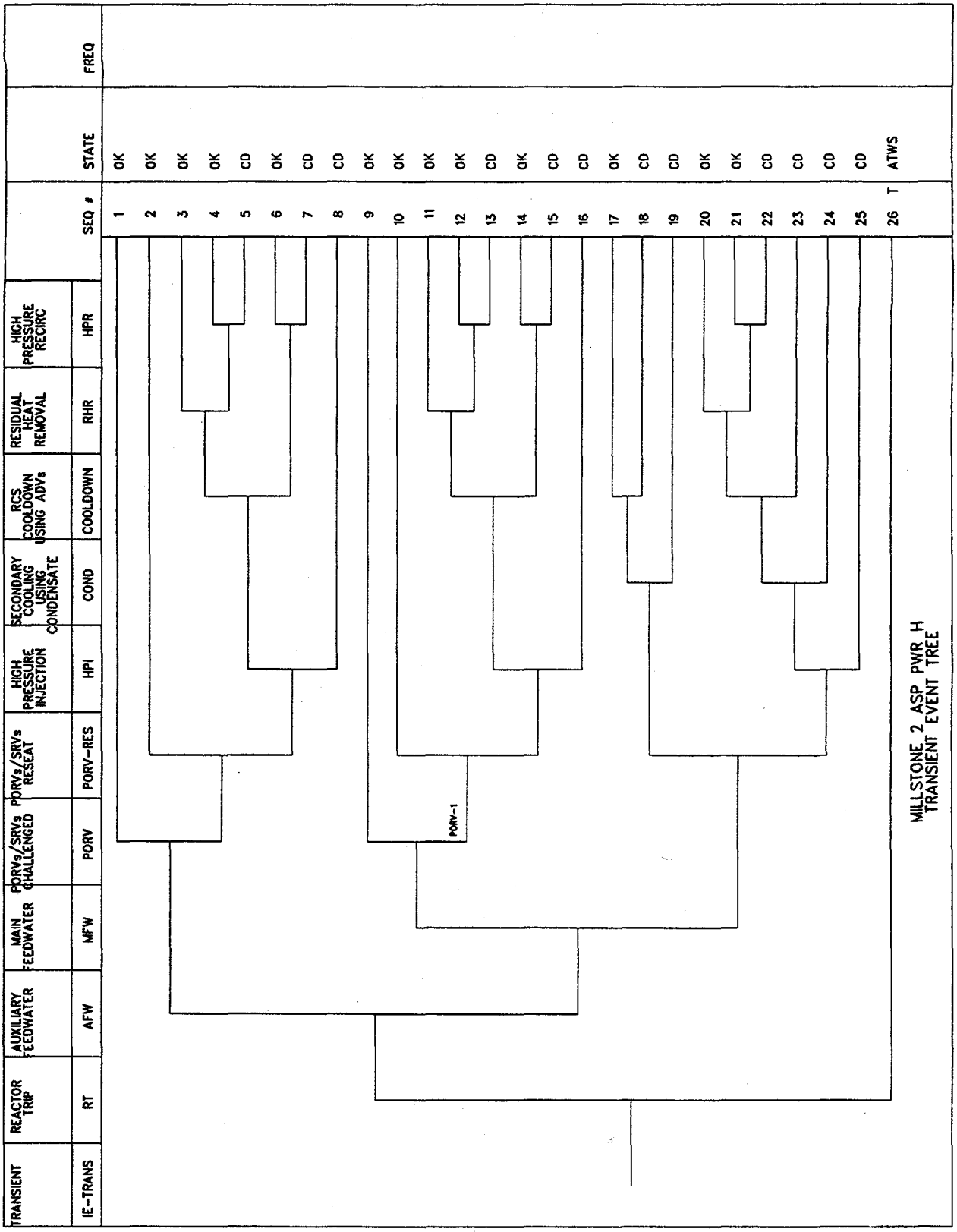
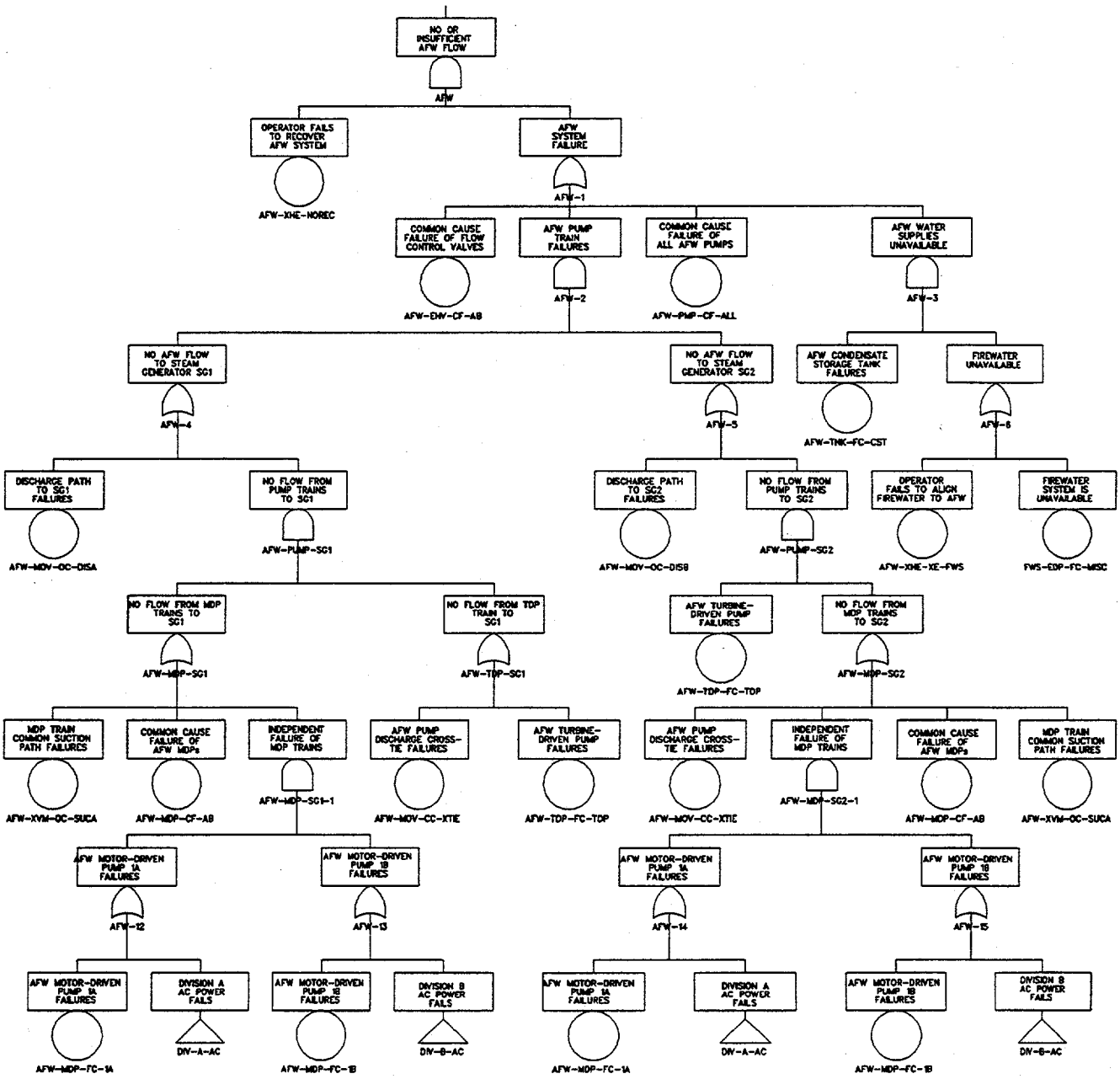


Figure 1. Millstone 2 transient event tree.



MILLSTONE 2 ASP PWR H
AUXILIARY FEEDWATER
1-OF-3 TRAINS TO 1-OF-2 SGs
FOR SUCCESS

Figure 2. Millstone 2 Auxiliary Feedwater System fault tree.

ASSESSMENT OF SPENT FUEL COOLING

J.G. Ibarra, W.R. Jones, G.F. Lanik, H.L. Ornstein, S.V. Pullani

U.S. Nuclear Regulatory Commission
Office for Analysis and Evaluation of Operational Data

ABSTRACT

The paper presents the methodology, the findings, and the conclusions of a study that was done by the Nuclear Regulatory Commission's Office for Analysis and Evaluation of Operational Data (AEOD) on loss of spent fuel pool cooling. The study involved an examination of spent fuel pool designs, operating experience, operating practices, and procedures. AEOD's work was augmented in the area of statistics and probabilistic risk assessment by experts from the Idaho Nuclear Engineering Laboratory. Operating experience was integrated into a probabilistic risk assessment to gain insight on the risks from spent fuel pools.

EXECUTIVE SUMMARY

As directed by the Executive Director for Operations, the Office for Analysis and Evaluation of Operational Data (AEOD) has performed an independent assessment of the likelihood and consequences of an extended loss of spent fuel pool (SFP) cooling. The overall conclusions are that the typical plant may need improvements in SFP instrumentation, operator procedures and training, and configuration control.

Six site visits were conducted to gain an understanding of the licensees' SFP physical configuration, practices, and operating procedures. The assessment found great variation in the designs and capabilities of SFPs and systems at individual nuclear plants.

In November 1992, two contractors working at the Susquehanna Steam Electric Station submitted a defects and noncompliance report on the Susquehanna SFP to the U.S. Nuclear Regulatory Commission. They were interviewed by AEOD to better understand their concerns. Their report, which has potential generic implications, provided the impetus for the NRC and the nuclear industry to take a closer look at the SFPs.

AEOD reviewed the applicable SFP regulations and the NRC Standard Review Plan for the acceptance criteria and the applicable Regulatory Guides. Because of the evolution of the criteria and the different times that reactors were licensed, the criteria to evaluate the SFP designs varies among the operating facilities.

AEOD performed independent assessments of the electrical systems, instrumentation, heat loads, and radiation. These assessments were utilized to determine the typical SFP configurations and potential problems.

Utilizing a previous Susquehanna risk analysis, Idaho National Engineering Laboratory performed model refinements that resulted in better estimates of near boiling frequencies. No quantitative estimates of core damage were performed but the analysis provided qualitative insights for identification of improvements in the SFPs to lessen the risks of events.

The conclusions are:

- Review of more than 12 years of operating experience determined that loss of SFP coolant inventory greater than 1 foot has occurred at a rate of about 1 per 100 reactor years. Loss of SFP cooling with a temperature increase greater than 20 °F has occurred at a rate of approximately 3 per 1000 reactor years. The consequences of these actual events have not been severe. However, events have resulted in loss of several feet of SFP coolant level and have gone on in excess of 24 hours. The primary cause of these events has been human error.

- Review of existing SFP risk assessments found that after correction for several problems in the analyses, the relative risk due to loss of spent fuel cooling is low in comparison with the risk of events not involving the SFP. The review determined that the likelihood and consequences of loss of SFP cooling events are highly dependent on human performance and individual plant design features.

- The need for specific corrective actions should be evaluated for those plants where failures of reactor cavity seal or gate seals, or ineffective antisiphon devices could potentially cause loss of SFP coolant inventory sufficient to uncover the fuel or endanger makeup capability.

- The need for improvements to configuration controls related to the SFP to prevent and/or mitigate SFP loss of inventory events and loss of cooling events should be evaluated on a plant specific basis.

- The need for plant modifications at some multiunit sites to account for the potential effects of SFP boiling conditions on safe shutdown equipment for the operating unit, particularly during full core off-loads, should be evaluated on a plant specific basis.

- Efforts by utilities to reduce outage duration have resulted in full core offloads occurring earlier in outages. This increased fuel pool heat load reduces the time available to recover from a loss of SFP cooling event early in the outage.

- The need for improved procedures and training for control room operators to respond to SFP loss of inventory and SFP loss of cooling events consistent with the time frames over which events can proceed, recognizing the heat load and the possibility of loss of inventory, should be evaluated on a plant specific basis.

- The need for improvements to instrumentation and power supplies to the SFP equipment to aid correct operator response to SFP events should be evaluated on a plant specific basis.

1 INTRODUCTION

In recent years there have been several instances in which the adequacy of spent fuel pool (SFP) cooling systems has been brought into question. For example, two contractors at Susquehanna Steam Electric Station plant, submitted a Title 10 of the *Code of Federal Regulations* (10 CFR) (Ref. 1) Part 21 report (Ref. 2) on the adequacy of SFP cooling at Susquehanna.

The "Susquehanna" 10 CFR 21 report postulated loss of SFP cooling resulting in boiling of the SFP, failure of emergency core cooling system (ECCS) and other equipment due to steam releases and condensation of SFP vapors, reactor core heatup and damage, spent fuel heatup and damage, and large offsite radioactivity releases.

The AEOD study:

- Developed generic configurations delineating SFP equipment for a boiling-water reactor (BWR) and a pressurized-water reactor (PWR) and utilized these generic configurations to assess the loss of SFP cooling and inventory.

- Reviewed and assessed 12 years of operational experience for both domestic reactors and foreign reactors with designs similar to that of the US.

- Performed six site visits to gather information on SFP physical configuration, practices, and procedures; and conducted interviews with the authors of the 10 CFR 21 report to better understand their concerns.

- Reviewed applicable SFP regulations and the NRC Standard Review Plan (SRP) for the acceptance criteria and applicable Regulatory Guides.

- Performed independent assessments of electrical systems, instrumentation, heat loads, and radiation to better understand the role of these issues to loss of SFP cooling.

- Contracted with Idaho National Engineering Laboratory (INEL) to review existing risk analyses and use risk assessment techniques to evaluate the risk of losing SFP cooling and coolant inventory.

2 SPENT FUEL COOLING

A survey of SFPs indicates that a wide variety of configurations exists. Since most plants were built prior to issuance of specific NRC regulatory guidance, diverse designs would be expected. For purposes of this study, loss of spent fuel cooling is considered to include subcategories of loss of SFP coolant inventory and loss of SFP cooling; this convention will be used throughout. Potential problems with SFP coolant inventory and SFP cooling which can lead to loss of spent fuel cooling are discussed. The potential consequences of loss of spent fuel cooling are considered. Once the problems have been identified, possible approaches to prevention and response to loss of spent fuel cooling situations are described.

Figure 2.1 shows a "generic" PWR SFP and Figure 2.2 shows a "generic" BWR SFP.

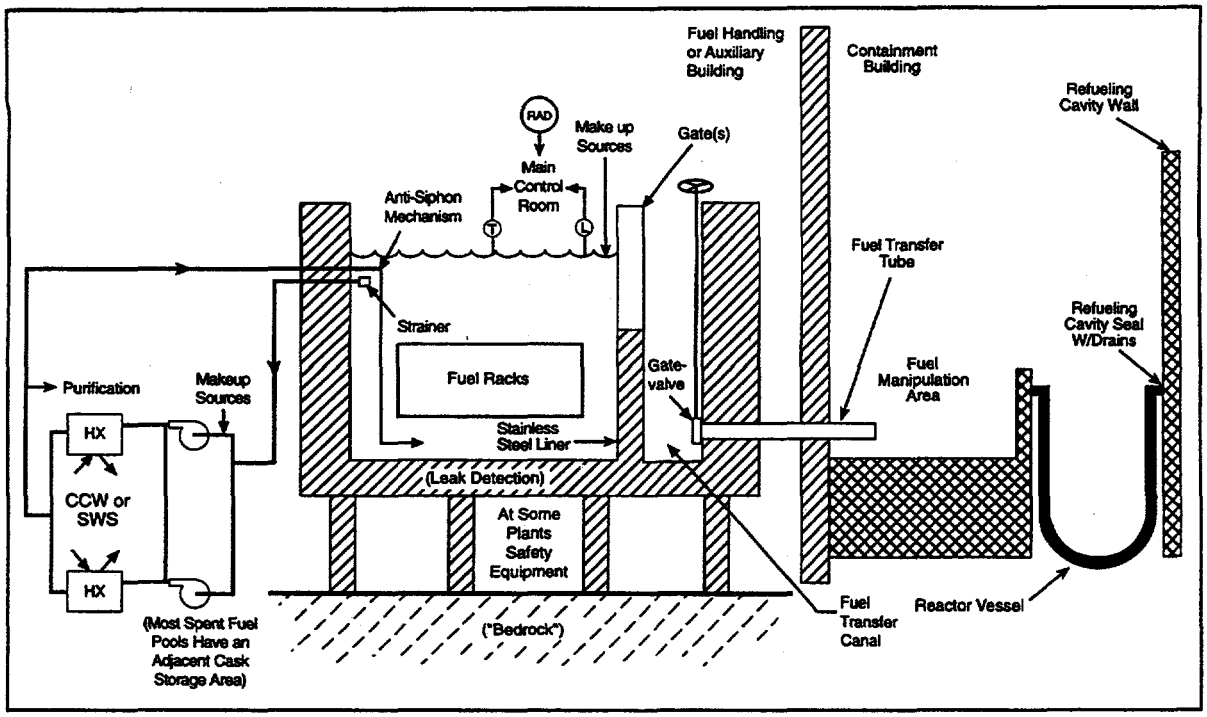


Figure 2.1 PWR Spent Fuel Cooling Systems

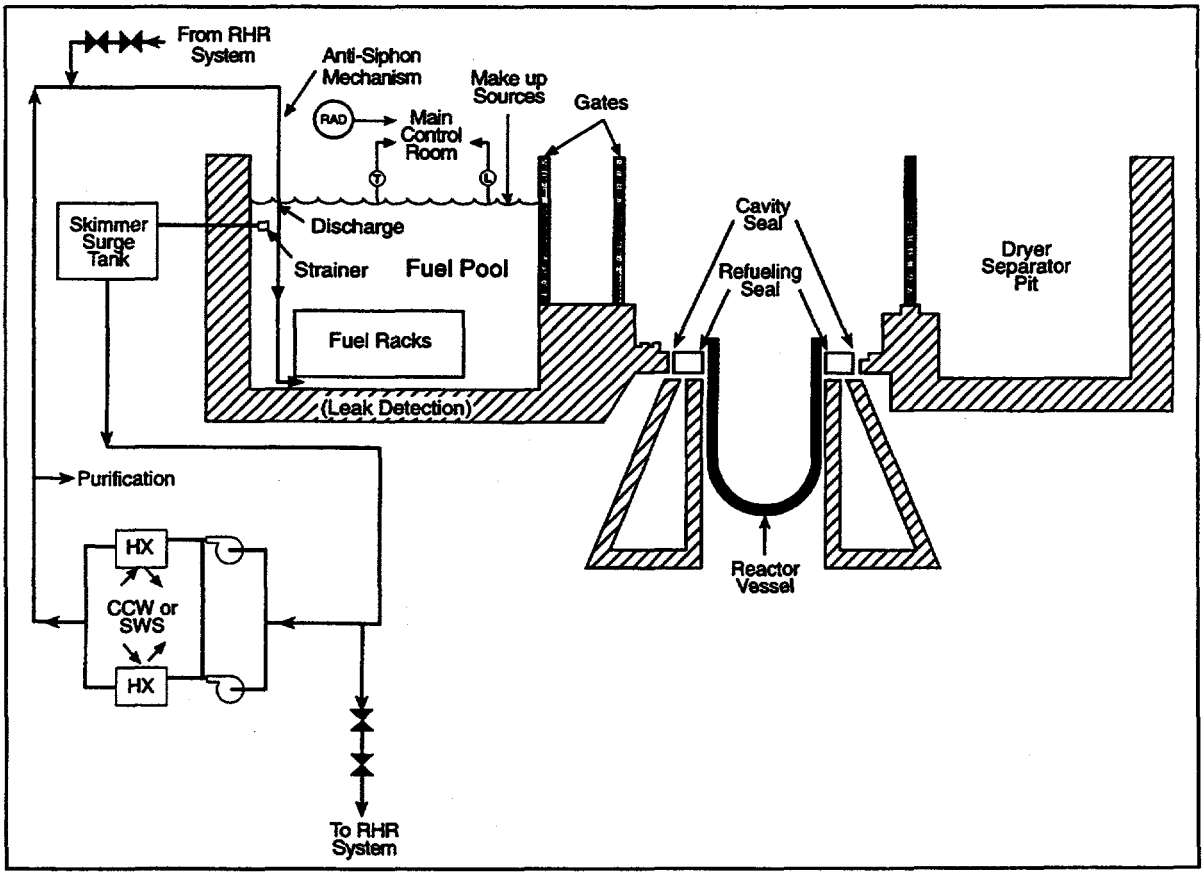


Figure 2.2 BWR Spent Fuel Cooling Systems

The following discussion considers potential scenarios which can lead to loss of spent fuel cooling due to (1) loss of SFP coolant inventory sufficient to interrupt heat transfer to the cooling system or result in uncovery of the fuel and (2) failure of the SFP cooling system pumps and heat exchangers to transfer heat from the pool to the ultimate heat sink. Figure 2.3 is a schematic classification of the types of events which could lead to loss of spent fuel cooling.

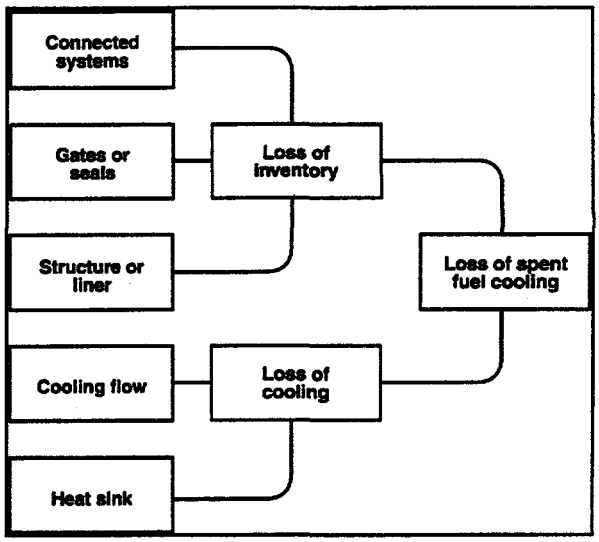


Figure 2.3 Loss of Spent Fuel Cooling

2.1 Loss of Spent Fuel Pool Coolant Inventory

The primary pathways for loss of SFP coolant inventory can be broadly categorized as (1) loss through connected systems, (2) leakage through movable gates or seals, and (3) leakage through or failure of the fuel pool or the fuel pool liner.

2.1.1 Connected Systems

Piping connected to the SFP may include the SFP cooling and purification system, the spent fuel shipping cask pool and fuel transfer canal drains, and, when in communication with the reactor during refueling operations, reactor piping systems such as the residual heat removal (RHR) system and the chemical and volume control system.

Losses through connected systems could include both pipe breaks or leaks and configuration control problems. Piping systems which extend down into the SFP have the potential to siphon. For most designs, the loss of SFP coolant inventory via the SFP cooling system piping, whether initiated due to a pipe break or configuration control problem, would be limited due to antisiphon devices. However, siphoning can occur if the antisiphon devices are incorrectly designed, are plugged, or otherwise fail. A recent survey of all power reactors conducted by the Office of Nuclear Reactor Regulation (NRR) (Ref. 3) determined that some sites do not have antisiphon devices in potential siphon paths.

During refueling operations, when a flow path exists to the reactor vessel, inventory loss through the RHR, chemical and volume control system, or reactor cavity drains would not be limited by the antisiphon devices; the same applies when the SFP is open to the spent fuel shipping cask pool drains. For these situations, for many designs, the extent of the inventory loss is limited by internal weirs or drain path elevations which maintain level above the top of the stored fuel in the SFP.

2.1.2 Gates and Seals

A second classification of inventory loss is through movable gates or seals and, during refueling operations, the reactor cavity seal. As shown in Figures 2.1 and 2.2, both PWRs and BWRs have seals which keep water above the vessel in the refueling cavity during refueling. For BWRs, there are usually two seals required to keep refueling water above the reactor vessel; in Figure 2.2 these seals are referred to as the refueling seal and the cavity seal. Some plants use inflatable bladders to

form a seal between the reactor vessel flange and the containment building (PWRs) or the drywell, and the reactor building (BWRs). In some BWRs, these cavity seals are permanent spring steel bellows which are expected to have little susceptibility to large leaks. There are several other types of seals used which do not rely on inflatable bladders. These include bolted cavity seal rings which use gaskets to seal between mating surfaces and permanent seals which are welded in place. These types of seals are not prone to rapidly developing large leaks.

The refueling cavity seal and movable gate seals at some plants are inflatable seals of many different designs. Depending on physical relationship of adjacent structures, catastrophic failure of an inflatable seal could result in rapid loss of inventory. However, the geometry of the relationship between the SFP, adjacent cavities, reactor vessel, and connecting structures must be considered in evaluating the vulnerability to loss of SFP coolant inventory due to inflatable seals. Many seal failures will result in only limited level loss because of the various physical configurations.

In BWRs, the bottom of the movable gate separating the reactor cavity from the SFP is generally above the top of the stored fuel so that for a loss of the cavity seal the level in the SFP will remain above the top of the fuel. Although the fuel would not immediately uncover, SFP cooling would be lost due to SFP pumps tripping on loss of suction; and the remaining SFP coolant inventory would heat up to near boiling within a few hours. Also, because of reduced water level above the fuel, high radiation fields would inhibit access to the refueling floor. Plants which have gate bottoms or internal weirs which limit the draindown from cavity seal or gate seal failures to a level that would continue to provide sufficient radiation shielding to not hinder operator actions would be more likely to be able to mitigate these events. When not in refueling, most BWRs have two gates in series at major openings.

Where PWRs do not have interposing structures between the fuel transfer tube and the SFP or where the gates between the SFP fuel transfer canal are left open, a vulnerability to loss of SFP coolant inventory through the fuel transfer tube is increased. The NRR survey assessment found that only five SFPs have fuel transfer tubes which are lower than the top of the stored fuel without interposing structures.

2.1.3 Pool Structure or Liner

Finally, inventory loss could occur directly due to SFP liner leakage or gross failure of the SFP structure. The impacts of drop of a heavy load or a seismic event are potential causes of gross failure. SFPs are designed to survive seismic events. Radiological and structural response and makeup capability for drops of light loads (those weighing no more than a fuel assembly) are bounded by analyses of a fuel handling accident. On the other hand, drops of heavy loads have the potential to exceed the design basis of the fuel pool structure and the make-up system. Thus, heavy load control programs have been instituted to evaluate potential heavy load drops or implement special controls on the design and operation of heavy load handling equipment.

2.1.4 Consequences of Loss of Spent Fuel Pool Coolant Inventory

For a large loss of SFP inventory, the primary consequence is potential uncovery of the stored fuel. Given the unlikely occurrence of a large leak at the bottom of the SFP structure, beyond the available make-up capacity, the fuel could uncover and heat up to the point of clad damage and release of

fission products. The uncovery of the fuel would also result in extremely high radiation fields around the SFP area.

A more likely sequence would be a loss of inventory through a gate or seal which would terminate when the level reached the elevation of the leak. Then, due to the decreased inventory of water in the SFP and the loss of suction to the SFP cooling system, the remaining water in the pool would boil away until the fuel was uncovered. Unless corrective actions were taken, the final consequences would be similar to loss of SFP coolant inventory described above.

Loss of SFP coolant inventory events for which corrective actions are taken prior to the severe consequences described above have the potential for other problems. Even a minor loss of SFP coolant inventory can lead to loss of SFP cooling because the lower SFP level causes loss of suction to the SFP cooling system. Losses of SFP coolant inventory may produce flooding or environmental problems in other areas of the plant. Ventilation and drain systems can transport water and steam to other parts of the plant and impact emergency equipment. A significant amount of water vapor may be generated either by direct boiling or evaporation from the SFP. Various SFP equipment and ventilation configurations may allow the water vapor to accumulate on and cause SFP cooling equipment to fail, further exacerbating the loss of inventory.

Where the SFP area atmospheric water vapor can be transported to areas which house other equipment important to safety, that equipment may be affected. This potential problem is important in some multiunit sites during and immediately following full core off-loads, where the fuel pool atmospheric water vapor from the unit refueling can be transported to areas housing safety equipment for the unit operating at or near full power. In this situation, this transport could cause equipment required for a safe shutdown of the operating unit to be damaged or to fail. This issue is discussed in Section 5.2. Most plants have sufficient flood protection, ventilation, and equipment separation so that this scenario is not a problem. However, according to the NRR survey assessment, eight multiunit sites may be susceptible to this scenario.

2.2 Loss of Spent Fuel Pool Cooling

Figure 2.3 also presents potential causes of loss of cooling to the SFP. Cooling can be lost by loss of SFP cooling flow or due to an ineffective SFP heat sink. Losses of SFP cooling system flow can occur due to several mechanisms including: loss of electrical power to the SFP cooling pumps, pump failure, loss of suction due to loss of level, flow blockage or diversion in the SFP cooling system. Losses of heat sink can occur due to operation with less than the required SFP cooling system complement or with heat loads in the SFP in excess of the SFP cooling system design capability.

2.2.1 Loss of Spent Fuel Pool Cooling System Flow

All SFP cooling pumps are electrically powered. Loss of electrical power to these pumps results in loss of SFP cooling system flow. Loss of electrical power can occur due to losses of offsite power or human error in electrical alignments. Most SFP cooling system pumps have the capability to be loaded on available on site power sources. The NRR survey assessment found that four SFPs did not have the capability to be cooled by systems which could be powered by on site power sources.

The likelihood of an extended loss of SFP cooling due to loss of electrical power to the pumps is fairly low due to the combination of available on site power, the existence of workable procedures for power restoration, the general knowledge of the plant operations staff of the need to restore power and the time available to restore power.

For other than loss of electrical power, failure of both SFP cooling pumps is unlikely. Except for situations where a full core has been transferred to the SFP relatively soon after plant shutdown, a single SFP cooling pump generally provides sufficient cooling.

Losses of SFP coolant can result in losses of cooling flow when the level drops below the suction intake of the SFP cooling pumps. Thus, such losses of inventory will be accompanied by a loss of SFP cooling.

Flow can also be lost due to blockage or diversion. For example, foreign material could clog a filter or strainer in the SFP cooling system. If flow blockage were to occur during a full core off-load, implementation of a backup cooling process might be required to prevent adverse conditions from developing in the SFP.

2.2.2 Ineffective Spent Fuel Pool Heat Sink

SFP cooling system heat exchangers are usually cooled by the component cooling water system or the service water system. An ineffective SFP heat sink can occur due to: misalignment of cooling water sources, failure of the cooling water source, heat exchanger fouling, and insufficient heat exchanger capacity, among others.

Current practice of full core off-loads a short time after shutdown has greatly increased the heat load in the SFP. Any degradation in the heat removal of the cooling system at these times could result in heat up of the SFP. Errors in the calculated heat load or assumption of nonconservative ultimate heat sink temperatures could mislead operators.

2.2.3 Consequences of Loss of SFP Cooling

An extended loss of SFP cooling would result in heat up and boil off of SFP coolant inventory and eventual uncovery of the stored fuel in the unlikely event that no corrective actions were taken. This would result in high levels of radiation in the SFP area and deny personnel access. Clad failure and radiation release could be the final outcome. However, losses of cooling pose less hazard than loss of inventory because loss of cooling does not pose the immediate threat of fuel uncovery. No fuel damage is likely until the fuel is uncovered.

During an extended loss of SFP cooling, water vapor may be generated either by direct boiling or evaporation from the SFP. Various SFP equipment and ventilation configurations may allow the water vapor to condense and accumulate in locations which could affect other equipment. All the potential impacts that apply to the situation described above for loss of SFP coolant inventory leading to generation of steam and water vapor which is transported to other parts of the plant applies to the extended loss of SFP cooling.

2.3 Preventing and Responding to Spent Fuel Pool Events

There are no systems available for automatic response to a loss of SFP coolant inventory or loss of SFP cooling. Consequently, operator actions form the basis for preventing and responding to a loss of spent fuel cooling.

Preventing a loss of SFP coolant inventory due to gate seal failures or cavity seal failures relies on correct installation and testing of the seals, and testing and control of the air supply for the inflatable seals. Better seal performance could be achieved by seal replacement at intervals consistent with manufacturers recommendations or when inspection of seals shows evidence of aging, cracking, or tearing.

The response to loss of inventory events depends, first of all, on timely discovery of the event by the operator. The rate of loss of SFP coolant inventory can vary greatly depending on the cause; for example, water level drop from a reactor cavity seal failure can be quite rapid. The reduction in level during these events is usually discovered either by direct observation by operations staff in the spent fuel area or due to alarm actuation in the control room. Reliable and accurate instruments and annunciators can alert the operator to a SFP event. If the operators are aware of a SFP event in a timely manner, the large volume of water in the SFP will usually allow sufficient opportunity for operator response to diagnose and correct the problem.

Response to loss of SFP cooling requires effective instrumentation, procedures and training. Most operating situations would allow a relatively long time to respond to such an event. However, following a full core off-load, the SFP could heat up to near boiling in a few hours. Operators would attempt to restore cooling either by correcting any problems with the SFP cooling system, or by initiating operation of backup cooling systems, if available.

As with prevention and response to SFP coolant inventory events, prevention and response to loss of SFP cooling is also largely dependent on configuration control and human performance. The primary concern is to maintain electrical power to the equipment involved in SFP cooling.

3 OPERATING EXPERIENCE

Operating experience with SFP loss of coolant inventory and loss of cooling was reviewed. The primary source of information was licensee event reports (LERs) from 1984 through early 1996, screened from the Sequence Coding and Search System. In some cases, events before 1984 were included due to sparse data for some types of events. Additional information sources included event notifications made in accordance with 10 CFR 50.72, NRC Inspection Reports, NRC regional morning reports, NRC preliminary notifications, and industry communications. More than 700 separate sources of information were reviewed. This screening process resulted in about 260 events related to SFPs. Table 3.1 is a summary of these SFP events listing the number of events of each type under the two main categories (loss of SFP coolant inventory and loss of SFP cooling). That table indicates that numerous precursor events were found during the study. These precursor conditions represent potential losses of SFP coolant inventory or loss of SFP cooling given the condition which did occur plus other postulated failures.

The operating events obtained in this study provide a reasonable representation of experience with SFPs. However, during discussions with operations staff, a number of additional events were discovered which provide insights into problems with SFPs. While these events have been included in this study, they were not initially captured by the study's event review process, primarily because some relevant events are below the reporting threshold required by NRC regulations.

Table 3.1 Spent Fuel Pool Events

Type of Event	Actual	Precursor
SFP Inventory	38	55
Connected Systems	20	12
Gates and Seals	10	8
Structure or Liner	8	35
SFP Cooling	56	22
Cooling Flow	50	20
Heat Sink	6	2

3.1 Loss of Spent Fuel Pool Coolant Inventory

About 38 events involved actual loss of SFP coolant or refueling water. There were about 55 precursor events. Table 3.2 provides some details about loss of SFP coolant inventory events. Figures 3.1 and 3.2 provide an overview of the SFP loss of coolant inventory events for which level drops and duration times could be quantified. These figures show that SFP losses of coolant inventory have been infrequent. However, several events have lasted more than 12 hours and about 10 events have resulted in level decreases of more than 1 foot before the event was terminated. The low number of events found with smaller level changes may be due to a lack of reporting of such events.

Using the number of events found during this study over a period of about 12 years for which level drops could be quantified, the frequency of loss of inventory events in which loss of more than 1 foot occurred can be estimated to be on the order of less than 1 per 100 reactor years.

Table 3.2 Loss of Coolant Inventory Events

Type of Event	Actual	Precursor
Connected Systems	20	12
Configuration Control	16	2
Siphoning	3	1
PWR Transfer Tube	1	1
Piping	0	1
Piping Seismic Design	0	7
Gates and Seals	10	8
Cavity Seals	0	6
Gate Seals	10	2
Pool Structure or Liner	8	35
Liner Leaks	7	1
Load Drops	1	32
Pool Seismic Design	0	2

3.1.1 Connected Systems

The majority of losses of SFP coolant inventory through connected systems was due to configuration control problems. These connected systems include: the SFP cooling and purification system, a spent fuel shipping cask pool, sources of make-up, the fuel transfer tube(s) (in PWRs), the fuel transfer canal (in BWRs), and, during refueling, the reactor.

Configuration Control

Sixteen loss of SFP coolant inventory events were due to configuration control errors. These events are about equally distributed between BWRs and PWRs. Two recent configuration control events are described here.

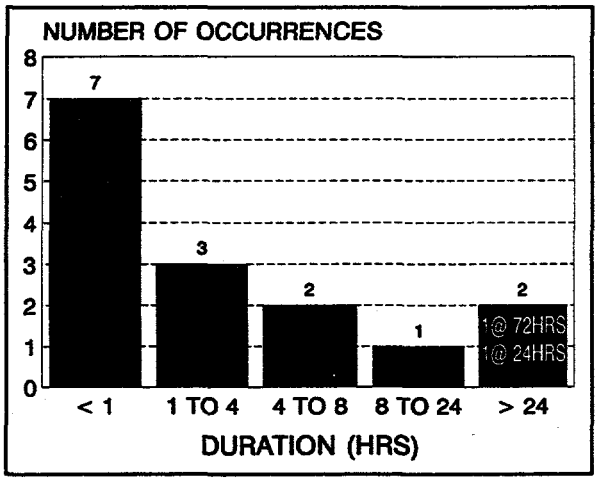


Figure 3.1 Loss of Inventory Duration

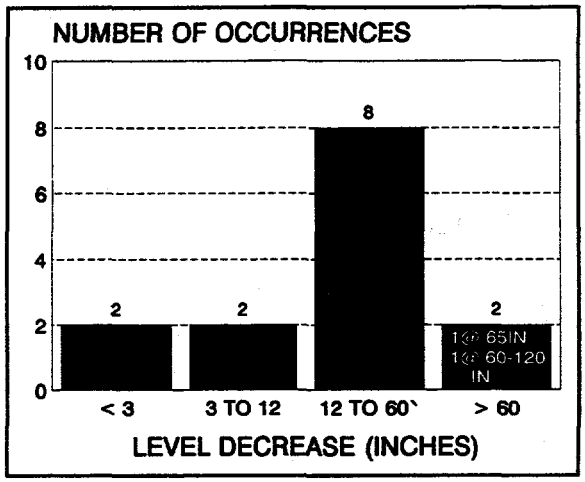


Figure 3.2 Loss of Inventory Levels

At Cooper Station on October 31, 1995, about 10,000 gallons of refueling water were inadvertently lost from the refueling cavity and transferred to the plant's low level waste system (Ref. 4). At the time, the full core had been placed in the SFP, the reactor refueling cavity was filled with refueling water, and the refueling gates were open. A cable from a remote video camera came in contact with and caused a submerged valve to open. The valve was part of the main steam line plug. This allowed refueling water to flow to the main steam line drains. About 30 minutes after the valve was opened, the SFP surge tank low level alarm alerted the operations staff to an ongoing loss of water. While the operations staff started to add water, the make-up was not sufficient to avoid tripping both SFP cooling pumps on low suction pressure. One SFP cooling pump was restarted in about 3 minutes with no observed increase in SFP temperature. About 40 minutes later, the source of the inventory loss was identified and the valve was closed. This event resulted in reduction of about 1 inch in the refueling cavity and SFP. There was still more that 23 feet of water above fuel in the SFP. This was a fairly slow drainage rate.

At Millstone Unit 2 on July 6, 1992, about 10,000 gallons of SFP water was drained to the reactor coolant system (RCS). At the time of the event, the unit had been shut down about 37 days and the full core had been placed in the SFP. A loss of normal power resulted in loss of SFP cooling. During the response to the event, the operations staff decided to align the shutdown cooling system to provide cooling to the SFP. However, during the alignment process, a flow path was created which permitted flow via a gravity drain from the SFP to the RCS. SFP level dropped about 14 inches. Based on available reported information, there was at least 23 feet of water above the fuel because no Technical Specification violation was reported. A 4 °F temperature rise occurred before SFP cooling was restored (Ref. 5).

Siphoning

Although reported operating experience with siphons (both actual events and precursor conditions) is very sparse (three actual events), losses of SFP coolant inventory have occurred because of siphoning problems. One event at River Bend on September 20, 1987, (Ref. 6) involved plugging of a single (nonredundant) vertical vent pipe acting as an antisiphon device. In this event, the SFP coolant loss due to siphoning was masked by the SFP low level annunciator being in the alarm condition due

to other ongoing plant work. The event lasted about one-half hour. This event was terminated when a radiation alarm occurred coincident with a high level in the tank receiving the SFP water. This event resulted in loss of SFP level of between 5 and 10 feet, one of the largest level decreases found in the study. Further, it is not clear how far the level would have fallen had no operator action occurred.

In another event at San Onofre Unit 2 on June 22, 1988, (Ref. 7) about 9000 gallons of SFP coolant drained from the SFP to the reactor cavity through the SFP purification system due to lack of siphon protection in that system. This event lasted about 5.5 hours. The licensee stated that this condition would be corrected by providing siphon protection. The licensee determined that the minimum amount of water above top of active fuel in the SFP would be about 13 feet if the operations staff failed to respond to two alarms.

Another event at Davis Besse on February 1, 1982, (Ref. 8) involved a temporary pump used to fill the SFP which created a siphon path when the pump was secured. In this event, about 21 feet 9 inches remained above the fuel.

One precursor event was reported in which antisiphon holes in the two SFP cooling return lines were not present even though 0.5-inch holes were previously thought to exist. Also, further investigation indicated that the 0.5-inch holes would not have been adequate to stop a siphon given postulated failures.

Pressurized-Water Reactor Transfer Tube

Only one actual event was found in which the transfer tube actually leaked while closed. In this event, the SFP end of the transfer tube was open and the flange on the containment end of the transfer tube leaked. AEOD was informed during some site visits that minor leakage through transfer tubes has occurred.

One site (Oconee Units 1 and 2) has a fuel transfer tube which has piping penetrations at a level 6 feet below the top of the spent fuel in the SFP. This penetration is used during operation of the Oconee Standby Shutdown Facility. This facility has a mission time of 72 hours. Water is taken from the SFP through the transfer tube via the penetration and injected into the reactor coolant pump seals for cooling. In this design, continued use of SFP coolant inventory for reactor coolant pump seals could have caused radiation doses in the SFP to reach high levels such that make-up to the SFP would be impossible. This problem has been corrected by adding remote make-up capability to the SFPs.

Piping and Piping Seismic Design

No actual events were found where SFP system piping actually leaked, causing a loss of SFP coolant inventory. However, there have been a variety of seismic piping design problems reported. The most prevalent type of problem involves use of the nonseismic SFP purification system for purification of the large sources of refueling water in both BWRs and in PWRs. Failure of the nonseismic SFP purification system while connected to the refueling water source could cause loss of this source as make-up to the SFP as well as compromise these sources as ECCS sources. In addition, other minor piping seismic design problems were discovered and reported.

3.1.2 Gates and Seals

Large losses of SFP coolant inventory have occurred through SFP gate seals. Also, there is a potential for large losses of SFP coolant inventory through reactor cavity seals.

Refueling Cavity Seals

There have been at least two rapidly developing leaks due to inflatable reactor cavity seals. In both these cases, the SFP was isolated from the reactor cavity by the closed fuel transfer tube prior to the event. At Haddam Neck on August 21, 1984, the seal failed and about 200,000 gallons of water were drained to the containment building in about 20 minutes. At Surry Unit 1 on May 17, 1988, with all the fuel in the SFP, the seal failed and about 25,800 gallons were drained to the containment in about one-half hour. In the case of Surry, the instrument air supply to the containment was isolated and a backup nitrogen supply was used to reinflate the seal. Problems resulted in the inflatable seal deflating enough to cause leakage. While in both these cases, the SFP was not connected to the reactor cavity, these events and an additional four events discussed below are precursors which indicate the possibility of failure of the cavity seals and consequent loss of inventory. Review of individual plant specific geometry is required to evaluate each plant's vulnerability to this type event.

This study found four additional events in which cavity seals failed tests prior to flooding the refueling cavity or where leaks developed in the seals following refueling. These events indicate that testing of inflatable seals is important in ensuring their operability. The events further emphasize the need to be aware of potential failures. Most of these events involved design problems. Only one was due to failure to maintain an adequate air supply to the inflatable seal. One event involved a gasket type (noninflatable) seal which leaked during the draining operation following the refueling.

Gates

The second most prevalent type of loss of SFP coolant inventory (10 events) was leaking fuel pool gates. The majority of these leaks were due to failure to maintain the air supply to the gate seals. In one case, there was a failure to completely inflate the seal. The majority of the air supply events was due to human error. Three of these events involved failed or disconnected level instrumentation. Most of these events occurred at PWRs. Leaks were generally large, involving tens of thousands of gallons of water, and 2 or more feet of SFP level decrease. Level drop rates ranged from fractions of a foot per hour up to several feet per hour. These rates seem a reasonable pace to deal with and, in fact, in these events, the operations staffs responded and restored level effectively.

One event, at Hatch on December 2, 1986, resulted in the fuel pool level dropping about 5.5 feet (Ref. 9). This event resulted from isolating the single air supply to the transfer canal's six gate seals. The seals partially deflated. This deflation resulted in a path for SFP water to go to the gap between the two unit reactor buildings and into areas of both units' reactor buildings. When the source of the leak was discovered, the air source was restored and the leak was stopped. However, the event lasted about 24 hours. During this time, the SFP level was noted to be low and make-up was performed several times without attempts to determine the cause. The leak detection alarm was miscalibrated and a drain valve was left open which defeated or impaired the ability to detect a leak from the transfer canal gates. Subsequent corrective action included alternate supplies for alternate

gate seals such that inner seals were supplied from one unit and outer seals were supplied from the other unit so that a degree of redundancy was established.

3.1.3 Pool Structure or Liner

No events involving major SFP leakage have been reported. However, some events involved small leaks or potential leaks.

Liner

There were seven events involving leaking from the fuel pool liner. These events generally involved relatively small leak rates (less than about 50 gallons per day). One event, involving small tears in a PWR refueling cavity seal, was also reported. The events appear evenly spread out over the review period. Thus, operating experience suggests that occurrence of SFP liner leakage is relatively low. However, Salem reported (Ref. 10) a PWR design problem in which the SFP liner could buckle and leak at temperatures above 180 °F. This site is one of the sites which apparently does not have liner drainage isolation capability. Subsequent licensee analysis determined that the liner would not fail. The NRC is currently evaluating the licensee's analysis.

Load Drops

Only one event was found during the operating experience review in which the fuel pool liner was punctured by dropping a load into the SFP. This event at Hatch Unit 1 on December 28, 1994, involved a core shroud bolt which was dropped. An approximate 0.7 gallons per minute leak resulted which was contained between the fuel pool liner and the concrete structure. The fuel pool level was restored and maintained with normal make-up (Ref. 11).

There were no other examples of loads actually being dropped and damaging the SFP. However, there were many situations (more than 30) involving loads heavier than allowable being moved or potentially moved over the SFP. Less than about 20 percent of these events involved actual downward motion or drops of objects (usually fuel assemblies) into the SFP. Although not judged safety significant by themselves, these events represent continuing precursors to potential SFP puncture events. They indicate that movement of loads heavier than allowed over the SFP is continuing even though the NRC has taken steps to reduce the problem.

Pool Seismic Design

Only two conditions were found related to seismic design problems with SFPs. One condition was related to block walls in the fuel handling building which could collapse during a seismic event. The walls were replaced. The other condition involved only the fuel racks.

3.1.4 Spent Fuel Pool Make-up Capability

Only two events found during the operating experience review involved potential loss of SFP inventory make-up capability. No actual losses of make-up capability were found. One event involved a small accumulation of marine life in the service water pipe used for make-up to the SFP. Had the accumulation of clams gone undetected, it may have blocked the pipe. Another Seismic

Class I source was available. One event involved a 2 minute loss of an electrical bus needed to supply make-up water to the SFP. Operating experience indicates that losses of all make-up capability are not very likely.

3.1.5 Impact on Safety Equipment

There were several reported events involving flooding due to SFP overflow. These events had the potential to affect equipment in other portions of the plant. In some of the events, actual flooding took place when the SFP overflowed into the ventilation system or the reactor building. None of these flooding events was serious. They were all caused by human error. There were two reports of conditions in which problems within the SFP could potentially lead to failure of important safety equipment. One report of a potential effect on safety equipment due to boiling of the SFP was submitted by Susquehanna on November 17, 1992 (Ref. 12). It describes a condition in which a loss of SFP cooling is postulated to occur subsequent to a design basis accident such as a loss-of-coolant accident (LOCA) or a loss-of-offsite power (LOOP). The design basis accident is postulated to prevent makeup to the SFP. Subsequent boiling of the SFP is postulated to create an environment which could be transported to safety-related equipment in the reactor building. The LER stated that the postulated events were beyond the plant's design basis. These conditions were postulated in the "Susquehanna" 10 CFR 21 report and were addressed in a June 1995 letter from the NRC to Pennsylvania Power and Light Company (Ref. 13).

The second report was an LER from WNP 2, issued May 28, 1993 (Ref. 14), which describes a circumstance where, under operating conditions at the time of discovery (local manual service water valve closed), a postulated LOCA would render emergency SFP make-up capability inoperable. Subsequent evaporation of SFP inventory and tripping of SFP cooling pumps were postulated to result in SFP boiling. The evaporated and boiled water is postulated to condense and flood the ECCS pump rooms, causing failure of ECCS equipment needed to mitigate the ongoing LOCA. The LOCA is postulated to make the local manual SFP make-up valve inaccessible. In this postulated scenario, the normal nonsafety make-up source is also assumed to be unavailable.

Subsequent licensee investigation indicated that the local manual valves in the service water lines for make-up to the SFP could be opened when required after LOCA.

Table 3.3 Loss of Cooling Events

Type of Event	Actual	Precursor
Cooling Flow	50	20
SFP Pumps	39	8
Configuration Control	1	0
Loss of Pump Suction	4	0
Flow Blockage	1	0
Single SFP Pump Failure	5	12
Heat Sink	6	2

3.2 Spent Fuel Pool Cooling

Fifty-six events found during the operating experience review involved actual losses of SFP cooling. There were 22 precursor events which when coupled with additional failures or postulated events could result in losses of SFP cooling. Table 3.3 provides a summary of the numbers and types of loss of SFP cooling events. Figures 3.3 and 3.4 provide an overview of the loss of SFP cooling events for which temperature increase and duration could be quantified. These figures indicate that the losses of SFP cooling are infrequent. However,

some events have lasted for significant time periods and four events have resulted in temperature increases of more that 20 °F. The low number of events found with small temperature increases may be due to a lack of reporting of such events.

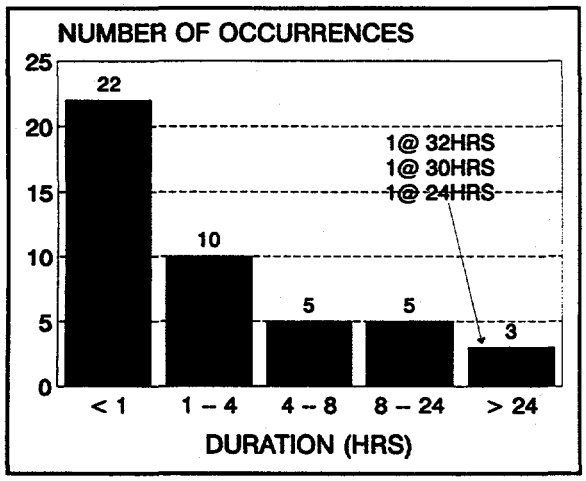


Figure 3.3 Loss of Cooling Duration

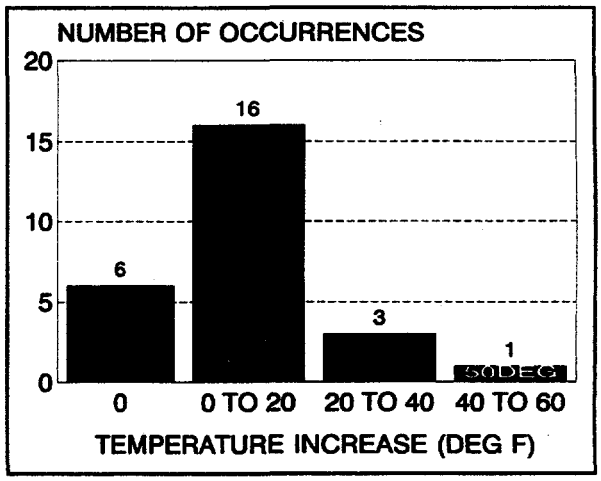


Figure 3.4 Loss of Cooling Temperatures

Using the number of events found during this study over a period of about 12 years for which temperature and duration could be quantified, the frequency of loss of SFP cooling events in which a temperature increase of more than 20 °F occurred can be estimated to be on the order of about 2 to 3 per 1000 reactor years.

3.2.1 Loss of Spent Fuel Pool Cooling

The dominant cause of the actual loss of SFP cooling events was loss of electrical power to the SFP cooling pumps. Thirty-nine of the loss of cooling events were due to loss of power to the SFP cooling pumps. For these losses of electrical power, the time for which cooling was not available ranged from a few minutes with no accompanying temperature increase to 8 hours with an associated temperature rise of 20 °F. Most plants have alternate sources of SFP cooling pump power available. No attempt was made during the event review to determine if alternate power was available in each event. The primary causes appear to be human error and administrative problems (22 of the 39 events). The events appear evenly distributed between BWRs and PWRs.

There were five events involving failure of one SFP cooling pump while the second pump remained operable. During these events, the second SFP cooling pump was adequate to cool the SFP. Because these events did not result in an actual loss of SFP cooling, they are not counted in the overall total for this category. While events with the potential for common cause-common mode failure have been reported, none have occurred.

There were four events found in the study in which SFP cooling was lost due to loss of SFP coolant inventory and consequent tripping of the SFP cooling pumps on loss of suction. There was one flow blockage event in which a rubber boot blocked a SFP cooling pump strainer. The time required to remove the blockage was about 6 hours. Engineered safety features actuations have resulted in losses

of SFP cooling. However, these resulted in almost no temperature increase and generally lasted for only short periods. They did not appear to have presented a threat to long-term cooling.

No actual events involving insufficient cooling have occurred. However, several conditions were reported in which full core off-loads were performed with insufficient evaluation of the heat loads or SFP cooling system during the off-load. Errors in the calculated heat load and nonconservative ultimate heat sink temperature assumptions have also occurred. This issue surfaced due to a situation at Millstone Unit 1 (Ref. 15). For Millstone Unit 1, licensee analysis determined that during prior refueling outages the SFP cooling system would not have been capable, by itself, of maintaining pool temperature below the 150 °F design limit under certain postulated conditions including a single active equipment failure.

3.2.2 Ineffective Heat Sink

The second leading cause of loss of SFP cooling, although there were significantly fewer events, was loss of SFP heat exchanger cooling. Of the 6 events, almost all were caused by human error. These events lasted from some very short periods of time to about 13 hours with temperature increases ranging from zero to 40 °F.

3.3 Spent Fuel Pool Instrumentation Experience

There have been several events involving losses of SFP coolant inventory or SFP cooling, where associated instrumentation was inoperable or failed prior to or during the events. In one event, a shared annunciator window was illuminated due to an instrumentation problem when the loss of inventory occurred. Since the window was already illuminated, the operations staff was not alerted to the loss of coolant inventory event when it began. While there have been relatively few of these instrumentation problems, they raise concerns about how SFP instrumentation is treated and regarded.

3.4 Effect of Shortening Refueling Outage Times

Review of operating experience has shown that in an effort to minimize refueling outage times, many plants perform full core offloads early in their outages. The effect of such practices is to reduce the time available to recover from a loss of SFP cooling event. AEOD discussions with the engineering manager of Nine Nile Point Unit 2 provided good insight to the effect this practice has upon reducing the time available until boiling begins.

Figure 3.5 shows the history of full core offloading times at Nine Mile Point Unit 2. Figure 3.6 shows the ranges of calculated times available to initiate boiling at Nine Mile Point Unit 2. For operation with the SFP gates out, the licensee's conservative calculations estimated the time to initiate boiling reduced from 51 hours during the first refueling outage to 24.2 hours during the fourth refueling outage. For operation with the SFP gates installed, the licensee's conservative calculations estimated the time to initiate boiling reduced from 17.6 hours to 8.4 hours. Similarly, during a visit to the South Texas plant, AEOD learned that calculations performed for the most recent refueling outage estimated that the initiation of boiling could begin approximately 5 hours after SFP cooling is lost. A recent survey assessment performed by NRC's Office of Nuclear Reactor Regulation (NRR) indicated that, if a full core had to be offloaded during midcycle, boiling could begin about 2 to 3 hours after losing SFP cooling.

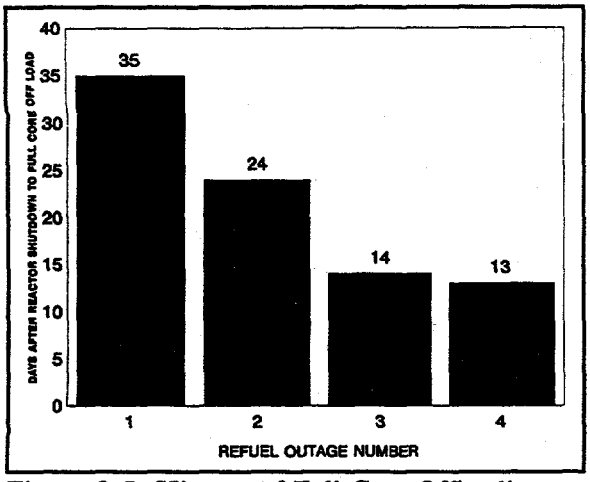


Figure 3.5 History of Full Core Offloading

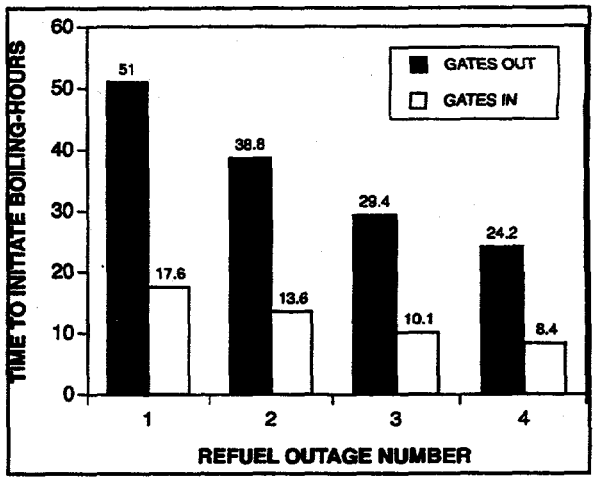


Figure 3.6 Reduced Time to Boil

3.5 Operating Experience Review Findings

Losses of SFP or refueling water inventory are dominated by events involving system or SFP configuration control problems due to human error. The second most prevalent cause of loss of SFP inventory is leaking inflatable gate seals generally due to loss of air to the seals because of human error. Losses of inventory from SFP gates due to leaking inflatable gate seals have generally been of greater magnitude than those due to configuration control problems. Loss of inventory due to configuration control problems is more easily controlled by the operations staff than leaks from gates. However, configuration control problems seem to have taken longer to diagnose.

Pool leakage events do not appear to have caused problems with long-term losses of spent fuel cooling. Inadvertent movement of heavier than allowed loads over SFPs is continuing even though the NRC has taken steps to reduce this problem.

The most prevalent type of loss of cooling events involved loss of electrical power to the SFP cooling pumps, generally due to human error. The few losses of SFP cooling due to loss of SFP heat exchanger cooling were also generally due to human error. Both types of events resulted in losses of about the same time frame and associated temperature rises. The events were evenly distributed between BWRs and PWRs.

While conditions have been reported suggesting the possibility of SFP boiling affecting other plant equipment important to safety, operating experience does not provide insights into what is apparently a very complex issue.

Operating experience provides only limited insight into instrumentation problems. Several loss of level events have taken place while level instrumentation was inoperable or level annunciators were already actuated for other reasons. There have been relatively few of these instrumentation problems captured by this study. They represent concerns about how SFP instrumentation is treated and regarded.

Some ventilation events (damper problems, heater problems) could be potential areas of concern when coupled with postulated SFP events which could lead to radiation release.

Foreign operating experience appears to be consistent with that from U.S. plants. Operating experience suggests that losses of make-up capability are not very likely.

4 OBSERVATIONS FROM THE SITE VISITS AND INTERVIEWS

Six site visits were conducted to gain understanding of the licensees' SFP physical configurations, practices, and operating procedures. Site selection was a cross sampling of the industry that included BWRs and PWRs, large and small architect-engineer designs, shared and single pools, old and new designs and all four nuclear steam supply system vendor designs. The sites visited were: North Anna, South Texas Project, Susquehanna, Three Mile Island, River Bend, and Calvert Cliffs. In addition to the site visits, one trip was made to Pennsylvania Power and Light headquarters. The following observations are from the site visits and the interviews. These observations are a cross-sampling and representative of the nuclear power industry.

In general, utilities are doing a good job of analyzing the SFP heat loads and heat up rates. However, control room operators are not always being made aware of the analysis and results. This information could prove to be critical in worst case refueling outage conditions (e.g., full core off-load and a very short outage schedule). Some of the utilities are performing risk analysis as part of the outage planning.

Some utilities have used lessons from operating experience and have done a very good job in correcting problems through better analysis, good operator aids, training, and procedure revisions. Some utilities have a good system to evaluate industry experience.

The site visits identified events where connected systems could have caused loss of SFP coolant inventory. Many events such as draindowns are not being reported through the standard mechanisms that would allow for the standard analysis of the events. Therefore, the actual frequency of draindowns is higher than is typically assigned in the risk analysis. The site visits also identified that little attention is paid to the antisiphon devices. Very few sites performed testing or had analysis on the efficacy of the antisiphon devices.

There is a large variation in utility practice regarding full core off-loads versus fuel shuffles. One plant visited that had been performing full core off-loads now plans to do fuel shuffles instead. Another plant that had intended to do fuel shuffles now routinely does full core off-loads.

The newer designs have more of the better features such as safety-related power, analog control room meters, more parameter indicators in the control room, more sources of water, and generally better qualified equipment. However, some older plants have made improvements by adding indicators or annunciators in the control room, and supplying safety-related power to the SFP equipment. All of the sites visited are including the SFP system in the equipment covered by the Maintenance Rule.

All the plants visited had examples of good practices. Some of the good practices observed in our visits, but not all in one plant, include:

- Using licensed reactor operators and training them for the refueling outages.
- Including SFP risk in the outage planning.
- Having SFP system power restored in the top level emergency operating procedures.
- Forming a refueling team with formal structure.
- Providing classroom and simulator training in preparation for the outage.
- Producing user friendly graphs of pool heat up rates from the analysis, for use in the control room.
- Doing analysis beyond heat loads and heat rates, such as SFP risks in outage planning.
- Having strong command and control of SFP activities.
- Providing a second source of power for the SFP system.
- Having a mimic on the control board for the SFP system lineup.
- Utilizing a system diagram prior to making SFP system alignment changes.
- Having an effective program to learn from internal and industry operating experience.
- Refining the SFP risk model used in the outage planning down to the component level.

Three good design modification examples were found:

- Adding additional SFP indication to the control room.
- Adding safety-related power to the SFP instrumentation.
- Providing a dedicated heating, ventilation, and air conditioning system for refueling.

The interviews with the authors of the Susquehanna 10 CFR part 21 report were very informative. They provided the details of their concern that the as-found Susquehanna SFP configuration did not meet the licensing basis. The report that they filed does have potential generic implications, including:

- mechanisms to transport vapor to and create high temperatures in other parts of the plant
- electrical and instrumentation weaknesses in SFPs
- potential for multiunit sites with shared pools to have an increased SFP risk
- a lack of awareness for SFP issues

The 10 CFR 21 report provided an impetus for the NRC and the nuclear industry to take a closer look at SFPs, which historically have not received much attention. In the efforts to address the

10 CFR 21 report concerns, Pennsylvania Power and Light has improved the Susquehanna SFP design, modified its operation, improved emergency procedures, and improved operator training. A limited probabilistic risk assessment (PRA) found that the net effect of these actions at Susquehanna was to diminish the risk from SFP events.

5 RISK ASSESSMENT

Over the years, the SFP has not received the risk assessment attention that the reactor had because early analysis put the risk of a SFP accident an order of magnitude below a reactor event. Therefore, the analyses done for the SFP were limited. However, in recent years several issues have required that certain aspects of the SFP be studied further. INEL was contracted to review the previous SFP risk assessments and to utilize the useful insights to assess the current risk of SFP accidents. In addition to those risk insights, INEL utilized the AEOD operating experience review, engineering analyses, site visits, and site interviews in assessing the likelihood of SFP events.

5.1 "Risk Analysis for Spent Fuel Pool Cooling at Susquehanna Electric Power Station"

In October 1994, Battelle Pacific Northwest Laboratory (PNL) prepared a draft report, "Risk Analysis for Spent Fuel Pool Cooling at Susquehanna Electric Power Station," (Ref. 16) for NRC's Risk Applications Branch of NRR. The report presented the results of PNL's analysis of loss of SFP cooling events at the Susquehanna nuclear power plant, including estimates of the likelihood for loss of SFP cooling, the near-boiling frequency (NBF), and order of magnitude estimates of core damage frequency (CDF) attributed to SFP heat-up events.

The PNL analyses addressed design basis accidents which would cause mechanistic failure of the nonsafety-related SFP cooling system. The accident scenario postulated in the Susquehanna 10 CFR 21 report, an RCS LOCA, would result in de-energizing SFP power and could also induce hydrodynamic loading of systems and equipment associated with SFP cooling. In addition to addressing RCS LOCA, NRR had PNL analyze other initiating events; earthquakes, LOOP, and flooding. The PNL analysis did not consider major SFP coolant inventory losses from configuration control, gates, and seals to be credible events.

The results of the analyses indicated that the risk from SFP events was low compared to reactor events which did not account for any risk contribution from the SFP. The PNL study showed that for the Susquehanna plant, the largest contributors to SFP risk emanated from extended LOOP and LOCA events. The analyses also showed that the improvements that were made at the Susquehanna station in response to the issues raised by the 10 CFR 21 report resulted in a NBF reduction of about a factor of four with a commensurate reduction of risk of about a factor of four.

The results of the PNL study were integrated into NRR's Safety Evaluation, "Susquehanna Steam Electric Station, Units 1 and 2, Safety Evaluation Regarding Spent Fuel Pool Cooling Issues." The PNL analysis was used to augment the deterministic analysis of the Susquehanna plant. From their deterministic analysis NRR found that "systems used to cool the spent fuel storage pool are adequate to prevent unacceptable challenges to safety-related systems needed to protect the health and safety of the public during design basis accidents." Based upon the PNL analysis NRR indicated that "loss of

SFP cooling events represented a low safety significance challenge to the plant [Susquehanna] at the time the issue [Part 21 report] was brought to the staff's attention."

Although there may be large uncertainties associated with the absolute values and specific numerical results of the PNL analyses, much insight can be gained from the PNL analyses of the Susquehanna station. For example, the PNL analysis shows that the most significant risk reduction could be achieved from three strategies:

(1) installing SFP level and temperature instrumentation in the control room
(2) enhancing SFP normal and off-normal procedures and training staff to be proficient
(3) cross-tieing SFPs

5.2 Risk Assessment

AEOD obtained technical assistance in the area of risk assessment from INEL. INEL reviewed the PNL Susquehanna PRA, assessed the adequacy of the risk analysis, and addressed the adequacy and reasonableness of the assumptions made. INEL extracted insights from the PNL Susquehanna PRA and the other relevant PRAs in industry to assist in generically assessing the likelihood of loss of SFP cooling. Information from the AEOD reviews of operating experience, interviews, site visits, and independent SFP analyses was used to refine the developed PRA model. This study provided quantitative estimates of the NBF and qualitative discussions about the risk of losses of SFP cooling. The following sections provide the results and the insights obtained from these INEL efforts (Ref. 17).

5.2.1 Risk Assessment — Quantitative Results

INEL corrected modeling problems identified in the PNL study. The event and fault trees were refined to more accurately describe current Susquehanna plant operations. To refine the event trees, INEL staff visited PP&L engineering offices and the Susquehanna station. The event and fault trees were quantified using recent operating experience data supplied by AEOD. In performing the analyses, INEL also refined and updated the data and models that PNL had used to account for human performance.

In some cases the modifications and improvements resulted in increases in the NBF in the SFP, which in turn would result in increased estimates of risk. Correcting the initiating event frequencies for station blackout, LOCA, seismic events, configuration control errors, and seal failures would tend to increase the NBF. Counterbalancing this, the study identified possible sources of conservatism in the PNL study. Chief among them were the estimates of human performance associated with recovery and mitigation.

INEL performed the aforementioned refinements, including modifications of the initiating event frequencies using AEOD's operational event database, to cover a full spectrum of loss of SFP inventory events, including catastrophic seal failure. The results of their analysis are shown in Table 5.1. The analysis found the NBF for the Susquehanna plant after implementing the 10 CFR 21 improvements was 5E-5/year, which is approximately twice that found by PNL.

The dominant event initiators were LOOP and SFP inventory losses including configuration control errors and seal failures. Due to the limited time and resources available, INEL did not extend the analysis to include a quantitative estimate of the CDF. Also, given the limited data available for development of estimates of event frequencies and the limited resources available for model development, more refinement is required before these estimates can be used as a basis for regulatory actions.

Table 5.1 Near-Boiling Frequencies

	INEL	PNL
Total NBF	5 E-5	2 E-5
LOOP	3 E-5	1 E-5
Inventory Losses	2 E-5	1 E-6

5.2.2 Risk Assessment — Qualitative Results

The SFP PRAs which were done by PNL and INEL were specifically for the Susquehanna plant. Many features of the design and operation of Susquehanna are unique, consequently the results of the PNL and INEL analyses cannot be applied directly to other plants. Nonetheless, there are certain qualitative insights that have been learned from those studies which may have generic applications. For example:

(1) Effect of defueled unit upon operating unit

The analyses showed that for a dual unit BWR, it is possible for a problem with SFP cooling at a shutdown unit to affect the adjacent operating unit. The accident scenario postulated in the Susquehanna 10 CFR 21 report was found to be a credible event, but less likely than other events.

(2) Uncertainties of core damage frequency estimates

The task of estimating the NBF appears to be amenable to the use of PRA techniques. However the task of estimating CDF is subject to very large uncertainties. PNL and INEL both acknowledged that the methodology used for this task provided only "order of magnitude estimates."

(3) Effect of the Susquehanna 10 CFR 21 Report

Comparison of the analyses that were done for the Susquehanna plant as it existed at the time of the 10 CFR 21 report and after corrective actions were taken revealed that the improvements that were made in the areas of instrumentation, accident response procedures, operator training, and shutdown operations reduced the estimated NBF.

Improvements in instrumentation consisted of providing reliable SFP level and temperature monitoring instruments in the control room.

Improvements in operations and accident response procedures involved:

- ventilation system isolation
- installation of drains in the standby gas treatment system
- utilization of the RHR system of the operating unit to cool the SFP
- verification that removal of cask storage pit gates results in effective heat transfer between the SFPs

(4) Dominant accident sequences

For the Susquehanna plant, the PNL analysis found that the accident sequences which were the largest contributors to NBF were extended LOOP, and LOCA. The extended LOOP is a dominant contributor because at the Susquehanna station the SFP cooling system pumps are not on the emergency busses. The original accident scenario raised in the 10 CFR 21 report did not appear to be a significant contributor to NBF. The INEL study found the dominant contributors to NBF were LOOP and SFP inventory loss.

(5) Deviation from the modeled plant design

Risk estimates from the SFP for the Susquehanna plant may be affected by changes planned for future refueling outages, which may represent major deviations from the models used by PNL and INEL. Some of those anticipated changes are:

- operation without the SFP cross-tied for the future dry cask storage operations
- reduction of refueling outage from 55 days to 35 days
- partial core off-loads taking place earlier in the outage

(6) Operating experience

INEL found that SFP inventory losses such as draindowns or pneumatic seal failures may be important contributors to NBF at the Susquehanna plant. In previous PRAs such events were either not modeled or their occurrence frequency was assumed to be very low; once every 10,000 reactor years.

6 FINDINGS AND CONCLUSIONS

The findings and conclusions presented below are based on review of operating events and interpretations of the available risk analyses. The conclusions are stated, followed by indented paragraphs which are the findings on which those conclusions are based. These findings and conclusions are grouped under the headings of: (1) likelihood and consequences of SFP events, (2) prevention of SFP events, and (3) response to SFP events.

6.1 Likelihood and Consequences of Spent Fuel Pool Events

6.1.1 Review of more than 12 years of operating experience determined that loss of SFP coolant inventory greater than 1 foot has occurred at a rate of about 1 per 100 reactor years. Loss of SFP cooling with a temperature increase greater than 20 °F has occurred at a rate of approximately 3 per 1000 reactor years. The consequences of these actual events have not been severe. However, events

have resulted in loss of several feet of SFP coolant level and have gone on in excess of 24 hours. The primary cause of these events has been human error.

- There have been two loss of SFP coolant inventory events with SFP level decreases in excess of 5 feet. These events were terminated by operator action with approximately 20 feet of coolant remaining above the stored fuel. Without operator actions, the inventory loss could have continued until the SFP level had dropped to near the top of the stored fuel resulting in radiation fields which could have prevented access to the SFP area. The events with the largest level decrease involved unavailable or inaccurate instrument readings. Ten other loss of inventory events resulted in level decreases between 1 and 5 feet. Operator response to one of the largest losses of SFP coolant inventory events (loss of 5.5 feet level in SFP) was deficient because several opportunities to diagnose and correct the problem were missed when make-up coolant was added to the system without evaluating the cause of the need for make-up. There were two precursor events involving cavity seals which involved rapidly developing leaks. In one case, about 200,000 gallons of water was lost in about 20 minutes. In the second case, about 25,800 gallons were lost in about 30 minutes.

- Several losses of SFP cooling have lasted in excess of 24 hours; one had a maximum temperature increase of 50 °F to a final temperature of 140 °F. There were no reported approaches to boiling found during the experience review period.

- While the operating experience review results are believed to be reasonably representative, discussions with operations staff revealed a number of additional events that did not reach the reporting threshold required by NRC regulations, and therefore were not initially captured by the study's event review process.

6.1.2 Review of existing SFP risk assessments found that after correction for several problems in the analyses, the relative risk due to loss of spent fuel cooling is low in comparison with the risk of events not involving SFP. The review determined that the likelihood and consequences of loss of SFP cooling events are highly dependent on human performance and individual plant design features.

- The risk assessment identified loss of offsite power and loss of SFP coolant inventory as major contributors to near boiling frequency. LOOP was a major contributor largely because the analysis was based on the Susquehanna plant where the SFP cooling system is not connected to emergency power.

- Human performance is the most important factor for both loss of spent fuel cooling event initiators and recovery actions. Problems with configuration control caused most of the SFP events. Lack of automatic functions for detection and recovery from SFP events places full reliance on operator actions. The results of risk assessments involving operator actions are sensitive to the level of administrative controls, instrumentation, procedures, and training provided to aid operator performance.

- The impact of instrumentation, procedures, and training is dependent upon plant specific design features. The NRR survey of SFPs identified a wide range of plant design features and specific limitations at existing plants. Plants which have identified limitations relating to

configuration control, instrumentation, procedures, and training could reduce the risk of SFP events by relatively modest improvements in these areas. Modest improvements to instrumentation and operations made by Susquehanna resulted in reduced risk.

6.1.3 The need for specific corrective actions should be evaluated for those plants where failures of reactor cavity seal or gate seals, or ineffective antisiphon devices could potentially cause loss of SFP coolant inventory sufficient to uncover the fuel or endanger makeup capability.

- Review of the SFP risk assessment identified Loss of SFP coolant inventory as a major contributor to near boiling frequency and review of operating experience and the site visits identified that problems with configuration control, seals, and antisiphon devices were contributors to large losses of inventory.

- The risk assessment identified that the near boiling frequency is sensitive to individual plant specific design features and human performance. Plant specific design features which impact the near boiling frequency include pneumatic reactor cavity seals and gate seals and SFP geometry which might result in draindown to near or below the top of the stored fuel.

6.2 Prevention of Spent Fuel Pool Events

6.2.1 The need for improvements to configuration controls related to the SFP to prevent and/or mitigate SFP loss of inventory events and loss of cooling events should be evaluated on a plant specific basis.

- Operating experience shows that the most frequent cause of loss of inventory and loss of cooling is ineffective configuration control. Mistaken valve alignments have diverted water from the SFP and have isolated the air supply to pneumatic seals. Mistaken electrical alignments have resulted in loss of power to SFP system pumps and other equipment.

6.2.2 The need for plant modifications at some multiunit sites to account for the potential effects of SFP boiling conditions on safe shutdown equipment for the operating unit, particularly during full core off-loads, should be evaluated on a plant specific basis.

- The Susquehanna 10 CFR 21 report brought to light the potential problem that, when two units have a common pool, the refueling of one unit when SFP cooling is lost could impact the operating unit. A specific need is the assessment of the potential mechanisms to transport vapor to create high temperature in other parts of the plant that have critical plant equipment. The NRR survey assessment identified seven sites besides Susquehanna that have shared pools. Since the scenario involves many things going wrong and each configuration is different, more assessment and evaluations need to be performed on these seven units.

6.3 Response to Spent Fuel Pool Events

6.3.1 The need for improved procedures and training for control room operators to respond to SFP loss of inventory and SFP loss of cooling events consistent with the time frames over which events can proceed, recognizing the heat load and the possibility of loss of inventory, should be evaluated on a plant specific basis.

- Refueling outages are getting shorter. Control room operators at some plants are not aware that early transfer of the entire core from the reactor to the SFP during a refueling outage results in significant heat loads in the SFP and potential for near boiling conditions within 5 to 10 hours if cooling to the SFP is lost. Current operator training and procedures do not typically include this information, or if the information is provided it is not easy to interpret.

- All licensees have to some degree, work scheduling, training, and procedures that deal with the SFP activities during a refueling outage and during normal plant operations. However, the effectiveness of these efforts was not apparent at all the plants visited. Of the licensees that had: (1) a formal training structure consisting of classroom lectures for the workers involved in the refueling activities, (2) a schedule program that incorporated the SFP risks, and (3) detailed procedures for all the activities, there was knowledge and awareness on the part of the engineers and operators of relevant SFP issues. Regarding backup sources for SFP coolant inventory and SFP cooling, discussions with the licensees during the site visits revealed many ways that water could be provided to the pool which had not been formerly described and for which procedures did not exist.

6.3.2 The need for improvements to instrumentation and power supplies to the SFP equipment to aid correct operator response to SFP events should be evaluated on a plant specific basis.

- Instrumentation available to the operators regarding the SFP parameters can be very limited. A single annunciator may be the only indication of SFP trouble. Some plants have SFP level or temperature indication readouts on control room back panels. All indications of the SFP parameters could easily be lost in a reactor accident since not all of these instruments have safety-related power. Plant operators make rounds to the SFP location but the time between successive visits may be too long to adequately trend data and stop a developing problem before it becomes a serious event. The operating experience review found several events where SFP cooling was lost due to loss of power to the SFP pumps. Most power supplies to the SFP pumps are safety related, but for the units that do not have this capability, an assessment to provide power during accident conditions would assist them in reacting faster to a SFP event.

7 REFERENCES

1. *U.S. Code of Federal Regulations*, Title 10, "Energy," U.S. Government Printing Office, Washington, D.C., revised periodically.

2. Lochbaum, D.A., and Prevatte, D.C., Letter to Martin, T., U.S. Nuclear Regulatory Commission, "Susquehanna Steam Electric Station, Docket No. 50-387, License No. NPF-14, 10 CFR Part 21 Report of Substantial Safety Hazard," November 27, 1992.

3. Taylor, J.M., U.S. Nuclear Regulatory Commission, Memorandum to the Commission, "Resolution of Spent Fuel Pool Action Plan Issues," July 26, 1996.

4. U.S. Nuclear Regulatory Commission, Inspection Report 50-298/95-014, December 18, 1995.

5. Northeast Nuclear Energy Company, Millstone Unit 2, Licensee Event Report 50-336/92-012, "Partial Loss of Normal Power (LNP)," January 17, 1993.

6. U.S. Nuclear Regulatory Commission, Information Notice 88-065, "Inadvertent Drainages of Spent Fuel Pools," August 18, 1989.

7. Southern California Edison Co., San Onofre Unit 2, Licensee Event Report 50-361/88-017-01, "Spent Fuel Pool Drainage Due to the Failure to Implement Updated Safety Analysis (FSAR) Commitments," January 2, 1990.

8. Toledo Edison Co., Davis Besse, Licensee Event Report 50-346/82-007, March 3, 1982.

9. U.S. Nuclear Regulatory Commission, Augmented Inspection Team Report 50-321/86-41 and 50-366/86-41, January 8, 1987.

10. Salem Unit 1 and Unit 2, Event Notification 30528, May 22, 1996.

11. U.S. Nuclear Regulatory Commission, Morning Report II-94-0112, December 29, 1994.

12. Pennsylvania Power & Light Co., Susquehanna Unit 1, Licensee Event Report 50-387/92-016, "Voluntary Report-Spent Fuel Pools," November 17, 1992.

13. Stolz, J.F., U.S. Nuclear Regulatory Commission, Letter to Byram, R.G., Pennsylvania Power and Light Company, "Susquehanna Steam Electric Station, Units 1 and 2, Safety Evaluation Regarding Loss of Spent Fuel Pool Cooling Issues (TAC No M85337)," June 19, 1995.

14. Washington Public Power Supply System, Washington Nuclear Plant Unit 2, Licensee Event Report 50-397/93-018, "Spent Fuel Pool Makeup Not Adequate to Mitigate Accident Conditions," May 28, 1993.

15. Northeast Nuclear Energy Company, Millstone Unit 1, Licensee Event Report 50-245/93-011-02, "Spent Fuel Pool Cooling Capacity," July 25, 1996.

16. Battelle Pacific Northwest Laboratory, Draft Report under NRC Contract DE-AC96-76RLO 1830, "Risk Analysis for Spent Fuel Pool Cooling at Susquehanna Electric Power Station," October 1994.

17. Idaho National Engineering Laboratory, "Loss of Spent Fuel Pool Cooling PRA: Model and Results," INEL-96/0334, September 1996.

LOW-POWER AND SHUTDOWN MODELS FOR THE ACCIDENT SEQUENCE PRECURSOR (ASP) PROGRAM

Martin B. Sattison, Tami A. Thatcher, and
James K. Knudsen
Lockheed Martin Idaho Technologies Company
Idaho National Engineering Laboratory
P.O. Box 1625
Idaho Falls, Idaho 83415-3850
(208) 526-9626

J. S. Hyslop
U.S. Nuclear Regulatory Commission
Washington, DC 20555
(301) 415-6197

ABSTRACT

The U.S. Nuclear Regulatory Commission (NRC) has been using full-power, Level 1, limited-scope risk models for the Accident Sequence Precursor (ASP) Program for over fifteen years. These models have evolved and matured over the years, as have probabilistic risk assessment (PRA) and computer technologies. Significant upgrading activities have been undertaken over the past three years, with involvement from the Offices of Nuclear Reactor Regulation (NRR), Analysis and Evaluation of Operational Data (AEOD), and Nuclear Regulatory Research (RES), and several national laboratories. Part of these activities was an RES-sponsored feasibility study investigating the ability to extend the ASP models to include contributors to core damage from events initiated with the reactor at low power or shutdown (LP/SD), both internal events and external events. This paper presents only the LP/SD internal event modeling efforts.

I. INTRODUCTION

Two prototype LP/SD models were created for pressurized water reactors (PWRs) as part of the investigation into the feasibility of creating simplified risk models suitable for Accident Sequence Precursor evaluations of low power and shutdown events. The plants modeled were Surry Unit 1 and Sequoyah Unit 1. Model development relied heavily on the information provided in the Surry LP/SD study (NUREG/CR-6144).[1] The models focus on the aspects of low power and shutdown expected to be the most important for evaluating the risk of fuel damage although the coverage of shutdown accidents is not complete.

A reduced set of plant operating states (POSs) suitable for simplified ASP modeling of PWRs was identified by grouping the fifteen detailed POSs delineated in NUREG/CR-6144. Six POS "Groups" were defined:

POS Group 1: Low power/cooldown with steam generators.

POS Group 2: Pressurized Residual Heat Removal (RHR) cooldown.

POS Group 3: Depressurized RHR cooling with normal inventory.

POS Group 4: Depressurized RHR cooling with reduced inventory.

POS Group 5: Depressurized RHR cooling with the refueling cavity filled.

POS Group 6: Reactor Coolant System (RCS) heatup.

The models currently focus on POS Groups 2, 3, and 4 since it is expected that sufficient coverage of the many risk-significant aspects of shutdown can be accommodated by modeling these three POS Groups with the appropriate time windows. Limiting the model to three POS Groups was made in the interest of reducing model size and complexity and is in keeping with the general philosophy of the ASP models. Four time windows were defined in NUREG/CR-6144 to establish decay heat rates. These have been retained in the ASP LP/SD models. They are:

	Time After Shutdown	Percent Full Power
Time Window 1	< 75 hours	0.54%
Time Window 2	75-240 hours	0.41%
Time Window 3	240-768 hours	0.29%
Time Window 4	> 768 hours	0.20%

II. INITIATING EVENTS

Three initiating event categories were defined that were deemed most relevant for ASP event evaluation and event tree models were developed for each initiating event. The initiating event types are:

- Loss of decay heat removal (excluding those initiated by loss of inventory)
- Loss of inventory events
- Loss of offsite power.

The initiating events that were used in this study were based on those initiating event evaluations documented in the Surry LP/SD study, NUREG/CR-6144. In NUREG/CR-6144, licensee event reports (LERs) were reviewed and the events were arranged into various initiating event categories based on the type of events and how they affected plant response. For the ASP shutdown models, the detailed categories of initiating events were combined into groups that share the same plant response. Many initiating events relevant to low power and shutdown were screened from the ASP shutdown models based on the frequency of occurrence and applicability to the selected POS Groups. Some initiating events were omitted by decision in discussions with the NRC in order to reduce the project scope. Also, the support system events were screened consistent with the level of detail included in the ASP program.

The loss of inventory initiating event was based on those events that cause a reduction in RCS inventory, which would lead to a loss of RHR. Overdraining while going to reduced inventory and failure to maintain level during reduced inventory are two loss of inventory initiators important to midloop or the more encompassing "reduced inventory" POS Group 4. Additionally, loss of coolant accidents (LOCAs) due to flow diversion, LOCAs in connected systems, and maintenance-induced LOCAs were included in determining the loss of inventory frequency for all POS Groups.

To represent the loss of inventory with sufficient detail, demand-related and time-related categories were distinguished. The demand-related category applies only to POS Group 4. For the demand-related overdraining initiator, the particular initiating event value depends on the number of times an intentional drain-down to midloop or reduced inventory occurs during the period being assessed. Including demand-related initiating events increased the model complexity in that the current GEM[2] module of SAPHIRE[3] does not accommodate demand-related initiating events for condition assessment.

The initiating event categories modeled were limited to dominant initiating events that were within the scope of the project. Areas not addressed by the model include reactivity control, cold overpressurization of the RCS, spent fuel pool and fuel handling events.

III. EVENT TREE DESCRIPTION

Event trees for shutdown were developed for the three initiating event categories: loss of decay heat removal or residual heat removal (RHR), loss of inventory, and loss of off-site power. Each event tree also addressed the needs of the three prominent POS Groups:

POS Group 2:	Pressurized RHR cooldown
POS Group 3:	Depressurized RHR cooldown with normal inventory
POS Group 4:	Depressurized RHR cooling with reduced inventory

The event tree structure was designed to be generic with the plant-specific details being modeled at the fault tree level. The structure was intended to limit the number of event trees required while allowing considerable modeling detail. The event trees use fault trees that can accommodate success criteria for four time windows. The fault tree for a top event on an event tree include any systems that can perform the function required.

For each initiating event, there is a single event tree (called a root tree, Figure 1) that transfers to three event trees, one for each POS Group (Figures 2 through 4). The structure of the root tree that branches to the appropriate transfer event tree allows specific information concerning the POS Group and time window to automatically be associated with the branch being analyzed. The root trees for each initiating event are nearly identical.

The root tree top events are as follows: the initiating event, the POS Group, and the time window. For each of the three POS Groups, there are four possible time windows. The model information pertaining to POS Group and time window is conveyed via the split fractions and fault trees assigned to the branches using IRRAS[4] event tree rules. The fault tree assignments for the loss of RHR event tree are shown in Figure 1, and the rules that accomplish these assignments are defined in the IRRAS linking rules for the RHR event tree.

For a POS Group, the success criteria for the fault trees called by the event tree are dependent on the time window. This event tree structure is intended to be as generic as possible, allowing plant-specific variability to be modeled at the fault tree level. This structure allows flexibility in performing the two types of event analysis: initiating event assessment and condition assessment.

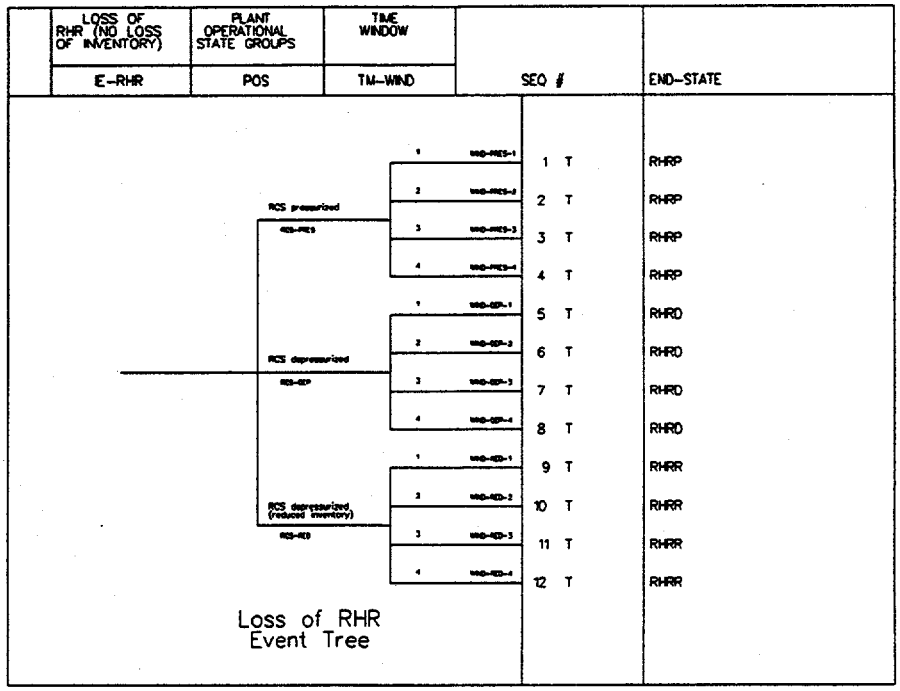


Figure 1. Loss of RHR event tree (root tree).

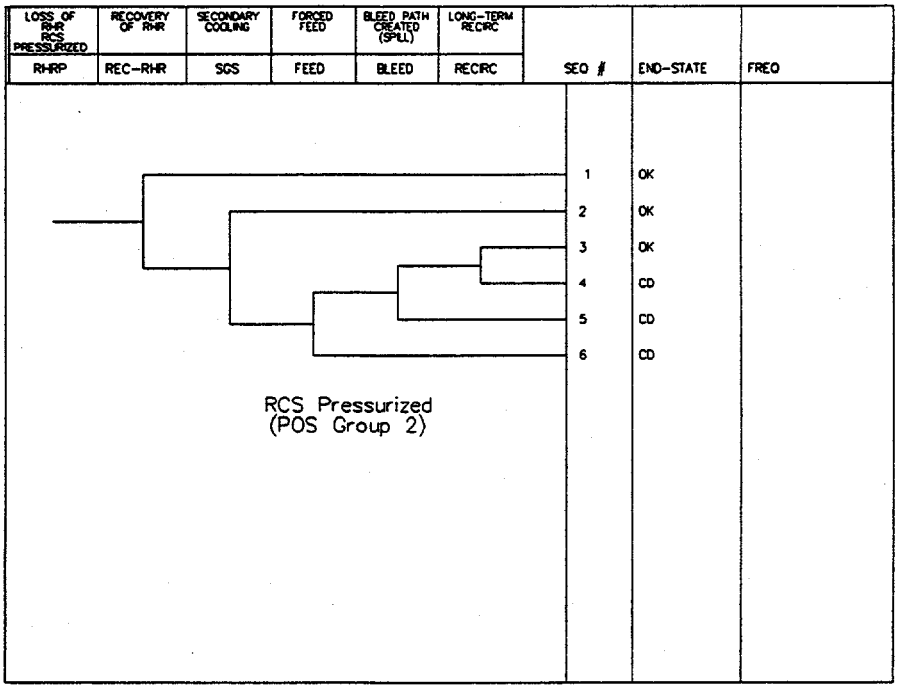


Figure 2. Loss of RHR (RCS pressurized) transfer event tree.

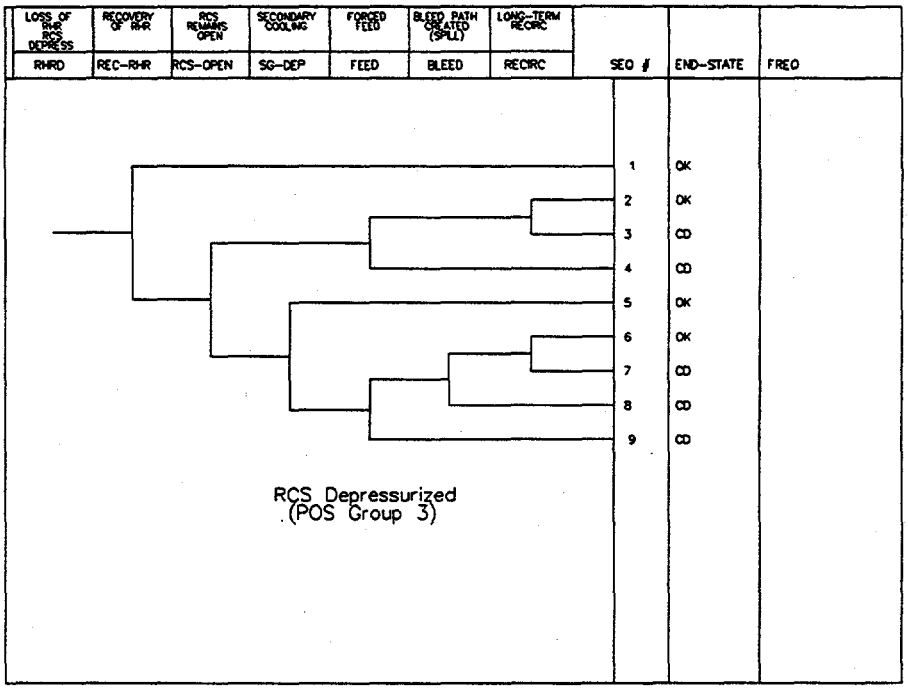


Figure 3. Loss of RHR (RCS depressurized) transfer event tree.

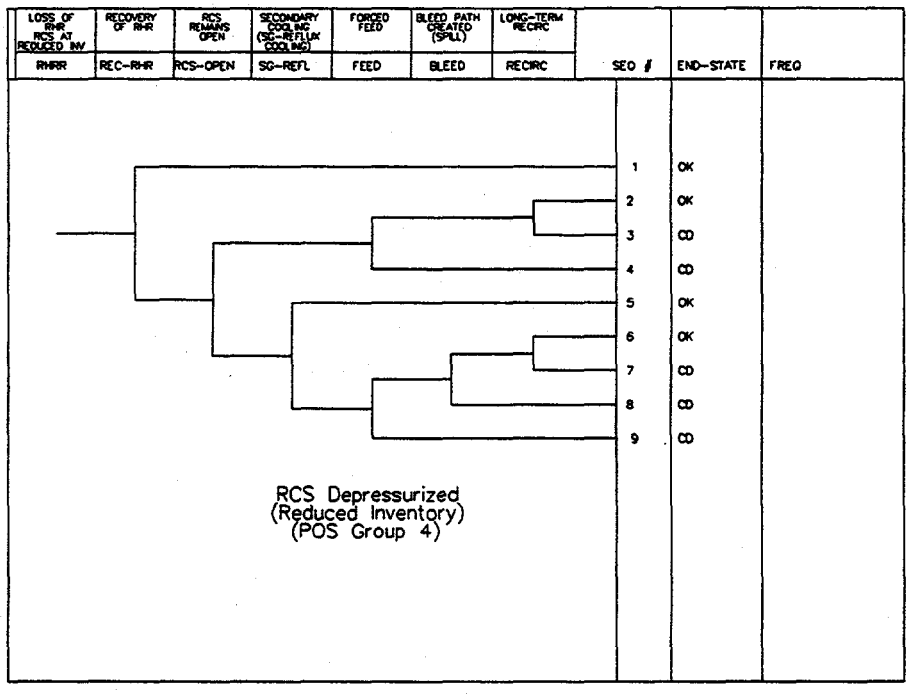


Figure 4. Loss of RHR (RCS at reduced inventory) transfer event tree.

An initiating event assessment evaluates the risk associated with a specific initiating event that occurred. For an initiating event assessment, the user would use only the portion of the model that pertains to the specific POS Group and time window in which the actual initiating event took place. In Figure 1, for example, if the initiating event was a loss of RHR that occurred while the plant was at reduced inventory during time window 2 (between 75 and 240 hours after shutdown), the user would effectively turn off all branches through the event tree except the branches leading to sequence 10. Sequence 10 transfers to the event tree appropriate for loss of decay heat removal during time window 2. The core damage sequences for this case would have the sequence numbering 10-3, 10-4, 10-7, 10-8, and 10-9 (see Figure 4).

A condition assessment evaluates the risk for a particular set of conditions discovered in the plant. No specific initiating event had occurred. For a condition assessment, where any initiator could occur, not only the duration of the condition but also the applicable POS Groups and time windows would need to be determined from the actual event. For an actual condition assessment, many combinations of POS Groups and time windows are possible. The fraction of time during which the condition existed in a particular POS Group and time window would be based on the actual event. If an actual condition spanned several shutdowns, the user may select the probabilities for a particular POS Group and time window that are based on available Surry data to model "average" conditions. This may be desirable if no other data are accessible to the user. The user can specify the type of outage as well: (1) refueling outage, (2) drained maintenance, or (3) non-drained maintenance with RHR.

For the purposes of illustration in this paper, only the Loss of RHR event tree will be further described.

The loss of RHR event tree begins on Figure 1, and transfers to Figures 2, 3, and 4 as indicated in the end state column. (In IRRAS, event trees with a "T" next to the sequence number transfer to the name indicated in the end state column.) The top events on Figure 1 are described below:

Top Event IE-RHR. This top event represents the initiating event for loss of RHR.

Top Event POS. This top event represents the probability that a particular POS Group is entered. An "average" probability is used as the default in the model; however, the user may need to specify this probability (fraction of time) when performing condition assessments.

Top Event TM-WIND. This top event represents the probability that the plant is in a particular time window given that the plant is in a particular POS Group. An "average" probability is used as the default in the model; however, the user may need to specify this probability (fraction of time) when performing condition assessments.

The loss of RHR top events are described below for each transfer event tree (Figures 2, 3, and 4):

Top Event REC-RHR. This top event models recovery of RHR including the human error and RHR system failures.

Top Event RCS-OPEN. This top event models the probability that the RCS is open due to the configuration present during shutdown. This top event is questioned in the depressurized case and the reduced inventory case where the RCS may have a bleed path available to prevent over pressurization while nozzle dams are installed. The RCS opening must be of sufficient size to provide an adequate bleed path for "feed."

Top Event SGS. This top event models secondary cooling via steam generators for the pressurized case where the steam generators would typically be available.

Top Event SG-DEP. This top event models secondary cooling via steam generators for the depressurized case where the steam generators may or may not be available.

Top Event SG-REFL. This top event models secondary cooling via reflux cooling with steam generators for the reduced inventory case where the steam generators may or may not be available.

Top Event FEED. This top event models RCS feed via any allowable combination of pumps specified in the success criteria. The provision of gravity feed has been made in this top although primarily "forced" feed is modeled. The gravity feed portion of the model is available but uses the human error probability of 1.0 assigned in NUREG/CR-6144.

Top Event BLEED. This top event represents creation of an adequate bleed path.

Top Event RECIRC. This top event represents long term recirculation which is only applicable to time windows 1 and 2.

All of the loss of RHR event trees result in successful RCS heat removal by (1) recovery of RHR cooling, (2) secondary cooling via steam generators, or (3) feed, bleed, and recirculation if needed. The loss of RHR (RCS depressurized) event tree and loss of RHR (RCS at reduced inventory) question whether the RCS is open (and not closeable in the time available). When the RCS is open, secondary cooling cannot be provided; however, a bleed path is established by the RCS opening. The loss of RHR (RCS at reduced inventory) event tree results in successful RCS heat removal by secondary cooling *via reflux cooling* using the steam generators.

IV. FAULT TREE DESCRIPTION

The fault trees developed for the shutdown models were based on the fault trees in the full-power ASP models and NUREG/CR-6144 as much as possible. The success criteria are the same as found in NUREG/CR-6144. The shutdown fault trees are relatively simple models using supercomponents for basic events whenever possible. Supercomponents are basic events that represent an entire string of simple basic events that would generally appear under an "OR" gate in a typical fault tree. The use of supercomponents reduces the size of the fault trees and the resulting minimal cut sets while retaining the desired level of modeling completeness. The fault trees do not include failures of the support systems, except for basic electric power needs.

A typical shutdown model fault tree is shown in Figure 5 (BLEED top event). The same shutdown fault tree is used for each of the different time windows. House events are used to turn on and off the appropriate portions of the logic for a specified time window and event tree sequence and to assign the appropriate basic event values. Flag Sets are used to define the house event settings (TRUE/FALSE). Flag Sets are groups of house event settings that are needed for specific event tree sequences. The Flag Sets are used to accomplish the following:

- Assign human error probabilities based on initiating event, time window, and POS Group.
- Assign test and maintenance unavailabilities based on time window and POS Group.
- Assign system power dependencies from offsite power to emergency power for LOOP sequences.

The use of house events in the event trees, while making the trees a bit larger, dramatically reduced the number of fault trees needed in the LP/SD models.

Component basic event data was based on the full-power ASP models and the Surry LP/SD study. Basic event data pertaining to test and maintenance unavailabilities and human error probabilities were obtained from the Surry LP/SD study and the Surry full-power Probabilistic Risk Assessment (NUREG/CR-4550[5]).

V. CONCLUSION

The feasibility of creating relatively simple, compact models that capture the important aspects of low power and shutdown risk was proven. The shutdown models developed for this project were comparable in size to the full-power, internal event ASP models for the same number and types of initiating events. The level of complexity with the different POS Groups and time windows, while much simpler than a typical full-scope shutdown risk model, is somewhat greater than previously experienced in the ASP program. However, with a little familiarization, it should not be difficult for an outside analyst to pick up a model and documentation and begin using it.

VI. REFERENCES

1. 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,* Vol. 2, NUREG/CR-6144, June 1994.

2. K. D. Russell, et al., *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 5.0, Graphical Evaluation Module (GEM) Reference Manual,* Vol. 6, NUREG/CR-6116, October 1995.

3. K. D. Russell, et al., *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 5.0,* NUREG/CR-6116, July 1994.

4. K. D. Russell, et al., *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 5.0, Integrated Reliability and Risk Analysis System (IRRAS) Reference Manual,* Vol. 2, NUREG/CR-6116, July 1994.

5. R. C. Bertucio and J. A. Julius, *Analysis of Core Damage Frequency: Surry Unit 1 Internal Events,* Vol. 3, NUREG/CR-4550, April 1990.

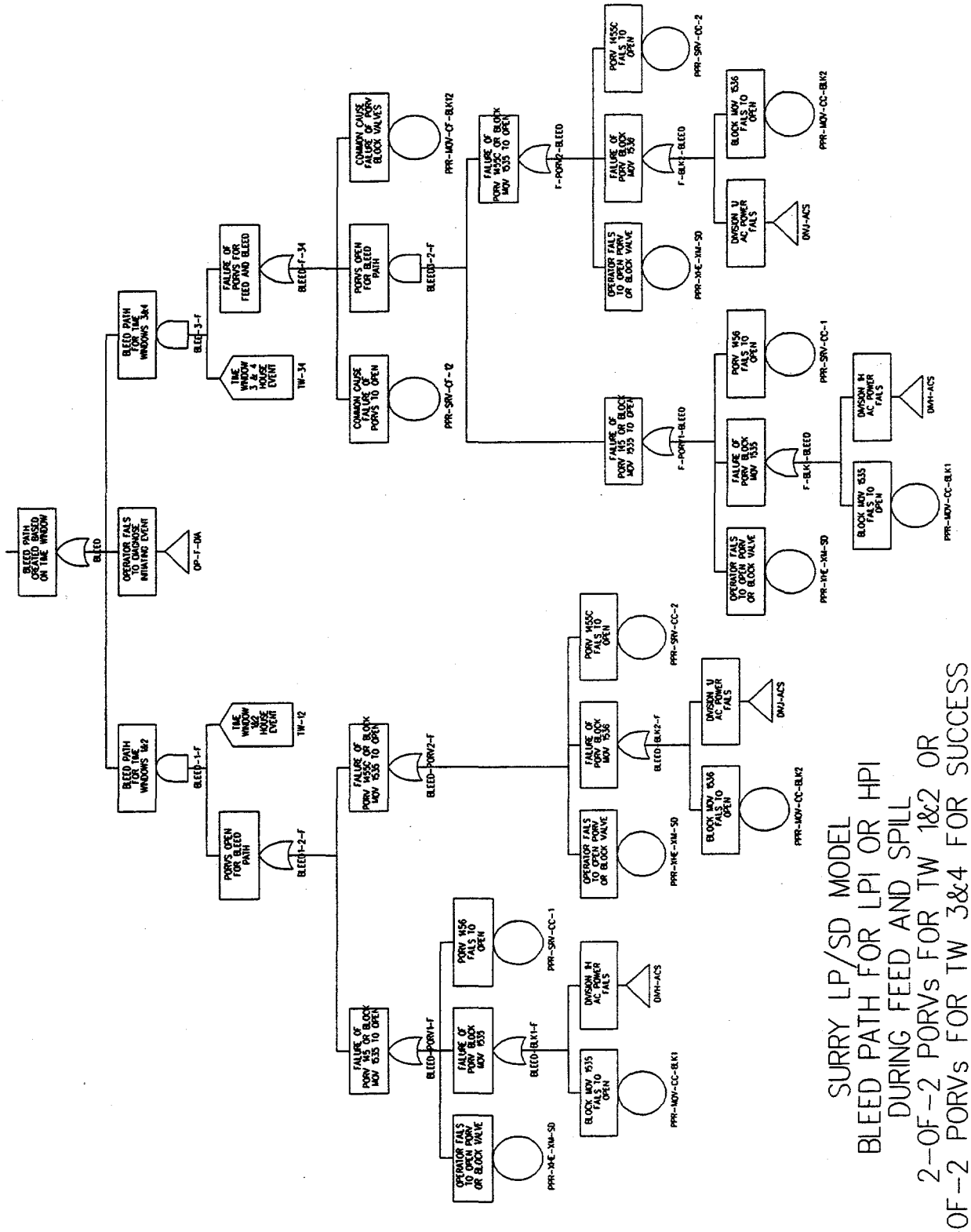


Figure 5. Fault tree for the BLEED top event.

ACCIDENT SEQUENCE PRECURSOR ANALYSIS LEVEL 2/3 MODEL DEVELOPMENT

Christiana H. Lui
U.S. Nuclear Regulatory Commission
Mail Stop T10E50
Washington, DC 20555
(301)415-6200

William J. Galyean
Idaho National Engineering Laboratory
P.O. Box 1625, MS 3850
Idaho Falls, ID 83415
(208)526-0627

Thomas D. Brown
Sandia National Laboratories
P.O. Box 5800, MS 0748
Albuquerque, NM 87185
(505)844-6134

Douglas A. Brownson
Idaho National Engineering Laboratory
P.O. Box 1625, MS 3840
Idaho Falls, ID 83415
(208)526-9460

Julie J. Gregory
Sandia National Laboratories
P.O. Box 5800, MS 0748
Albuquerque, NM 87185
(505)844-7539

ABSTRACT

The U.S. Nuclear Regulatory Commission's Accident Sequence Precursor (ASP) program currently uses simple Level 1 models to assess the conditional core damage probability for operational events occurring in commercial nuclear power plants (NPP). Since not all accident sequences leading to core damage will result in the same radiological consequences, it is necessary to develop simple Level 2/3 models that can be used to analyze the response of the NPP containment structure in the context of a core damage accident, estimate the magnitude of the resulting radioactive releases to the environment, and calculate the consequences associated with these releases. The simple Level 2/3 model development work was initiated in 1995, and several prototype models have been completed. Once developed, these simple Level 2/3 models are linked to the simple Level 1 models to provide risk perspectives for operational events. This paper describes the methods implemented for the development of these simple Level 2/3 ASP models, and the linkage process to the existing Level 1 models.

I. INTRODUCTION

The U.S. Nuclear Regulatory Commission's Accident Sequence Precursor (ASP) program was initiated by the Office of Nuclear Regulatory Research (RES). The ASP program provides a probabilistic method for reviewing operational experience to determine and assess both known and previously unrecognized vulnerabilities that could lead to core damage accidents. The ASP program is currently implemented by the Office of Analysis and Evaluation of Operational Data (AEOD), and simple Level 1 plant models are used to assess the conditional core damage probability for internal initiating events during full power operation. Since not all accident sequences leading to core damage will result in the same radiological consequences, it is necessary to develop simple Level 2/3 plant models that can be used to analyze the response of the containment structure in the context of a core damage accident, estimate the magnitude of the resulting radioactive releases to the environment, and calculate the consequences associated with these releases. Once developed, these simple Level 2/3 models are linked to the simple Level 1 models to provide risk perspectives for operational events.

II. APPROACH

The ASP Level 2/3 model development work was initiated in 1995, and has been divided into three phases: feasibility study, reference model development, and production. All commercial nuclear power plants (NPPs) were first sorted into groups based on the combination of different containment and nuclear steam supply system designs. This initial categorization produced four boiling water reactor (BWR) groups and six pressurized water reactor (PWR) groups. During the feasibility study, four plants, two PWRs and two BWRs, were selected across these plant groups for which the Level 2/3 models were developed. The objectives were to demonstrate (1) the process for the simple Level 2/3 model development,

(2) the information required for the development of these simple Level 2/3 models, (3) the appropriate interface between the Level 1 and Level 2/3 models, and (4) the integration of Level 2/3 models into the existing ASP software, SAPHIRE[1]. Among the four plants, one PWR and one BWR had detailed probabilistic risk assessments (PRA) performed during the NUREG-1150[2] study and the other two plants did not. Therefore, the process to develop simple Level 2/3 models when the detailed PRA models were not available was also investigated. During the reference model development phase, the current phase, one particular plant was selected from each of the remaining plant groups, and the simple Level 2/3 models are being developed following the same process which was formulated during the feasibility study. The reasonableness of extrapolating the reference plant model to the remaining plants in the same group will also be examined. If needed, additional NPP groups will be formed, and a reference plant model will be developed for each new group. The current NPP groups and the reference plant selected for each group are listed in Table 1. During the production phase, simple Level 2/3 models will be built for all NPPs and linked to their corresponding Level 1 ASP models.

The ASP Level 2/3 modeling process follows the NUREG-1150 Level 2/3 modeling process closely. All accident sequences leading to core damage are sorted into plant damage states (PDS) based on the type of initiating events and the status of important mitigation systems. Accident progression analyses are performed for the different PDSs, and source terms (STs) are estimated at the conclusion of the accident progression analyses. Consequence calculations are performed for the different STs. The risk results are produced by linking all the analyses. The overall process is illustrated in Figure 1 and explained in the following subsections.

A.. Level 1 and Level 2/3 Interface

Since the end states of the existing ASP Level 1 models indicate only the core status (OK or Core Damage) for the accident sequences, and often do not include sufficient containment system information that is crucial for the Level 2 analysis, bridge event trees (BET) which model the required containment systems are developed and connected to those accident

Table 1. Plant groups and reference plant for each group

Reactor Group	Reference Plant
Westinghouse PWR with a large dry containment	Zion
Combustion Engineering PWR with PORVs	Calvert Cliffs
Westinghouse PWR with a subatmospheric containment	Surry
Westinghouse PWR with an ice condenser containment	Sequoyah
Combustion Engineering PWR without PORV	Palo Verde
Babcock & Wilcox PWR	Oconee
BWR with Mark I containment (steel drywell and wetwell)	Peach Bottom
BWR with Mark I containment (reinforced concrete drywell and reinforced concrete with steel liner wetwell)	Brunswick
BWR with Mark II containment	LaSalle
BWR with Mark III containment	Grand Gulf

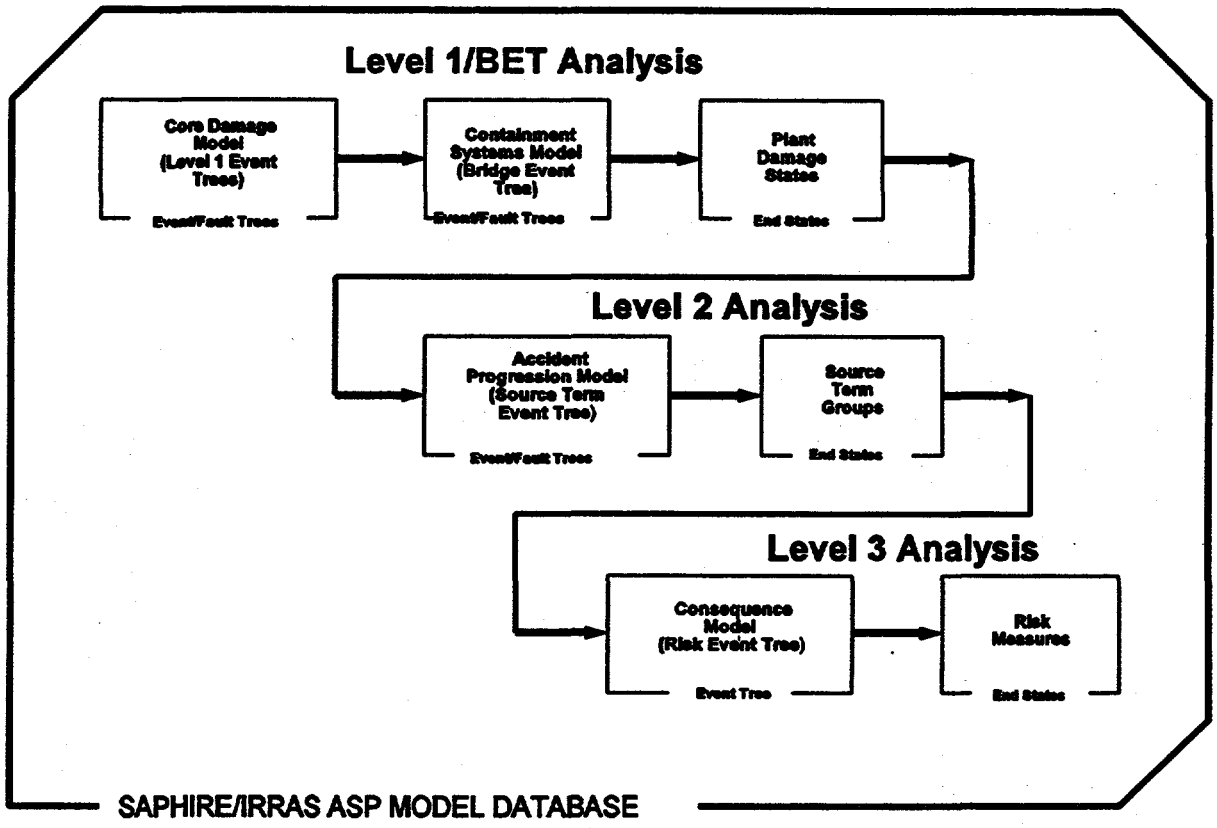


Figure 1. Linking Level 2/3 with Level 1 ASP models in the SAPHIRE/IRRAS database

sequences leading to core damage. The use of BET allows system dependencies, such as electrical power, between the various systems to be accounted for in the fault trees that support the BET top events. The typical top events considered in a PWR BET are: low pressure injection, low pressure recirculation, containment spray, containment spray recirculation and containment emergency fan cooler system. The typical top events considered in a BWR BET are: low pressure injection, containment sprays and containment venting. After propagating the core damage event through the BET, the PDSs are generated using a set of logic rules that examine the status of those systems affecting the subsequent accident progression. The various PDSs then become the new end states for the Level 1 analysis and the initiating event for the Level 2 analysis. Typical characteristics that are examined in the PDS logic rules can be found in Table 2.

B. Accident Progression Analysis

To be consistent in the level of detail with the existing Level 1 ASP model, the Level 2 ASP event tree which is termed Source Term Event Tree (STET) in this project models approximately a dozen or so top events. When a detailed PRA is available for a plant, only those phenomena and events deemed most relevant to the estimation of STs are extracted from the detailed analysis, and the split fractions are generated by rolling up the detailed accident progression event tree (APET) to the corresponding level. The advantage of this approach is that the simplicity of the resulting model makes it fast-running and more transparent to the users. However, unless the user of the model has a good understanding of the detailed accident progression model from which the STET was simplified, it is difficult for the user to modify the split fractions in the STET

Table 2. Typical Plant Damage State (PDS) Characteristics

Characteristic	BWR	PWR
1	Status of the Reactor Protection System	Status of the Reactor Coolant System at the Onset of Core Damage
2	Status of Electric Power	Status of Emergency Core Cooling Systems
3	Status of Reactor Pressure Vessel Integrity	Status of Containment Heat Removal Systems
4	Status of the Pressure in the Reactor Pressure Vessel	AC Power
5	Status of High Pressure Injection Systems	Contents of the Reactor Water Storage Tank
6	Status of Low Pressure Injection Systems	Heat Removal from the Steam Generators
7	Status of Containment Heat Removal	Cooling for the Reactor Coolant Pump Seals
8	Status of Containment Venting	Status of the Containment Fan Coolers
9	Status of Containment Integrity	
10	Timing for Onset to Core Damage	

without affecting the dependencies between the different physical phenomena modeled in the detailed accident progression analysis which are preserved during the simplification process.

In anticipation of future ASP model refinements that may require user manipulation of the detailed accident progression information in the ASP software, during the feasibility study, another approach for STET split fraction generation was investigated. For one of the NUREG-1150 plants, fault trees that mimic the logic and reproduce the quantitative information contained in the detailed APET were built to support the STET top events. These fault trees had the NUREG-1150 APET questions as basic events. Therefore, if the user desires to change the response to a particular question, the change would be reflected in all the STET fault trees, and thus preserves the dependencies among the different phenomena. This approach, though promising, was very resource intensive. After examining the project scope and schedule, a programmatic decision was made to use the "rolling up" method for split fraction generation, and the users are advised not to change the split fractions in the STET without first consulting the model developers.

When a detailed accident progression model is not available for a plant, as a starting point, a NUREG-1150 plant PRA that is closest to the plant of interest is used as a surrogate. The Final Safety Analysis Report, Individual Plant Examination submittals, and relevant thermal-hydraulic calculations are used to supplement the information required to develop and quantify the STET. Table 3 lists the typical STET top events and the associated phenomena examined under each top event for both PWRs and BWRs.

C. Source Term Analysis

Based on a set of logic rules that examine the accident progression characteristics, the STET sequences are mapped into like groups for ST estimations. These ST characteristics can be found in Table 4. The XSOR code which was developed during the NUREG-1150 study, and the expert judgments that were elicited for ST estimation during that study have been applied to several reference plant models. Since the objective of this ASP model development effort is to build Level 2/3 models for all operating NPPs, and the NUREG-1150 study was performed for a limited number of NPPs, modifying the ST database from the NUREG-1150 study for all other plants' ST estimation may not always be feasible. An alternative means for ST estimation, therefore, has been developed. A fast-running Parametric Source Term (PST) code which can readily utilize results from plant-specific thermal hydraulic calculations for ST estimations has been implemented for the remaining reference plant models. More information on the PST code and its application in this particular model

Table 3. Typical Phenomena and Systems Considered in Source Term Event Tree (STET)

Initiating Event: Plant Damage State (PDS)		
Top Event	**PWR**	**BWR**
1	Occurrence of Steam Generator Tube Rupture (SGTR) - No SGTR - SGTR	Status of Vessel Breach (VB) - No VB - VB at low pressure - VB at safety relief valve set point
2	Status of containment Isolation - Containment isolated - No containment isolation	Early Status of the Suppression Pool - No early flow from the reactor pressure vessel (RPV) to the drywell - Partial flow from the RPV to the drywell - Complete flow from the RPV to the drywell
3	Reactor Coolant System (RCS) Pressure at Vessel Breach - Safety relief valve set point - High RCS pressure - Intermediate RCS pressure - Low RCS pressure	Early Status of Drywell Sprays - Operational - Not operational
4	Mode of Vessel Breach - No vessel breach - Small vessel failure area - Large vessel failure area	Early Containment Venting (hardware and operator action) - Vented - Not vented
5	Early Containment Failure Mode - No failure - Leak - Rupture - Catastrophic	Early Containment Failure - No early containment failure - Leak in the wetwell - Leak in the drywell - Leak in the drywell head - Rupture in the wetwell - Rupture in the drywell - Rupture in the drywell head
6	Status of Containment Heat Removal Systems - Available - Not available	Late Injection of Coolant to the Reactor Cavity - Injection to the cavity and core debris - No injection
7	Presence of H_2O in Reactor Vessel Cavity - Wet - Dry	Molten Core Concrete Interaction (CCI) - No CCI - CCI occurs in a flooded cavity - CCI occurs in a dry cavity
8	Occurrence of Core Concrete Interaction - No core concrete interaction - core concrete interaction occurs	Late Status of Drywell Sprays - Operational - Not operational
9	Late Containment Failure Mode - No failure - Leak - Rupture - Catastrophic	Late Containment Venting - Vented - Not vented

Table 3. Typical Phenomena and Systems Considered in Source Term Event Tree (STET) (continued)

Top Event	PWR	BWR
10		Late Containment Failure - No late containment failure - Leak in the wetwell - Leak in the drywell - Leak in the drywell head - Rupture in the wetwell - Rupture in the drywell - Rupture in the drywell head
11		Level of Reactor Building Bypass - Nominal or small bypass - Partial or complete bypass

development effort can be found in a separate paper in these proceedings[3]. If a large number of unique STs are generated, to expedite the consequence calculations, the STs are partitioned into source term groups (STGs) that would give similar health effects consequences. Since the STs will not change for a given severe accident scenario, the ST estimation is performed once and hardwired to the STET endstates in the ASP database in SAPHIRE. The STs or STGs become the initiating event for the Level 3 analysis.

D. Consequence Analysis

The MACCS[4] code is used to calculate the offsite consequences associated with each ST or STG. The consequence calculations are performed for a generic site, and include: 50-mile population dose, 50-mile population thyroid

Table 4. Source Term Characteristics

Characteristic	BWR	PWR
1	Core Damage Time	Containment Failure Timing
2	Level of In-Vessel Zr Oxidation	Availability of Containment Heat Removal Systems
3	Status of Vessel Breach	Occurrence of Core Concrete Interactions
4	Fraction of Core Participating in Direct Containment Heating or an Ex-Vessel Steam Explosion	Reactor Coolant System Pressure at Vessel Breach
5	Containment Failure Mode	Mode of Vessel Breach
6	Containment Failure Timing	Occurrence of Steam Generator Tube Rupture
7	Status of Drywell Sprays throughout the Accident	Presence of Water in the Reactor Cavity
8	Occurrence of Molten Core Concrete Interaction	Amount of Oxidation in Vessel
9	Level of Suppression Pool Bypass	Containment Failure Size
10	Level of Reactor Building Bypass	Core Damage Time

dose, number of early and latent fatalities within 50 miles from the site boundaries, average individual early fatality risk within 1 mile from the site boundary, and average individual latent cancer fatality risk within 10 miles from the site boundary. Since these consequence results will not change for a given ST, once calculated, they are hardwired to the corresponding ST or STG group in the ASP database in SAPHIRE.

E. Risk Integration

The information on the split fractions from the Level 1 and Level 2 analyses is retained in SAPHIRE for each consequence measure. The risk results are shown in an event tree format, the Risk Event Tree (RET), which is depicted in Figure 2. The end states of the RET give the numerical values for the different types of health effects risk.

III. IMPLEMENTATION

All parts of the ASP models, including Level 1 and Level 2/3, have been constructed for execution in SAPHIRE. Several coding changes have been completed to automate the linkage process between the existing Level 1 models and the Level 2/3 models, and to accommodate the need for performing Level 2/3 analyses. Currently, the user has the option of

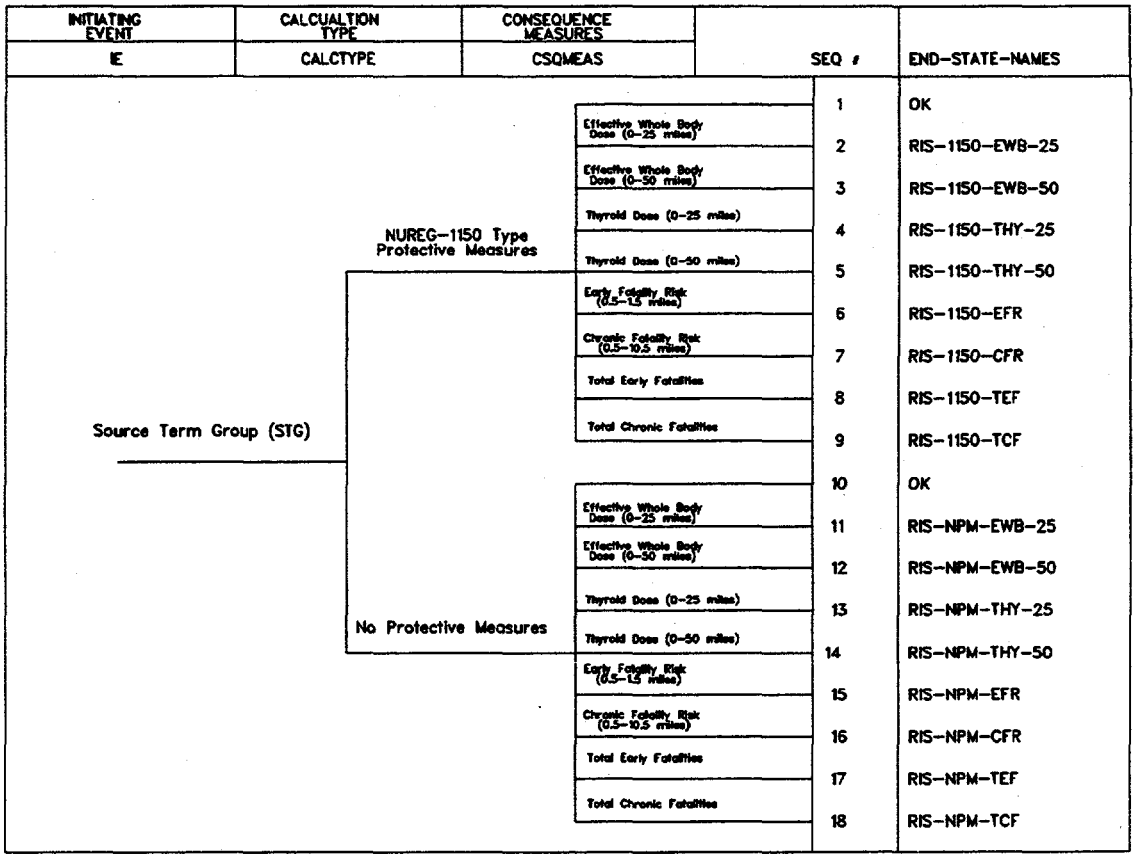


Figure 2. Risk Event Tree (RET) for the Accident Sequence Precursor Program.

carrying the analysis to estimating conditional core damage probability or obtaining risk results. In the near future, conditional containment failure probability will also be available from the ASP analysis.

The Level 2/3 analysis, as illustrated in Figure 1, is performed by repeating the same process several times in SAPHIRE: linking trees, analyzing sequences, generating cut sets, partitioning cut sets, gathering end states, and re-generating the database so that the split fractions are properly propagated throughout the analysis. Although conceptually straightforward, many individual steps are required to complete this analysis process. With this many steps involved, it is extremely easy to make a mistake. Therefore, a simpler and thus less error prone execution process is being developed to ease the Level 2/3 analysis process using SAPHIRE.

Most of these simple Level 2/3 models are being developed from detailed PRA databases and codes. Therefore, if a more in-depth analysis is necessary, the original detailed PRA model can always be exercised.

IV. SUMMARY

The objective for the Level 2/3 ASP model development work is to complete a versatile database package that can be directly interfaced with the existing Level 1 models, is technically correct, incorporates NUREG-1150 results and any new information since the NUREG-1150 study, is consistent with the level of detail required by the existing ASP program, and can be executed in SAPHIRE. These models are fast-running and can be used in a variety of ways to provide risk insights, such as estimating conditional containment failure probability and health effects risk.

An approach was formulated during the feasibility study for the development of simple Level 2/3 models for the ASP program. The required SAPHIRE coding changes have also been completed to facilitate the linkage between the existing Level 1 models and the newly developed Level 2/3 models, and the required capability for performing Level 2/3 analyses. Ten reference Level 2/3 plant models, including six PWR models and four BWR models, which cover a wide variety of containment and nuclear steam supply systems designs will be complete by late 1996. These reference models will be used as the starting point for developing the simple Level 2/3 models for the remaining NPPs.

As the Level 2/3 models are completed, they are linked to the corresponding Level 1 models, and are incorporated into the ASP database. As the Level 1 ASP models evolve to include more analysis capabilities, the Level 2/3 models will also be refined to reflect the appropriate level of detail needed for the new capabilities.

REFERENCES

1 K. Russell, et al., *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 5.0*, NUREG/CR-6116, EGG-2716, Idaho National Engineering Laboratory, Idaho Falls, Idaho, July 1994.

2. U.S. Nuclear Regulatory Commission, *Severe Accident Risks: An Assessment for five U.S. Nuclear Power Plants*, NUREG-1150, Washington, DC, December 1990.

3. J. L. Rempe, M. J. Cebull, and B. G. Gilbert, *PST - A New Method for Estimating PSA Source Terms*, presented at American Nuclear Society International Topical Meeting, PSA '96: Probabilistic Safety Assessment, Part City, UT, September 29 - October 3, 1996.

4. D. I. Chanin, et al., *MACCS Version 1.5.11.1: A Maintenance Release of the Code*, NUREG/CR-6059, SAND92-2146, Sandia National Laboratories, Albuquerque, New Mexico, October 1993.

TIME-INDEPENDENT AND TIME-DEPENDENT CONTRIBUTIONS TO THE UNAVAILABILITY OF STANDBY SAFETY SYSTEM COMPONENTS

by
E. V. Lofgren
Science Applications International Corporation
Fairfax Station, Virginia 22039

S. Uryasev and P. Samanta
Brookhaven National Laboratory
Upton, New York 11973

ABSTRACT

The unavailability of standby safety system components due to failures in nuclear power plants is considered to involve a time-independent and a time-dependent part. The former relates to the component's unavailability from demand stresses due to usage, and the latter represents the component's unavailability due to standby-time stresses related to the environment. In this paper, data from the nuclear plant reliability data system (NPRDS) were used to partition the component's unavailability into the contributions from standby-time stress (i.e., due to environmental factors) and demand stress (i.e., due to usage). Analyses are presented of motor-operated valves (MOVs), motor-driven pumps (MDPs), and turbine-driven pumps (TDPs). MOVs fail predominantly (approx. 78%) from environmental factors (standby-time stress failures). MDPs fail slightly more frequently from demand stresses (approx. 63%) than standby-time stresses, while TDPs fail predominantly from standby-time stresses (approx. 78%). Such partitions of component unavailability have many uses in risk-informed and performance-based regulation relating to modifications to Technical Specification, in-service testing, precise determination of dominant accident sequences, and implementation of maintenance rules.

1. INTRODUCTION

The unavailability of standby safety-system components encompasses many contributions which include unavailability due to random failures that may occur during the standby period. Typically, this unavailability is either expressed as a constant or as a function of the failure rate and the test interval. In obtaining this value, the number of failures observed is used to obtain either the failure rate (considering the corresponding standby time) or a constant unavailability (considering the corresponding number of demands), but no analysis of the causes of the failures is made. The failures may be either due to stresses from demand or stresses during the standby period. Failures can be partitioned into these two types of stresses and, correspondingly, the component's unavailability can be obtained as a sum of time-independent and time-dependent terms. Such a derivation of component unavailability is very helpful in many applications of probabilistic risk assessments (PRAs) in decisions about the operability of equipment, surveillance testing, and maintenance.

In this paper, we discuss the following topics:

(a) approaches to partitioning the component's unavailability into standby- and demand-failure contributions by dividing its failure records into standby stress and demand stress,

(b) applications for motor-operated valves (MOVs), motor-driven pumps (MDPs), and turbine driven pumps (TDPs).

We used readily accessible data, e.g., nuclear plant reliability data system (NPRDS), in developing the approaches and demonstrating the applications. Previous attempts at separating component unavailability into time-independent and time-dependent contributions focussed on plant-specific maintenance records (Ref. 1, 2) which are difficult to obtain and resource-consuming to analyze.

2. COMPONENT UNAVAILABILITY MODEL: SEPARATION INTO TIME-DEPENDENT AND TIME-INDEPENDENT CONTRIBUTIONS

The unavailability of standby components from failures usually is estimated in probabilistic risk assessments (PRAs) using a model of the form:

q = constant (i.e. a probability of failure on demand), or;
$q = 1/2\lambda T$ (where λ is the failure rate and T is the time between tests of the component)

Other unavailability terms also may be added to the above, such as unavailability of the component due to repair of unplanned degradations or failures, or unavailability from planned outages. These failure models make no assumptions about the type of stress leading to the component's failure. For instance, if a component fails primarily from environmental stresses when it is in standby, and the constant failure probability model is used to assess its

unavailability, regardless of its test period, the model may underestimate the contribution to risk for components having long test periods, and overestimate the contribution for those with short test periods.

In fact, a component's unavailability from failures may actually be of the form:

$q = \text{constant } (p) + 1/2\lambda T$

where the constant (p) represents the component's unavailability from demand stresses related to its usage, and the $1/2\lambda T$ term represents the component's unavailability from standby stresses related to the component's environment, and, therefore, is a function of the time between tests.

Applications that would benefit from this more comprehensive component unavailability model include the following ones: evaluating the impact on risk from extending surveillance test intervals for technical specifications and in-service testing; using generic failure probabilities more appropriately, especially for components with very long or very short test intervals; gaining insights for dominant accident sequences, especially those involving infrequently tested valves; and, perhaps, providing insights for scheduling preventive maintenance.

3. ANALYSIS APPROACH

In discussing the analysis approach, MOVs will be used as an example; the approach was the same for all types of components, with only minor exceptions. The NPRDS MOV records for 16 plants, 5 systems at each plant, and 5 years of data at each plant, were reviewed to categorize the data as standby stress or demand stress. Each record was placed in one of four categories: standby-stress-related; demand-stress-related; indeterminate events; or inappropriate events. Those records where the cause of failure could be easily determined fell into either the standby-stress or demand-stress categories. Those event records that had insufficient information to so categorize them were placed in the indeterminate category. Records that represented events that were of no risk consequence, as modeled in PRAs (i.e., minor external leaks whose repair was delayed until the next plant shutdown), categorized as inappropriate.

Next, the data were grouped by usage or application, such as the operating environment (i.e., the MOV regulates a liquid as opposed to steam or gas), the type of system (i.e., the MOV is in the AFW, or is part of the HPSI), and the size of the MOV (i.e., 2 to 4 inches, or 13 to 24 inches).

Following this, denominator information was obtained to estimate the failure probability of demand stress and the standby stress failure rate for each of the application categories, so that both a failure probability and a failure rate could be estimated for each. This involved counting the number of valves in the data population of each application category. The denominator for the failure probability of demand stress of an application category is the total number of demands

for all MOVs in the data population of that category. The denominator for the standby stress failure rate of an application category is the total MOV on-line time for all MOVs in that category.

The failure probability of demand stress for an application is estimated by dividing the number of MOV demand failures in the category by the number of MOV demands in the sample period for the category. The standby-stress failure rate for an application category is estimated by dividing the number of standby-stress failures for the category by the total MOV on-line time for MOVs in the category. To obtain accurate counts of failure, the failures in the indeterminate category were partitioned according to the fraction of standby- and demand-stress failures in the original partition. The resulting numbers of standby- and demand-events then were added to the failure counts in each category.

Several considerations were noted while partitioning component unavailability in this way. First, demand is difficult to count without recourse to detailed plant operating records. To compensate, the failure probability of demand stress was estimated by multiplying a generic failure probability by the fraction of events that were determined to be related to demand stress. This procedure was justified by assuming that the generic failure probability was likely to have been estimated originally using all failures, including demand-stress and standby-stress failures, so multiplying by the fraction of failures estimated to be demand-stress ones essentially provided a reasonable estimate of the failure probability of demand stress.

The second consideration involved the potential for subjectivity in dividing the data into standby stress and demand-stress categories. To compensate for potential subjectivity, we devised a set of key words and key-word combinations that would tend to identify a failure record as either standby-stress or demand-stress related. In addition, the indeterminate category was added to avoid guessing when there was insufficient information in the event record to reasonably assess the cause of failure. Finally, computer software using the key words and key-word combinations was developed to cross-check the data analysis and focus attention on those areas where the partitioning might be less objective than desired.

Several other considerations, particular to the NPRDS data base, were also noted. First, component counts using NPRDS information needed to be carefully done, since components that were replaced during the sample period were counted twice, once for the original component and once for its replacement. We checked the component counts against the system P&IDs in the plant FSARs. Second, the failure severity recorded in the NPRDS records does not always match the definition used in PRAs. Each record was independently evaluated for failure severity as used in PRAs. Finally, not all plants report completely to NPRDS, which is apparent from the numbers of records submitted in the sample period. To compensate, the MOV on-line times (denominators) were adjusted for those plants where incomplete reporting was suspected.

4. ANALYSIS RESULTS

Table 1 shows the results of partitioning the NPRDS data, and estimating demand-stress failure probabilities and standby-stress failure rates for several categories of MOV application.

Table 1
MOV Estimated Failure Probabilities and Failure Rates

Application Category	% Demand Stress	% Standby Stress	DS Failure Prob.*	SS Failure Rate
All MOVs	22	78	2.2E-4/d	2.3E-6/hr.
All PWR MOVs	21	79	2.1E-4/d	2.2E-6/hr.
All BWR MOVs	22	78	2.2E-4/d	2.4E-6/hr.
Liquid Environment	19	81	1.9E-4/d	2.3E-6/hr.
Gas/Steam Environ.	57	43	5.7E-4/d	2.2E-6/hr.
2 to 12 inch MOVs	22	78	2.2E-4/d	**
13 to 20 in. MOVs	21	79	2.1E-4/d	**

* All failure probabilities for demand stress were estimated using a generic failure probability of 1E-3/d multiplied by the fraction of failures in each application category that were evaluated as demand-stress related.

** Denominator data (MOV time on-line) could not be obtained for these estimates. However, based on the fractions that were related to standby stress, they likely range from 2.2E-6/hr. to 2.4E-6/hr.

The most striking feature of the table is the consistency of results among the application categories. The standby stress failure rates for all categories vary only from 2.2E-6/hr. to 2.4E-6/hr. Most of the demand-stress failure probabilities range from 1.9E-4/d to 2.2E-4/d, except that for MOVs operating in a gas/steam environment, estimated as 5.7E-4/d. It is not known why there is this difference. One possibility is that, if the actual MOV demands were counted, the demand-stress failure probability would come closer to the other values. We note that the estimate of failure rate for this application category is no different than the estimates for other categories. If there were a difference due to particular environmental stresses from this application category, it should show up as a difference in failure rates, not as a difference in demand-stress failure probabilities.

Table 2 gives the results of partitioning the NPRDS data, and estimating demand-stress failure probabilities and standby-stress failure rates for several motor- and turbine-pump applications.

Table 2
Motor- and Turbine-Pump Estimated Failure Probabilities and Failure Rates

Application Category	% Demand Stress	% Standby Stress	DS Failure Prob.	SS Failure Rate
All Pumps	59	41	5.9E-4/d *	1.6E-6/hr.
All Motor Pumps	63	37	6.3E-4/d *	1.4E-6/hr.
All Turbine Pumps	22	78	6.6E-4/d**	4.0E-6/hr.
PWR Motor Pumps	69	31	6.9E-4/d *	1.0E-6/hr.
BWR Motor Pumps	48	52	4.8E-4/d *	2.4E-6/hr.

* Demand-stress failure probabilities of motor pumps are estimated as the product of the fraction of failures identified as demand-stress related times a generic motor-pump failure probability of 1E-3/d.

** Demand-stress failure probability of turbine pumps is estimated as the product of the fraction of failures identified as demand-stress related times a generic turbine-pump failure probability of 3E-3/d.

The results for motor pump are not as consistent across application categories as were the MOV results. Overall, approximately 60% of motor pump failures may be related to demand stress, and about 40% to standby stress. However, for turbine pumps, the split is closer to 20% to 80%. From the standpoint of how they fail, motor pumps and turbine pumps appear to fail from different mechanisms. The former seem to fail from usage-related stresses slightly more often than from environmentally related stresses, while the latter fail predominately from environmentally related stresses.

5. CONCLUSIONS AND RECOMMENDATIONS

In this paper, data from the nuclear plant reliability data system (NPRDS), were used to partition component unavailability into standby stress (i.e., due to environmental factors) and demand stress (i.e., due to usage) contributions, rather than searching plant-specific data bases maintained at a nuclear plant site. The ability to use a database like NPRDS significantly reduces the efforts involved in making this division and makes such evaluations practical.

The applications carried out for MOVs and pumps provide the following important insights:

(a) MOVs appear to fail predominantly from environmental factors; the relative contribution of standby-stress related failures is more or less unchanged for different sizes of MOVs.

(b) MOVs operating in gas/stream environment, as opposed to liquid one, have a relatively

higher contribution from demand-stress failures. This finding implies that frequent testing of MOVs operating in gas/steam may be less effective in controlling their unavailability.

(c) Motor-driven pumps appear to fail slightly more frequently from demand stresses than standby-time stresses, while turbine pumps appear to fail predominantly from standby-time stresses. This may imply that there should be slightly different testing requirements for controlling their unavailability.

The partitioned data on component unavailability have potential uses in risk-informed and performance-based regulation. The data should allow risk-informed assessment of requests for extending test interval, and should result in more precise determination of dominant accident sequences in a PRA, especially those involving components with very long or very short test intervals. In theory, partitioning unavailability data would establish optimum test intervals for the components, although it may not be practical to test at the optimum frequencies.

Also, procedures can be developed to partition the reliability data expected to be collected under the Reliability Data Rule, so providing the NRC and licensees with partitioned component unavailability data for risk-informed regulation.

REFERENCES

1. E.V. Lofgren and M. Thaggard, "Analysis of Standby and Demand Stress Contribution," NUREG/CR-5823, U.S. Nuclear Regulatory Commission, 1992.

2. T. Huovinen and U. Pulkkinen, "Parameter Estimation of Linear Standby Failure Model," Research Notes 891. Technical Research Center of Finland, Espoo, Finland, 1988.

A Summary of Lessons Learned Activities Conducted at the OECD Halden Reactor Project

Bruce P. Hallbert
OECD Halden Reactor Project
P.O. Box 173
N-1751 Halden NORWAY
tel.: +47 69 18 31 00
email: bruce.hallbert@hrp.no

Abstract

A series of lessons learned studies have been conducted at the OECD Halden Reactor Project. The purpose of these lessons learned reports are to summarize knowledge and experience gained across a number of research project. This paper presents a summary of main issues addressed in four of these lessons learned projects. These are concerned with software development and quality assurance, software reliability, methods for test and evaluation of developed systems, and the evaluation of system design features.

Introduction

Research at the OECD Halden Reactor Project is conducted on the design, development, and test and evaluation of human-machine systems for nuclear power plant process control. Much of the systems that are the focus of this research are designed to support the main control room staff. Examples of such systems include displays providing overview information of the nuclear power plant and key parameters, condition and critical function monitoring, electronic procedures, expert systems for fault diagnosis, alarm systems, core monitoring and thermal performance, and advanced integration concepts. Research activities with these systems have taken place over a number of years and have involved the effort of many persons. Hence, the reports about these systems are numerous and represent a large experience base. A series of lessons learned reports were undertaken to summarize the main findings and insights across a number of these research projects. The purpose of these lessons learned reports are to summarize the experience with these types of systems and identify general issues and principles applicable to the design, development, test and evaluation of such control room support systems. This paper summarizes four such lessons learned activities dealing with: 1) development and quality assurance of software systems; 2) software dependability; 3) methods and measures in the test and evaluation of human-machine systems, and; 4) design and evaluation of human-machine systems. Each of these are discussed separately below.

Lessons Learned from Experience with Development and Quality Assurance of Software Systems

The OECD Halden Reactor Project has developed a number of software systems within the research programs in the human-machine systems area. These programs comprise a wide range of topics: studies of software for safety-critical applications; development of different operator support systems; and software systems for building and implementing graphical user interfaces. The systems developed range from simple prototypes to installations in process plants.

In the development of these software systems, much experience has been gained in quality assurance of different types of software. The various software systems developed at Halden are described in a number of reports that also contain information on all phases of the development process. This includes the specification, design, coding, implementation and testing of software. However, this information is spread through a number of individual reports. So this lessons learned report provides a unified summary of the accumulated experience at the Halden Project in quality assurance of software systems. Emphasis is placed on presenting the factors that have been found important in developing software systems for nuclear power plant control rooms to obtain high-quality, reliable systems. In this

report the different software systems developed at the Halden Project have been grouped into three categories: specific software systems (one-of-a-kind deliveries); generic software products; and safety critical software systems. These categories have different requirements to the quality assurance process.

The report also addresses the experience from use of software development tools and proprietary software systems at Halden. Hence, the report provides lessons learned from the entire software development cycle. The lessons learned are organized by the software life cycle starting with the planning phase and ending with operation and maintenance. The main findings are summarized as follows.

Software Planning and Requirements Analysis

Good project planning is essential for successful implementation of a software project. The waterfall model for system development with configuration phases, baselines, and unit milestones provided a solid foundation for the detailed development plans. In addition to the time schedules, the software quality assurance procedures to be implemented in the project must be chosen. Also, a software quality assurance plan with reviews and audits must be included to ensure that the established procedures are followed.

Detailed time schedules for all phases - design, implementation, testing, and integration - have proven to be a necessity. It is of vital importance that those responsible for production of a specific unit of the software product plan within the given time frame. The activity plans made by the units form the basis for the progress reporting. The more detailed the unit plans are with respect to detailed sub-tasks and unit milestones, the easier and more accurate the progress reporting will be.

In safety-critical software projects for which a formal development process has been chosen a large part of the efforts involved are invested in the production and assessment of the specification. In most cases, only a minor part is invested in the actual implementation. Investing effort in system specification, clarifying the functional requirements and focusing on the specific needs of the end-users by discussing and reviewing the specifications has been most beneficial. Execution of a formal specification is an effective means for detecting specification errors and can be performed incrementally during the production of the specification. Execution also increases the comprehensibility of the specification, and thereby facilitates the communication between agents with widely varying technical backgrounds.

Software Design

In the design phase, considering details such as functionality, data structures, interfaces, algorithms, and tests, before actually writing the code, is deemed extremely valuable. Detailed design documents have proven very important when a system is extended and exported to other computer platforms several years after the original development team is finished and other personnel are involved. A carefully-designed database paves the way for easy future extensions.

The detailed design documents may form part of a Detailed Functional Description, a document handed over to the customer for final discussion and acceptance. This is the last chance to reveal any misinterpretations regarding the requirements. A paragraph in this document should highlight any deviations, restrictions, and assumptions made with respect to the requirements.

Efficient use of theorem proving in formal software development requires that the specification language is supported by a powerful theorem prover. For safety-critical applications, parts of such a tool should probably be developed using formal methods. Several of the design steps involved in a formal development process follow specific transformation rules, and can to some extent be automated.

Software Integration Testing

Integration testing should begin before all units are completed. Integration in a project of large complexity is liable to be the phase with highest risk in the development process, so the earlier it begins

the better. The easiest way of achieving this is to make use of a build strategy. This implies a number of demonstrable subsets of the final system that can form integration milestones for progress checking purposes.

Configuration Management is an important mechanism for identifying, controlling and tracking the versions of each software item. When a software unit is placed under Configuration Management, a version of the software unit has been tested and found to function according to specification. Then the unit is, in principle, complete, and integration with other software, changes to the functionality and error detection must be handled on a formal level, identifying causes and consequences to any change to the software.

The integration request procedure and the error/change proposal procedure used during Configuration Management and Change Control, are some of the most important procedures in the Software Quality Assurance Handbook utilized at the Halden Project.

Software System and Installation Testing

The Test Folder document is also considered as a major contribution to the planning, specification, design, and documentation of the various system tests. The same template can be used for all tests from integration to final acceptance. Involving the customer in specification of the Factory Acceptance Test (FAT) and Site Acceptance Test (SAT) has proven valuable. Verification of the total system with respect to time responses during high load conditions should be documented. Modifications done to the system during the time between the validation and installation must be verified in a formal way. A system for QA by means of change control requests should be followed including appointment of a system and a QA responsible.

Project Management and Quality Assurance

Project management is also a key to success. Even though the rational, analytical aspects of project management are a necessity to reach the overall goal of delivering the right product, at the right time and the right cost, the "human" aspects are the most important factors. There is no analytical short-cut to good project management, and the ultimate goal of a successful project lies very much in the hands of the project manager.

At the very beginning of the project a kick-off meeting or seminar is arranged. In this meeting the project specification, breakdown structure, organization, plans, quality assurance, etc. are presented. A good idea is an open discussion and exchange of experience to get acceptance for the working procedures to be followed in the project. Regular meetings are necessary to highlight any problems and the project's progress to the project participants. One should not forget to allocate time to the meeting activities during the planning phase.

The extent of a project's quality assurance system has to be adjusted to each specific application. The Unit Development Folders (UDF) and Test Folders (TF) are the most important procedures concerning documentation, progress, and quality assurance of software development projects and are mandatory in all such projects at Halden.

Software Development Tools

In recent years the trend has been to utilize higher-level development tools to implement software systems. High-level tools close the gap between the design and the programming, and guide the developer in generating a software system true to the design. The major advantage of using high-level development tools is that the developer does not have to worry about technical programming solutions, thus the possibilities for introducing programming errors in the program code are limited.
Another benefit from using such tools is that the implementation effort is reduced. However, this type of high-level programming requires a reliable development tool, tested and proven by experience.
Case tools offer a variety of facilities. Automatic generation of forms and reports, among others, enables prototyping and testing of functionality in cooperation with the customer at an early stage.

However, one should remember that case tools are extensive systems requiring methodical coursing and expert consultancy in the initial stages.

Proprietary Software

With respect to proprietary software for safety related systems the general impression from information received from companies producing software in the Instrumentation and Control area is that they follow a software development practice of high quality standard. An argument for the use of commercial proprietary software in safety-related applications is that the wide user experience grants high reliability. This requires data both on failures and on applications. However, even if the companies
are willing to reveal such information, and state that the documentation is available, this does not guarantee that the needed information exists. This is particularly true for data needed when applying quantitative reliability models. Such models require quite detailed information on failure statistics and operation data, whereas the available data is often only correction reports and version documentation.
In order to apply quantitative reliability models to systems based on proprietary software, it will be necessary to develop models that take into account the type of information one can obtain on such systems.

Lessons Learned on Software Dependability

This lessons learned report provides a number of specific as well as general conclusions and recommendations based on a review of different projects. It classifies the different projects into a framework that is oriented towards the software life cycle. Some aspects do not, however, belong to any particular life cycle phase, either because they are relevant in all phases, or because they are special. The following summarizes a number of the conclusions or lessons learned drawn in this report.

Specification

Specification is the phase in the software life cycle in which the identification of a need, and an idea to satisfy that need by a computer system is transferred into a document that serves as a basis for the further development and verification of such a system. The specification is the basis for the further development and verification of a software system. Deficiencies in the specification are often a source of faults in the final system. These are also the faults that are most difficult to detect during the V&V process.

A prerequisite for the development of a safe and reliable software system is therefore a good specification, that should be correct, unambiguous, complete, consistent, verifiable, modifiable, and traceable. A good specification system (i.e. a specification language and associated tools) should support these attributes.

The operational requirements and the plant knowledge utilized in the design of a control and supervision system should be an integral part of the design documentation of such a system. Modern information technology provides techniques - automated logic reasoning is one of them - that can be utilized in the development of such systems and in tools supporting their design.
Algebraic specification can be used as a common basis for several different approaches to qualitative reasoning about physical systems and the HRP prover can be used to support this reasoning.

The specification phase can conceptually be divided into two sub phases, viz. requirement specification and manufacturer's specification. Both phases are equally important in terms of the life cycle of the software, though each is susceptible to different types of errors.

Design and Coding

The software system should be designed according to the principles of structured design, independent of which designed language is used. This simplifies the further coding, in particular assembly coding. It is preferable to avoid

faults in the first place by using better development methods, languages and automated means of transferring information such as system constants into the program code.

A design tool will ease the design phase and facilitate the design verification. Direct code generation could be useful, but that has not been investigated in any of the HRP projects. Design and code inspection is very effective at discovering typical design and coding errors, such as logical errors, counting errors, assembly code errors, clerical errors etc.

Verification and Validation.
A well structured specification is a necessary basis for the verification of the program. All single requirements, functional as well as others, should be traceable to the final program system.

Static analysis, the verification of a program by inspection of relevant documentation, may be done either manually or with the help of tools. Different static analysis methods have been investigated with respect to their ability to detect faults. None of them, neither separately nor collectively, detected all the faults that were later found by back-to-back testing. The static analysis method does thus not seem not to be sufficient to detect all faults, in particular not the most hidden ones.

Analysis and verification tools are helpful and are reliable and thorough. However, they are designed to assist, not replace, a human to validate software. Manual inspection can still reveal errors (e.g., errors in specification and errors of transcription of system constants) that current tools cannot detect.

Manual inspection coupled with simple control and data analysis was able to detect a high proportion of faults with less effort than the more advanced verification tools. It might well be more efficient to apply such simpler but less thorough verification checks to detect and repair the most obvious faults before attempting a more rigorous verification.

Testing
Testing means to execute the program with a number of test data to get a confidence that it performs correctly. A number of difficulties may be encountered in structuring a software test. A major problem with testing is to produce an 'oracle', i.e. a procedure to state whether the result of a program execution is correct. Since a balanced data set should check legal and illegal conditions, it is an enormous and completely impractical task to make an exhaustive set of acceptance test data with manually pre-calculated results. An error in the pre-calculation may also induce a fault in the program, if it is adjusted to fit to the acceptance test.

A diversely produced program based on the same specification as the real program is a sensible choice as an 'oracle' that can be used to check the correctness of the output from the program execution. One should, however, in this case consider the possibility of common mode errors. Back-to-back testing of diverse program is a very effective method to reveal program faults. All known real and seeded faults were found in this way in our experimental investigations.

Back-to-back testing with computer generated random input data is also a very inexpensive testing method, and can therefore be applied to a large amount of test data. This is a way to obtain high confidence in a program. Process simulation data was found to be less effective to reveal programming errors. However, process simulation tests can be good for a validation of the specification. The method of 'Stored Tested Paths' could be useful during testing, to measure the effectiveness of the set of test data.

Safety defenses
To prevent serious consequences or abnormal behavior of the system, one can design certain safety measures into the system. These measures can roughly be classified in two main types: Fault tolerance and safety checks. Fault tolerance provide correct functional operation (or at least the essential part of it), even in the presence of one or more

faults in the target system. This is particularly addressed in our research on software diversity. Safety checks and actions can be designed into the target system to detect failures or abnormal behavior that may threaten safety, and initiate safety defenses.

Software Diversity

Software diversity (N-version programming) means an independent development by separate teams of programs based on the same specification.

From the results of the PODS/STEM project one can conclude that software diversity:

- gives very good protection against non-common mode faults in the program.
- detects program discrepancies in all known cases
- provides no significant correction for common faults
- most common mode faults come from the specification, not the programming technique.

The use of software diversity can clearly reduce the number of failures, and is thereby an effective way to obtain high reliability. The method is more expensive than a single development, but this should be weighed against the possibility of finding obscure residual faults. A very high confidence in a computer program is necessary before it can be used in safety critical applications.

On-line Checks

The 'Stored Tested Paths' method was investigated in the SAP project. This method is technically simple to implement and use. The selection of test data to generate a base of tested paths, as well as the modularization of the program, must be made with great care if the method shall be useful for on-line checking. The main problem is that correctly executed paths may not be in the tested path base, and that a spurious action will be made.

The method is not able to trap all types of faults during on-line checking, only the "path dependent" ones. But it is, anyhow, useful to be able to trap this type of faults as an additional safety check.

Tools

Generally available (on commercial basis or free of cost) tools were used and investigated in several of the projects. A general experience with many of these tools is that they do not do what one expect them to do, that they do not solve the problems one have. One should take into account, however, that many of the observations were made some time ago, and that there is a fast development, and probably improvement, of supporting tools. Hence, no conclusions have been drawn concerning any particular tool, but rather where tools may best be applied, and the properties they should have.

To obtain the maximum benefit from advanced tools, they should be applied during software development (when verification problems can be detected and corrected) rather than retrospectively.. Formal specification languages have an advantage over informal ones, that they are supported by means for mechanical analysis and manipulation. There are, however, at the time being only a few tools for formal methods that are adequate for development of safety critical or safety related software.

Computer assisted specification is helpful to ensure that the software specification is internally complete and consistent. Extension of the tools into programming and verification tools is also desirable. A specification tool should be a guide through the specification process. It should be easy to use by the one making the specification, and a good user interface is therefore essential. Graphic displays, windows systems, easy text editing etc. are properties that will improve a user interface.

A tool should perform internal checking, like syntax-, completeness- and consistency checks. The tool should also detect typographical errors in system constants, for example by reporting outliers to patterns. The tool should produce good, and currently updated documentation. Later modifications of the documents for any phases in the software development should be facilitated with an automatic checking and updating of all other relevant documents.

Lessons Learned on Test and Evaluation of Human-Machine Systems: Methods and Measures

The design and implementation of new information and control systems for nuclear power plant control rooms include test or evaluation at various stages. The test and evaluation is a vital element of system design and should be conducted to ensure that the system meets the design requirements for acceptance and usability. A number of different methods for testing and evaluating new systems have been employed at the OECD Halden Reactor Project. These may be categorized as being either guideline evaluations, user tests, model-based evaluations, or simulator study. Each of these techniques have different strengths as well as limitations. These have to do with:

- realism and control of the technique(s);
- cost and design stage of implementation;
- requirements for the number and qualifications of test subjects;
- experimental environment;
- types of performance measures that may be assessed.

In tests and evaluations, there are inevitably a number of factors that lead to the choice of the type of test that is employed. These include: the need to use persons who are, to varying degrees, representative of the eventual end user group; construction or use of a test environment similar to the implementation environment; the types of performance measures desired; the need to observe usage of the system under conditions representative of possible operating situations, etc. These issues affect the degree of realism and control employed in a test and evaluation (T&E). These two issues represent goals that are, somewhat, at odds with one another. To achieve greater realism, some control in the test environment must often be sacrificed and vice versa. Both are desirable. Greater realism in the test situation enables those conducting the study to draw conclusions from the T&E that may be generalized to the work environment. On the other hand, these conclusions may need to be tempered by the fact that some factors in the test environment were not controlled, and may have contributed in different ways to the final results. Previous training or exposure to test scenarios, order and practice effects, standardization of role play and exchanges between simulator instructors and participants, among other things, may contribute to differences in performance measures. Such differences are undesirable, especially when they influence the conclusions drawn from the study in a way that confounds a more straight forward use or interpretation of the results. In such cases, greater realism may actually work against the validity of the results obtained from a T&E.

The different T&E methods each place different material requirements on the test environment. These requirements concern both the test facility itself and costs to carry out the evaluation. Guideline evaluations, for example, cover a broad spectrum of interface design issues and can be tailored to emphasize specific issues. The cost of guideline evaluations are mostly the time invested by the person(s) conducting the review. Similarly, model-based evaluations are easy to employ and do not require very much in the way of hardware or software systems to be used. However, both guideline and model-based evaluations tend to be input-limited in the quality of results they produce. A guideline evaluation depends on the quality of the guidelines used, may be affected by subjective factors, and tends not to deal with higher-level issues (e.g., function allocation, design specification, etc.). Similarly, the success of model-based evaluations depend very much on the model employed. This, in turn, is affected by the skill of the modeler in determining the correct level of detail to employ, assumptions made about users, the system, etc.

User tests and simulator studies tend to be less input-limited but place greater demands on physical systems. They also involve greater costs in terms of preparation, execution, and analysis. User tests may range from a structured interview with end users to part-task simulations using the candidate system. There is not as much emphasis placed

on full scale capabilities of the system. Hence, user tests can be used at various stages of system development, from initial mock-up to final design. Simulator-based studies, as discussed earlier, provide a high degree of realism to a T&E. A T&E of a candidate system could be conducted in a simulator of the work environment in principle at any stage. However, most full scope simulator-based studies are used to evaluate operator and system performance in as realistic a manner as possible. The costs in preparing test materials, such as scenarios, instructions, performance measurements, etc., in simulator-base settings are nearly always higher than for other types of evaluation techniques. Hence, simulator-based studies are often reserved for final or nearly final T&E of a system.

Different T&E methods also place different requirements on the types of participants that may be used. Some may place little or no requirements at all on the use of participants. For example, guideline evaluations may be conducted to a large extent by only one person. In practice, however, the resolution of issues and evaluation of some design-related questions may require involvement by one or members of the end user group. Model-based evaluations, especially task-based models require that subject matter expertise be made available. This is necessary to produce a model of the task domain, tasks structures, dependencies between tasks, persons, etc., and to obtain time estimates for actions. User tests and simulator studies place even greater emphasis on participant qualifications than other methods. In general, as the realism of a T&E increases, so do the demands for participants having backgrounds and qualifications more representative of the user group. Since the availability of Operations personnel who can meet these higher requirements is limited, this also limits the ability to carry out many such studies in practice. It often also results in the need for greater planning in the preparation for such studies, since they are typically an all-or-none activity: problems previously undiscovered prior to the actual data collection with Operations personnel greatly limit the utility of the T&E.

The experimental environment needed to carry out the different T&E methods varies considerably. The analytical methods – guideline evaluations and modeling do not place great demands on the experimental environment. Guidelines can be applied at various stages of completion, and be used to evaluate different issues. To perform an evaluation that integrates all system issues, however, requires a system that is near completion and representative of the final system and be in the intended work environment. Similarly, modeling techniques often require little in the way of actual I&C systems or work settings. Though, to develop the basic model(s) upon which subsequent analyses are based may require very detailed information and access to subject matter expertise.

User tests and simulator studies place increasingly greater demands on the experimental environment, both in terms of those in which they are carried out, and conditions that may be represented in the T&E. To produce user-system interactions that are representative of the system in a final stage of implementation requires that the test environment resemble the usage or work environment. It also requires that situations be created that allow observations and data collection on user performance. The conditions under which data are collected should be representative of a range of conditions in which the system will be used (i.e., normal, accident, post-accident, etc.).

The type of results that are needed from the T&E will, to a large extent, determine which of the different methods can best meet these needs. If a test and evaluation must be performed to determine whether the system conforms to established knowledge and guidance about human factors design, then a guideline evaluation may be appropriate. If at an early to intermediate state of system completion designers desire feedback from end users about usage and display options considered, then user tests may be employed. Full scale simulation studies are typically used when actual performance, and performance measures with the system under the most realistic conditions possible are needed.

Each of the T&E methods are capable of producing different results. The question of which method is the best or right one will nearly always be answered "It depends." The types of results required, costs to carry out the T&E, demands placed on test conditions and participants all influence the decision about which method is the best for the stated need. In practice, all methods provide different, complementary information. Much of the lessons learned about system test and evaluation point out that a combination of techniques, at various design stages, are preferable to any single method by itself. Usability and acceptance represent a variety of issues to designers and system end users alike. Since no single T&E method can provide all the information about these issues, the needs from system

T&E should first be defined and prioritized. It is important that both the system designers and end users agree on these needs. Once such agreement is achieved, then a plan including the methods that can best achieve these needs can be specified and carried out.

Lessons Learned from the Design and Evaluation of Human-Machine Systems

A number of tests and evaluations of new technology have been conducted to understand their influence on operator performance. A lessons learned report was written that describes and summarizes the lessons that have been learned from these tests and evaluations related to the design of and approach to the evaluation of these new technologies. The intent in conducting this lessons learned study was to provide information relevant to understanding human-machine systems that, together with other research, can serve as technical bases in the formulation of guidelines for design and evaluation of human-machine systems.

A secondary purpose in conducting this study was to learn from previous studies about the effectiveness of different computer-based systems for supporting operator performance, and the factors that influence effective system design and implementation. This information can serves as feedback from the previous studies about effective system design, and tradeoffs. It can be used in the design of current and future computer-based support systems. The findings from future studies that apply the lessons learned in this report can serve, then, to evaluate the utility of these lessons learned.

The test and evaluations conducted at Halden have been done to evaluate many new technologies in order to provide information about performance issues associated with such new systems. Many support systems have been evaluated, albeit with many different aims. One theme, however, runs through all of these reports: does the new system support the operator? Experiments, user tests, guideline evaluations, model-based evaluations, surveys, etc., have been employed to obtain information and feedback about the design of these computerized operator support systems. The lessons learned from the review of these studies can be summarized in the following ways:

- New technologies for supporting operator performance can greatly facilitate the task of the operator subject to a number of considerations that must be addressed in the design of the new system. These include ensuring that the technology:
  - supports the right tasks;
  - provides the right information for the task;
  - fits well with the existing information coding schemes in the control room;
  - does not result in excessive task demands in order to be used;
  - does not excessively increase the amount of information to be attended to;
  - is designed for the right user, and;
  - supports the continuity of operator activities.

- Care must be taken in the implementation of the system to ensure use and acceptance by the operator. These include:
  - establishing the correct expectation about the system with the operators prior to use;
  - obtaining design input from operators to ensure that the system supports their tasks the best way;
  - ensuring that operators trust the system enough to use it and understand its capabilities as well as limitations;
  - ensuring that operators are trained to use the system to a level where

- they can conduct operations using the system and achieve at least the
- same level of performance as they had without it (or as necessary), and;
- ensuring that the system can be used in the manner intended and does not produce undesired performance.

The individual test and evaluations provide illustrations of each of these lessons learned. In addition, they demonstrate the value of test and evaluation as part of the design of new human-machine systems, as part of the validation or proof-of-principle testing of a new product for the control room. Perhaps most importantly, the lessons learned can serve to temper our expectations for advanced technology and provide insights into some of the mechanisms that prove useful for supporting operator performance, and some of the conditions they are subject to. In the final analysis of the test of a new system, they show that it is operator performance, coupled with the system itself that provides either vindication or reproof of new system design. Taking this into account, it underscores the need for adequate human-system evaluations in order to establish the viability and utility of system design.

References

Follesø, K., & Volden, F.S. Lessons learned on test and evaluation methods from test and evaluation activities performed at the OECD Halden Reactor Project. HWR-336, September 1993.

Hallbert, B.P., & Meyer, P. Summary of Lessons Learned at the OECD Halden Reactor Project for the Design and Evaluation of Human-Machine Systems. HWR-376, September, 1995.

Dahll, G., & Sivertsen, T. A lessons learned report on software dependability. Part I: Survey and Conclusions and Recommendations. HWR-374, June 1994.

Dahll, G., & Sivertsen, T. A lessons learned report on software dependability. Part II: Technical basis. HWR-375, June 1994

Bjørlo, T.J., Berg, Ø., Pehrsen, M., Dahll, G., & Sivertsen, T. Lessons learned from experience with development and quality assurance of software systems at the Halden project. HWR-418, August 1995.

New Geological Perspectives on Earthquake Recurrence Models

David. P. Schwartz
U.S. Geological Survey, Earthquake Geology and Geophysics, Section Menlo Park, CA, USA

In most areas of the world the record of historical seismicity is too short or uncertain to accurately characterize the future distribution of earthquakes of different sizes in time and space. Most faults have not ruptured once, let alone repeatedly. Ultimately, the ability to correctly forecast the magnitude, location, and probability of future earthquakes depends on how well we can quantify the past behavior of earthquake sources. Paleoseismological trenching of active faults, historical surface ruptures, liquefaction features, and shaking-induced ground deformation structures provides fundamental information on the past behavior of earthquake sources. These studies quantify a) the timing of individual past earthquakes and fault slip rates, which lead to estimates of recurrence intervals and the development of recurrence models and b) the amount of displacement during individual events, which allows estimates of the sizes of past earthquakes on a fault. When timing and slip per event are combined with information on fault zone geometry and structure, models that define individual rupture segments can be developed. Paleoseismicity data, in the form of timing and size of past events, provide a window into the driving mechanism of the earthquake engine--the cycle of stress build-up and release.

A major concept derived from geological data is the characteristic earthquake model. This has implications for earthquake magnitude estimates and the frequency of different size earthquakes on individual faults. The characteristic earthquake model states that most of the seismic moment released by individual faults and fault segments occurs as successive earthquakes of essentially the same, or "characteristic", size and that these are at or near the maximum magnitude that can be produced by the geometry, mechanical properties, and state of stress of that fault or segment. This general observation was noted at about the same time by several workers using different data sets. Schwartz et al. (1982) and Schwartz and Coppersmith (1984) conceived the model using data on displacement per event from paleoseismic studies along the Wasatch and San Andreas faults. These data showed that at a point on a fault the amount of displacement during successive surface faulting earthquakes remains essentially constant. A major implication of this conclusion is that earthquake recurrence on an individual fault does not conform to an exponential (constant b-value) model. Wesnousky et al. (1983, 1984) compared recurrence based on geologic slip rates of Quaternary faults and the 400-year-long historical earthquake record in Japan and concluded that the data are best fit with a maximum moment model, a variation of the characteristic earthquake model in which recurrence is expressed as the recurrence of only the maximum-size event. Recently Wesnousky (1994) and Stirling et al. (1996) have used more

robust updated seismicity data sets to compare to geological estimates of recurrence on major strike-slip faults in California and other parts of the world. They conclude that most of these faults express characteristic, as opposed to exponential, recurrence behavior.

Since 1984 a significant amount of new historical and paleoseismic information on slip per event has been generated worldwide. This includes data from surface fault ruptures associated with the 1957 Gobi-Altay, 1980 Irpinia, 1983 Borah Peak, 1987 Superstition Hills, and 1992 Landers earthquakes as well as from many faults that have not produced historical events. This information is currently being reviewed to produce a worldwide slip-per-event database. To date, information has been compiled on slip per event for forty faults, representing all major fault types and a variety of tectonic settings worldwide. Two-thirds of these faults appear to demonstrate characteristic earthquake behavior. That is, the amount of slip during successive surface faulting earthquakes is very similar, as expressed by a low coefficient of variation 3. The analysis includes consideration of measurement uncertainty, problems with event recognition, and the quality and quantity of observations. The degree to which factors such as tectonic environment and length of the earthquake cycle control similarities or differences in the amount of slip during successive events on a fault is also being evaluated. It is clear that the characteristic earthquake model describes a fundamental type of fault behavior, particularly for large events in continental crust, although it is by no means inclusive.

Characteristic earthquakes are intimately related to fault segmentation, which is emerging as a field of earthquake research with important implications for increasing our understanding of the mechanics of faulting and for evaluating seismic hazard. The concept of fault segmentation is based on the common observation that fault zones, especially long ones, do not rupture their entire length during a single earthquake. As noted, where the amount of surface slip during successive events can be compared at the same location, it is frequently observed that this amount has remained essentially constant. It follows that the slip distribution along the fault, and by inference the rupture length, has also remained essentially constant. This argument, augmented with the results of structural and paleoseismicity studies, implies that the location of rupture is not random, that there are physical controls in a fault zone that define the extent of rupture and divide a fault into segments, and that rupture segments can persist through many seismic cycles. If a fault-specific segmentation model can be well-constrained, ideally by combining both paleoseismic timing data and geometric/structural observations, the specific location and length of future ruptures can be ascertained. In fact, fault segmentation provides the framework for time-dependent probabilistic earthquake forecasts. Dip-slip faults, where adjacent segments can be structurally decoupled, appear to be generally well-segmented. Segmentation modeling of long multi-segmented strike-slip faults that have master segments (1906 San Andreas) containing shorter segments that also produce their own earthquakes (1838 Peninsula San Andreas) is more complex. The degree to which fault segments persist as independent rupture segments over long periods of time is a major source of uncertainty and disagreement in segmentation modeling and hazard analysis.

The major parameter that distinguishes a probabilistic from a deterministic hazard analysis is time. The characteristic earthquake model is often used synonymously with uniform or quasi-periodic earthquake recurrence. This is a major misconception. The term characteristic refers only to the successive repeat of similar displacement events and not to the amount of time between them. Indeed, dating of paleoearthquakes has defined a spectrum of recurrence behavior, from relatively uniform to highly variable. High slip rate master segments of major plate-boundary faults, where repeat times of large events are measured in hundreds of years, tend to exhibit quasi-periodic behavior (a coefficient of variation of about .25 to .45 reflecting uncertainties in field measurements and dating as well as the effects of fault interactions). These are exemplified by segments of the San Andreas, Elsinore, and San Jacinto faults where radiocarbon dated intervals between successive events are similar to calculated average recurrence using independently derived slip per event observations and late Holocene slip rates. Faults off of these main structures or faults in intraplate or stable continental regions commonly have repeat times measured in thousands (or even tens of thousands) of years and often have recurrence intervals that are highly variable or clustered, even while the repeated size of events is the same. Clustering itself can take many forms including: a) the complete rupture of long, multi-segmented faulted zones in a few decades (North Anatolia, 1939-1968) or several hundred years (Wasatch, between about 300 and 1200 yr BP): b) long periods of quiescence (many tens of thousands of years) followed by an active cycle with inter-event times of a few thousand years (Lost River fault zone); c) closely timed repeated slip on low displacement segments of large ruptures (northern Imperial fault-1940, 1979); and d) closely timed events on a set of regional faults (Landers rupture segments and associated faults in the western Mojave at about 6-9 ka and again between about 1.5 ka and the present; western Mongolia where three M8 events occurred this century on three faults, each having individual repeat times of 5-10 ka).

There is also growing recognition that faults communicate with each other. That is, the stress changes produced by an earthquake on one can strongly affect the behavior of neighboring faults. This introduces variability into recurrence on individual faults and across regions. For example, calculations show the 1906 earthquake was so large that it effectively relaxed the stress on most of the major faults in the San Francisco Bay area and resulted in the formation of a regional "stress shadow". This was expressed by the relatively infrequent occurrence of moderate to large earthquakes in the Bay Area this century. In the 75 years between 1836 and 1911 the Bay Area sustained sixteen earthquakes of ~M6-7.8, four of which were ~M7 or larger. This was followed by a 68 year period (1911-1979) during which the largest events were four middle M5s, and by the most recent interval (1979 to present) with four events of ~M 6 to M7. There is no question that on a long term average (many hundreds to thousands of years), which geologic slip rates reflect, seismic moment is conserved, but in the short term its release can be variable.

Clearly, there is no unique form of fault behavior and no single recurrence model that can be used to estimate earthquake probabilities on a fault or for a region. Rather, there is a range--from the apparently random to the apparently repeatable. This presents a major challenge to earth scientists and modelers of earthquake probabilities.

Revised Seismic and Geologic Siting Regulations for Nuclear Power Plants

Andrew J. Murphy and Nilesh C. Chokshi
Office of Nuclear Regulatory Research, U.S.NRC

Background

The primary regulatory basis governing the seismic design of nuclear power plants is contained in Appendix A to Part 50, General Design Criteria for Nuclear Power Plants, of Title 10 of the Code of Federal Regulations (CFR). General Design Criteria (GDC) 2 defines requirements for design bases for protection against natural phenomena. GDC 2 states the performance criterion that "Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, . . . without loss of capability to perform their safety functions. . .".

Appendix A to Part 100, Seismic and Geologic Siting Criteria for Nuclear Power Plants, has been the principal document which provided detailed criteria to evaluate the suitability of proposed sites and suitability of the plant design basis established in consideration of the seismic and geologic characteristics of the proposed sites. Appendix A defines two earthquake levels, the Safe Shutdown Earthquake (SSE) and the Operating Basis Earthquake (OBE). The SSE is that earthquake which is based upon an evaluation of the maximum earthquake potential considering the regional and local geology and seismology and specific characteristics of local subsurface material. It is that earthquake which produces the maximum vibratory ground motion for which certain structures, systems, and components are designed to remain functional. The OBE, in part, is defined as that earthquake which produces the vibratory ground motion for which those features of the nuclear power plant necessary for continued operation without undue risk to the health and safety of the public are designed to remain functional. Appendix A also defines required seismological and geological investigations and requirements for other design conditions such as soil stability, slope stability, and seismically induced floods and water waves, and requirements for seismic instrumentation. As will be discussed further later, the NRC staff is in the process of revising Appendix A.

The NRC has recently revised seismic siting and design regulations for future applications. These revisions are discussed in the next section in detail.

Revision of Seismic Siting and Engineering Criteria

The NRC's revised seismic siting and engineering regulations have been published in the Federal Register Notice issued on December 11,1996 with the effective date of regulation January 10, 1997.

The more significant changes are highlighted below.

Seismological Aspects

The approach for determining a SSE[1] for currently operating reactors in US, embodied in Appendix A to 10 CFR Part 100, relies on a "deterministic" approach. Using this deterministic approach, an applicant develops a set of earthquake sources, develops for each source a postulated earthquake to be used as the source of ground motion that can affect the site, locates the postulated earthquake according to prescribed rules, and then calculates ground motions at the site.

Although this approach has worked reasonably well for the past two decades, in the sense that SSEs for plants sited with this approach are judged to be suitably conservative, the approach has not explicitly recognized uncertainties in geosciences parameters. Because so little is known about earthquake phenomena (especially in the eastern United States), there have often been differences of opinion and differing interpretations among experts as to the largest earthquakes to be considered and ground-motion models to be used, thus often making the licensing process very contentious and relatively unstable.

Over the past decade, analysis methods for incorporating different interpretations have been developed and used. These "probabilistic" methods have been designed to allow explicit incorporation of different models for zonation, earthquake size, ground motion, and other parameters. The advantage of using these probabilistic methods is their ability to not only incorporate different models and different data sets, but also to weight them using judgments as to the validity of the different models and data sets. Thereby they provide an explicit expression for the uncertainty in the ground motion estimates and a means of assessing the sensitivity of the ground motion estimates to various input parameters. Another advantage of the probabilistic method is that an uniform annual probability of exceeding the design basis can be maintained from site to site.

---

[1]In the new regulation, the acronym, SSE, is made more specific, i.e., Safe Shutdown Earthquake Ground Motion rather than the old Safe Shutdown Earthquake.

The revised regulation (for the future application only) explicitly recognizes that there are inherent uncertainties in establishing the seismic and geologic design parameters and allows for the option of using a probabilistic seismic hazard methodology capable of propagating uncertainties as a means of satisfying the requirement to address these uncertainties. The rule further recognizes that the nature of uncertainty and the appropriate approach to account for it depend greatly on the tectonic regime and parameters, such as, the knowledge of seismic sources, the existence of historical and recorded data, and the understanding of tectonics. Therefore, methods other than the probabilistic methods, such as sensitivity analyses, may be adequate for some sites to account for uncertainties. The scope and depth of site investigation has been maintained as before.

A detailed approach to implement the rule is described in a regulatory guide which will be published in March 1997. This guide makes use of the probabilistic seismic hazard analysis, and the key elements of the approach are:

- Conduct site-specific and regional geoscience investigations,
- Establish reference annual exceedance probability
- Conduct probabilistic seismic hazard analysis and determine ground motion level corresponding to the reference annual exceedance probability
- Determine site-specific spectral shape and scale this shape to the ground motion level determined above,

One of the key and necessary elements in implementing any probabilistic method is the establishment of a probabilistic target or criterion. In this case, the target or criterion is defined by a reference annual probability of exceeding design basis as noted above. In the guide, the NRC staff has established this reference value as a median of the annual probability of exceeding design bases of more recently licensed nuclear power plants. The rationale for this approach stems from the Severe Accident Policy Statement which implies that the current generation plants are adequately safe.

Although, this is not strictly a risk-based regulation (even though the implementation of the proposed approach will result into maintaining uniform probability of exceeding design basis from site to site, the seismic risk profile depends on the complete hazard curve and plant fragilities), it is a good example of a regulation explicitly addressing questions of uncertainties, and explicitly setting a probabilistic criterion. This is a first step in implementing performance based seismic design process.

Earthquake Engineering Aspects

The revision has also made a significant change with respect to the OBE. The Appendix A states that the maximum vibratory ground motion of the OBE is at least one half the maximum vibratory ground motion of the Safe Shutdown Earthquake ground motion. The appendix further states that the engineering method used to insure that structures, systems, and components are capable of withstanding the effects of the OBE shall involve the use of either a suitable dynamic analysis or a suitable qualification test. In some cases, for instance piping, these multi-facets of the OBE in the existing regulation made it possible for the OBE to have more design significance than the SSE. A decoupling of the OBE and SSE has been suggested and discussed over many years. It has been suggested that design for a single limiting event (the SSE) and inspection and evaluation for earthquakes in excess of some specified limit (the OBE), when and if they occur, may be the most sound regulatory approach.

The revised regulation allows the value of the OBE to be set at (I) one-third or less of the SSE, where OBE requirements are satisfied without an explicit response or design analyses being performed, or (ii) a value greater than one-third of the SSE, where analysis and design are required. There are two issues the applicant should consider in selecting the value of the OBE: first, plant shutdown is required if vibratory ground motion exceeding that of the OBE occurs, and second, the amount of analyses associated with the OBE. Thus, the proposed change with respect to the OBE will remove excessive conservatism and result in a reduced burden to future applicants.

DEPARTMENT OF ENERGY SEISMIC SITING AND DESIGN DECISIONS: CONSISTENT USE OF PROBABILISTIC SEISMIC HAZARD ANALYSIS

Jeffrey K. Kimball, DOE, Defense Programs
Harish Chander, DOE, Environment Safety & Health

The Department of Energy (DOE) requires that all nuclear or non-nuclear facilities shall be designed, constructed and operated so that the public, the workers, and the environment are protected from the adverse impacts of Natural Phenomena Hazards including earthquakes. The design and evaluation of DOE facilities to accommodate earthquakes shall be based on an assessment of the likelihood of future earthquakes occurrences commensurate with a graded approach which depends on the potential risk posed by the DOE facility. DOE has developed Standards for site characterization and hazards assessments to ensure that a consistent use of probabilistic seismic hazard is implemented at each DOE site. The criteria included in the DOE Standards are described, and compared to those criteria being promoted by the staff of the Nuclear Regulatory Commission (NRC) for commercial nuclear reactors.

In addition to a general description of the DOE requirements and criteria, the most recent probabilistic seismic hazard results for a number of DOE sites are presented. Based on the work completed to develop the probabilistic seismic hazard results, a summary of important application issues are described with recommendations for future improvements in the development and use of probabilistic seismic hazard criteria for design of DOE facilities.

INTRODUCTION:

DOE regulates itself and its contractors in matters relating to environmental, safety, and health protection through a hierarchy of documents, ranked in order of precedence as follows: policy, requirements (rules or DOE Orders), and guidance documents (either safety guides or standards). With respect to natural phenomena, specifically seismic hazards, it is the policy of DOE to design, construct, and operate DOE facilities so that workers, the general public, and the environment are protected from the impacts of natural phenomena hazards (NPH) at DOE facilities.

A key element of DOE NPH mitigation requirements is the use of a graded approach. DOE facilities are quite diverse, and as such warrant a graded approach (e.g., some are office buildings while others contain substantial inventories of hazardous material). Such an approach recognizes the diversity of objectives for NPH protection, the diversity of facilities, and the diversity of measures that are appropriate to ensure suitable NPH protection. When properly developed and implemented, a graded approach optimizes the allocation of effort and resources.

Over the past ten years, DOE has been explicitly utilizing probabilistic concepts, including the probabilistic assessment of seismic hazard, to implement the graded approach. This concept is described in a series of DOE NPH Standards which are listed in the reference section. The cornerstone of the graded approach for NPH mitigation is the concept of Performance Categories, with corresponding target probabilistic performance goals. Each Performance Category is assigned a structural performance goal in terms of the probability of unacceptable damage due to natural phenomena. The target performance goals range from those included in model building code provisions for office buildings to those intended for commercial nuclear power plant seismic criteria.

A necessary part of implementing the NPH graded approach is the selection of one or more levels of seismic ground motion. Because of the random nature of earthquakes, selection of a design level of ground motion inherently has a probability of occurrence associated with it. DOE has developed requirements and acceptance criteria to assure that the assessment of seismic hazard and the quantification of probabilistic ground motion is implemented in a consistent fashion from site to site.

The following topics will be summarized: DOE requirements and acceptance criteria for Probabilistic Seismic Hazard Analysis (PSHA); summary of seismic hazard results at DOE sites and a comparison to NRC criteria; identification of important issues in application of PSHA; and recommendations for future improvement of PSHA.

DOE REQUIREMENTS AND ACCEPTANCE CRITERIA FOR PSHA:

DOE Order 420.1, "Facility Safety" (Dated 10-13-95), establishes facility safety requirements including requirements related to NPH mitigation, and specifically related to natural phenomena hazards assessments. These requirements specify that:

- The design and evaluation of facilities to withstand natural phenomena shall be based on an assessment of the likelihood of future natural phenomena occurrences. The natural phenomena hazards assessment shall be conducted commensurate with a graded approach and commensurate with the potential risk posed by the facility.

- For new sites; natural phenomena hazards assessment shall be conducted commensurate with a graded approach to the facility. Site planning shall consider the consequences of all types of natural phenomena hazards.

- For existing Sites; if there are significant changes in natural phenomena hazards assessment methodology or site-specific information, the natural phenomena hazards assessments shall be reviewed and shall be updated, as necessary. A review of the natural phenomena hazards assessment shall be conducted at least every 10 years. The review shall include recommendations to DOE on the need for updating the existing natural phenomena hazards assessments based on identification of any significant changes in methods or data.

Review of the above requirements demonstrates that DOE is interested in the assessment of probability (likelihood of occurrences), and that changes in methodology and data should be evaluated on a cyclic basis (at least every 10 years). DOE has developed two Standards that outline acceptance criteria to aid in compliance with the above requirements, with respect to assessment of seismic hazards. These standards provide guidance related to site characterization and the quantification of the probabilistic seismic hazard.

DOE Standard 1022-96 provides comprehensive guidance for investigation of the site for natural phenomena hazards, including earthquakes. Acceptance criteria include criteria for seismic sources and vibratory ground motion, the two key inputs for completing a PSHA study. The following guidance is provided for seismic sources:

- Identify all seismic sources which could contribute more than 5 percent to the seismic hazard. Perform detailed investigations within 8 kilometers (5 miles) of the site and other near-site and regional investigations to ensure an accurate PSHA estimate;

- Select the types of investigations to assure highly reliable information particularly those techniques to assess the likelihood of earthquake occurrence;

- Complete a detailed investigation of fault seismic sources to define: rates of movement; sense of slip; length and displacements of previous ruptures; fault dip and down dip width; fault segmentation; and assessment of surface versus blind (buried) faults;

- Assess the frequency of occurrence including the type of recurrence model; and

- Define the maximum magnitude for each source.

The following guidance is provided for vibratory ground motion:

- Define regional and site attenuation characteristics; and

- Define site response including the consideration for geotechnical studies to define soil in-situ and dynamic properties.

The overall intent of the above criteria is to provide reasonable assurance that site investigations are sufficiently well understood to permit an adequate evaluation of the proposed or existing site. It is expected that the site characterization data base will be evaluated at the same time as the review of probabilistic seismic hazard curves which is about every 10 years. DOE also requires that site characterization efforts follow an approved quality assurance program and that peer review be performed by independent qualified personnel with extensive knowledge and experience in the various aspects of site characterization.

DOE Standard 1023-96 provides acceptance criteria for conducting a PSHA to produce a seismic hazard curve to be used in selecting the Design Basis Earthquake (DBE) for DOE facilities. Additionally, DOE-STD-1023-96 discusses the shape of response spectra developed for earthquakes of the magnitudes and distances that represent the earthquakes which control the PSHA. The following guidance is provided for completing a PSHA:

- The PSHA must include characterization of uncertainty in all parameters of the seismic hazard model including seismic sources, earthquake recurrence rates, maximum magnitudes, and all aspects of ground motion attenuation;

- Future PSHA's must follow the guidance developed by the Senior Seismic Hazard Analysis Committee (SSHAC) which was a joint effort between DOE, the NRC, and the Electric Power Research Institute (EPRI).

The methods for developing and using PSHA for seismic design purposes has caused concern on the part of several experts. The two principal concerns are that (1) the methods are subject to considerable judgment and may be misused, and (2) there is a potential for the process to imply unwarranted certainty about the selected hazard and thereby lead to unrealistic confidence in the state of knowledge about the seismic hazard. Those experts who are critical of PSHA tend to be supportive of alternative methods such as prescriptive procedures for selection of the Design Earthquake.

DOE-STD-1023 has recognized these differences in approach and has included criteria to perform an independent check of the probabilistic DBE based on a set of prescriptive rules. The overall approach for developing the DBE is based on three specific assessments. For the most stringent Performance Category these assessments are as follows:

- Complete PSHA and calculate mean uniform hazard spectra (UHS) for a annual probability of .0001 (10000 year earthquake);

- Deaggregate the PSHA to determine the controlling earthquakes which dominate the hazard and based on the controlling earthquakes develop spectral shapes consistent with their magnitudes and distances. Compare the uniform hazard spectral shape to the shape developed from the controlling earthquakes and determine if the UHS is sufficiently broad to represent design spectra;

- Review the historic earthquake record and determine if the site is within 125 miles (200 kilometers) of a moment magnitude equal to or greater than 6, calculate the 84th percentile ground motion, and compare it to the UHS.

- The DBE is established based on the envelope of the UHS (or modified based on deaggregated results) and the historic earthquake.

Similar to completion of site characterization, the development of any PSHA must undergo a thorough peer review to assure that the methodology used to develop the PSHA accurately represents the necessary data and information, and assesses the uncertainty in a rigorous fashion. This issue is discussed in more detail in the section pertaining to the identification of important issues in application of PSHA.

DOE initiated an effort with the American National Standards Institute in late 1994 to establish national consensus standards applicable to nuclear materials facilities. A group of NPH design standards constitutes one of the major activities, and these have been assigned to the American Nuclear Society (ANS) who is coordinating joint standards with the American Society of Civil Engineers (ASCE). Four new standards are being developed. Three by the ANS and one by the ASCE. This group of standards is intended to be suitable for replacement of DOE Standards NPH 1020, 1021, 1022, and 1023. These new standards employ a graded approach to select NPH (earthquake, tornado/wind, and flood) hazards and design requirements for Nuclear Materials Facilities.

Several ANS standards working group meetings have been held and the ASCE has also initiated their effort by gaining approval of the assignment of the standards to the Dynamic Analysis of Nuclear Structures Committee. Some or all of the standards may be carried forward to become international standards.

SUMMARY OF SEISMIC HAZARD RESULTS AT DOE SITES:

Efforts to update the probabilistic seismic hazard at many DOE sites were undertaken within the past 5 years, primarily as a result of new information pertaining to the characterization of seismic sources and the overall emphasis on PSHA results in the Eastern United States (EUS) as a result of understanding the differences between the Lawrence Livermore National Laboratory (LLNL) results and EPRI results. The PSHA results for many DOE sites are compiled in Tables 1 and 2 for peak ground acceleration and 1 hertz spectral acceleration. Table 1 provides results for a number of EUS sites, while Table 2 provides results for a number of Western United States (WUS) Sites. The information contained in the Tables is also shown on Figures 1 through 4, which provide seismic hazard curves for the sites shown on the Tables.

The PSHA results for the EUS are generally based on the direct average of the latest LLNL results and the EPRI results. In the late 1980's DOE requested that LLNL examine their PSHA methodology and as a result of this revise their seismic hazard estimates. LLNL revised portions of the expert elicitation process related to estimating earthquake recurrence rates and associated uncertainty, and revised the vibratory ground motion model and its associated uncertainty. The overall impact of these changes were twofold: (1) to reduce the mean seismic hazard estimate, and (2) to reduce the overall uncertainty in the seismic hazard estimate. One important finding of this effort was that differences between the LLNL and EPRI results were dramatically reduced and in many cases the LLNL and EPRI results were found to be comparable.

Review of Tables 1 and 2, and Figures 1 through 4 demonstrates that the range in seismic hazard estimates at DOE sites is very large, reflecting the large variations in seismic hazard in the United States. At any given probability the range in ground motion can be a factor of 10 or greater. Table 1 also includes several estimates for rock and soil at DOE EUS sites. These results show that the local soil conditions can have a dramatic impact on the seismic hazard, and that this impact can be more significant at low or high frequencies primarily depending on the depth of the soil, and the contrast in shear wave velocity between the underlying rock and the soil. The impact of local soil conditions can overwhelm the basic seismic hazard results, which can result in a generally low hazard site having moderate to large ground motions because of local site response.

COMPARISON TO NRC CRITERIA:

As a result of these efforts DOE has taken the position that it is acceptable to directly average the two studies to arrive at a PSHA estimate for DOE sites. For the most hazardous facilities, DOE is selecting the DBE based on the mean seismic hazard estimate at an annual probability of .0001 (10000 year earthquake). This is somewhat different than proposed NRC criteria for new nuclear power plants which bases the selection of the Safe Shutdown Earthquake on the median seismic hazard at an annual probability of .00001 (100000 year earthquake). In actuality the two approaches are quite comparable in the EUS, the region that the NRC based their selection of the reference probability on. The use of a median probability of .00001 is about equal to the use of a mean probability of .0001.

DOE has chosen to use the mean estimate of seismic hazard for assigning reference probabilities for two reasons: (1) because the intent of the performance goal approach is to provide roughly equal levels of risk, using the surrogate of equal levels of damage, the mean is the most appropriate value to select if one wants to account for uncertainties while using a point probabilistic estimate, and (2) the difference between the median and the mean seismic hazard curves is not constant between the EUS and WUS. The second point results in the conclusion that the use of the proposed NRC criteria may cause difficulties in the WUS, primarily resulting in overconservative design values. NRC has recognized this and allows for the selection of an alternative reference probability in these cases. DOE has attempted to address this issue by using the mean estimate of seismic hazard.

IDENTIFICATION OF IMPORTANT ISSUES IN APPLICATION OF PSHA:

As discussed previously, the methods for developing and using a seismic hazard curve have caused concern on the part of several experts. Stated another way, does the user have enough confidence in the PSHA results to apply PSHA in the design process? In DOE's case, the answer to the above question is yes. DOE recognizes, however, that there are a number of important issues in the application of PSHA which should be addressed. These issues include:

- Methodology issues and the fact that there is no standard for completing a PSHA;

- o Is the PSHA UHS is adequate to use as a design basis spectrum? Is it sufficiently broad banded?

- o Are all users of PSHA working together to develop a common PSHA estimate?

To address the first issue DOE collaborated with the NRC and EPRI to develop "Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on Uncertainty and Use of Experts" (SSHAC Report). It has been DOE's experience that when comparing different PSHA estimates (such as LLNL and EPRI), the difference between the estimates are often not technical, but due to the information gathering and assembly process used in the study. Stated another way, the integration of the different types of information required in a PSHA presents significant inter-disciplinary challenges and requires a project structure and process that assures proper integration. The skills required to be a good integrator and evaluator (what is necessary to complete a PSHA), are not necessarily the same skills needed to be a good scientist.

One of the key components contained in the SSHAC Report is that proper peer review must be conducted to review the process and substance of the PSHA study. The report goes on to encourage the use of a participatory peer review, one where the peer reviewers are actively involved in reviewing the project throughout its implementation. DOE has mandated such an approach for all our seismic hazard studies in the past 5 years.

It is DOE's expectation that any future study completed for DOE will follow the guidance in the SSHAC report. Additionally, it is our view the SSHAC report should become the standard procedure and method for doing a PSHA no matter who the sponsor is, and no matter how the PSHA will be used.

Issues related to whether the UHS is directly adequate for a design basis spectrum have primarily resulted from the observation that the UHS is relatively narrow compared to design spectrum typically used of critical facility evaluations. In the EUS, the PSHA is typically controlled by earthquakes of magnitude 6 and lower. Review of strong motion data indicates that the shape of the response spectra is dependent on magnitude, and because the EUS PSHA results are controlled by relatively small magnitudes, the shape should be expected to be narrower compared to spectra such as the Newmark/Hall spectra.

Figures 5 through 7 were developed to provide one explanation of this observation. Figures 5 and 6 show the ratio of peak velocity (mid to low frequency portion of the response spectra) to peak acceleration (high frequency portion of the response spectra) for the strong motion data which were used by Newmark/Hall to develop their classic design spectra. Review of this data indicates that the ratio of velocity to acceleration is dependent on magnitude. Figure 7 shows the result of taking this information and deriving an alternative response spectrum for earthquakes less than magnitude 6, while at the same time recognizing that in the EUS the response spectrum peaks at frequencies above 10 hertz. The point of this exercise is to provide one explanation that

the UHS is consistent with our expectation that the shape of the response spectrum is dependent on magnitude.

NRC has recently initiated a study that will develop magnitude dependent spectral shapes for use as design spectra. This effort should provide the confidence in the use of the UHS for design, or alternatively how the UHS should be broadened for design but still consistent with the magnitude of the earthquake which controls the PSHA.

The final issue is whether all users are working together to develop consistent estimates of PSHA. While it is true that the LLNL and EPRI results are comparable, recent seismic hazard results produced by the United States Geological Survey (USGS), as part of the National Earthquake Hazards Reduction Program , suggest that large differences may still exist in estimates of probabilistic ground motion. The USGS estimates appear to be significantly larger than either LLNL or EPRI estimates for the low frequency portion of the response spectrum (such as 1 hertz).

Figure 8 displays six different ground motion attenuation models for 1 hertz spectral acceleration, at a moment magnitude of 6.5, that have been used in the LLNL, EPRI and USGS studies. The LLNL PSHA results are based on the LLNL composite model, the EPRI PSHA results were based on models similar to EPRI 1987 and the Boore/Atkinson 1990 model, while the USGS results are based on the EPRI 1993 and USGS 1996 models. Figure 8 shows that the ground motion models being used by the USGS are generally larger than other models which can be found in the published literature. Figure 8 suggest that we should not be surprised to find that the USGS PSHA results will be larger than either EPRI or LLNL.

While the above discussion is not intended to be directly critical of the USGS PSHA work, it does point out that there is not a consensus in estimates of PSHA, particularly in the EUS. From DOE's perspective, until a common methodology to completing PSHA's is followed, such as the approach recommended in the SSHAC report, PSHA estimates are likely to remain somewhat divergent.

RECOMMENDATIONS FOR FUTURE IMPROVEMENT OF PSHA:

While future PSHA studies can be improved in a number of ways, until PSHA practitioners follow a common methodology and procedure, PSHA sponsors and users should not expect consensus in results. Thus, it is DOE's view that the single most important improvement in future PSHA studies is related to developing a common method for completing, documenting, and peer reviewing PSHA results. This is particularly important given the large uncertainties which exist in all aspects of PSHA input for virtually all regions of the United States. By following a common procedure clarity will be improved of why certain assumptions were made and why others were eliminated. Review of Figure 8 should demonstrate that this type of improvement is still necessary.

If the PSHA community can follow a common procedure than a systematic review of existing PSHA work will reveal the specific technical issues that need more work. In the EUS these issues may include the definition of seismic sources (smoothed seismicity versus tectonic structures), the incorporation of paleoliquefaction information into the PSHA (earthquake recurrence and maximum magnitude), and the selection of appropriate ground motion attenuation models (see Figure 8). PSHA sponsors and users, such as the NRC, DOE and USGS, should work together to see that these issues are objectively addressed following a common procedure.

Finally, the implementation of PSHA results at any given site is strongly dependent on the local site conditions which can dramatically impact the seismic hazard. The modification of ground motion at soil sites can range from large amplifications at the site resonant frequency to de-amplification as a result of soil damping. Presently the direct incorporation of site response into the PSHA is completed crudely at best. Either generic soil categories are used, or the PSHA is completed assuming the site is rock, and the site response is assessed deterministically. If the site response is directly incorporated into the PSHA, the care must be taken to assure that uncertainties are not double counted, or that the actual site response is missed. Future improvements in how site response is incorporated into PSHA is necessary to improve PSHA accuracy at soil site.

SUMMARY:

The Department of Energy has established requirements and acceptance criteria for natural phenomena hazards assessments following a graded approach. Efforts are underway to develop concensus standards from the DOE Standard. Seismic hazard studies have been completed for many DOE sites over the past five years. DOE based the seismic design on the use of the mean annual probability of exceedance to assure that consistent definition of design earthquakes is implemented from site to site. Future PSHA studies can be strengthened if a common method and procedure is developed, one that can be followed by all PSHA practitioners.

REFERENCES:

U.S. Department of Energy, 1995, "Facility Safety," DOE Order 420.1, Washington, D.C.

U.S. Department of Energy, 1995, "Draft Interim Guidelines for the Mitigation of Natural Phenomena Hazards for DOE Nuclear Facilities and Non-Nuclear Facilities." Washington, D.C.

U.S. Department of Energy, 1996, "Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities," DOE-STD-1020-94, Change Notice #1.

U.S. Department of Energy, 1996, "Natural Phenomena Hazards Performance Categorization Guidelines for Structures, Systems, and Components," DOE-STD-1021-93, Change Notice #1.

U.S. Department of Energy, 1996, "Natural Phenomena Hazards Site Characterization Criteria," DOE-STD-1022-94, Change Notice #1.

U.S. Department of Energy, 1996, "Natural Phenomena Hazards Assessment Criteria," DOE-STD-1023-95, Change Notice #1.

TABLE 1

Probabilistic Seismic Hazard Values at Eastern United States Department of Energy Sites

Site	Site Conditions	Peak Acceleration - g				1 Hz Spectral Acceleration - g			
		$2x10^{-3}$	$1x10^{-3}$	$5x10^{-4}$	$1x10^{-4}$	$2x10^{-3}$	$1x10^{-3}$	$5x10^{-4}$	$1x10^{-4}$
OR	Rock	.06	.08	.12	.26	.026	.035	.051	.11
OR	Soil[1]	.15	.20	.30	.65[2]	.044	.056	.081	.17[2]
Port.	Rock	.04	.06	.10	.14[2]	N/A	N/A	N/A	N/A
Port.	Soil[3]	.10	.15	.19	.25[2]	.028	.038	.05	.09[2]
Paduc.	Rock	.20	.30	.42	.75[2]	.05	.09	.14	.36
Paduc.	Soil[4]	.20	.25	.35	.60[2]	.20	.40	.57	N/A
KC	Rock	.02[2]	.025	.037	.088	.007	.011	.017	.043
SR	Rock	.04	.055	.09	.19	.016	.03	.045	.11
SR	Soil[5]	.065[2]	.09[2]	.14	.28	.06[2]	.09	.14	.39
BNL	Soil	.03[2]	.05	.09	.27	.018	.032	.054	.17
ANL	Rock	.02[2]	.03	.05	.13	.01	.014	.021	.055

Probabilities are mean annual probabilities.

[1] Soil ≥ 10 ft. thick
[2] Estimate
[3] Soil ~ 30 ft. thick
[4] Soil ~ 350 ft. thick
[5] Soil ~ F-Area ~ 975 ft. thick
N/A = not available

OR - Oak Ridge Y-12 Site, Tennessee
Port. - Portsmouth, Ohio
Paduc. - Paducah, Kentucky
KC - Kansas City, Missouri
SR - Savannah River, South Carolina
BNL - Brookhaven, New York
ANL - Argonne, Illinois

TABLE 2

Probabilistic Seismic Hazard Values at Western United States Department of Energy Sites

Site	Site Conditions	Peak Acceleration - g				1 Hz Spectral Acceleration - g			
		$2x10^{-3}$	$1x10^{-3}$	$5x10^{-4}$	$1x10^{-4}$	$2x10^{-3}$	$1x10^{-3}$	$5x10^{-4}$	$1x10^{-4}$
LLNL[1]		.50	.58	.68[2]	.98[2]	.43	.56	.68[2]	1.05[2]
NTS/YM		.19	.27	.37	.66	.09	.14	.185	.41
RF		.08	.13	.19	.41	.05	.075	.11	.23
LANL		.15	.22	.31	.58	.15	.26	.38	.85
INEL/TAN		.09	.13	.18	.33	.07	.105	.145	.28
INEL/CPP		.08	.10	.13	.22	.06	.09	.12	.23
HAN 200W		.13	.19	.26	.48	.12	.19	.26	.50
HAN 300		.11	.15	.21	.37	.11	.17	.23	.43

Probabilities are mean annual probabilities

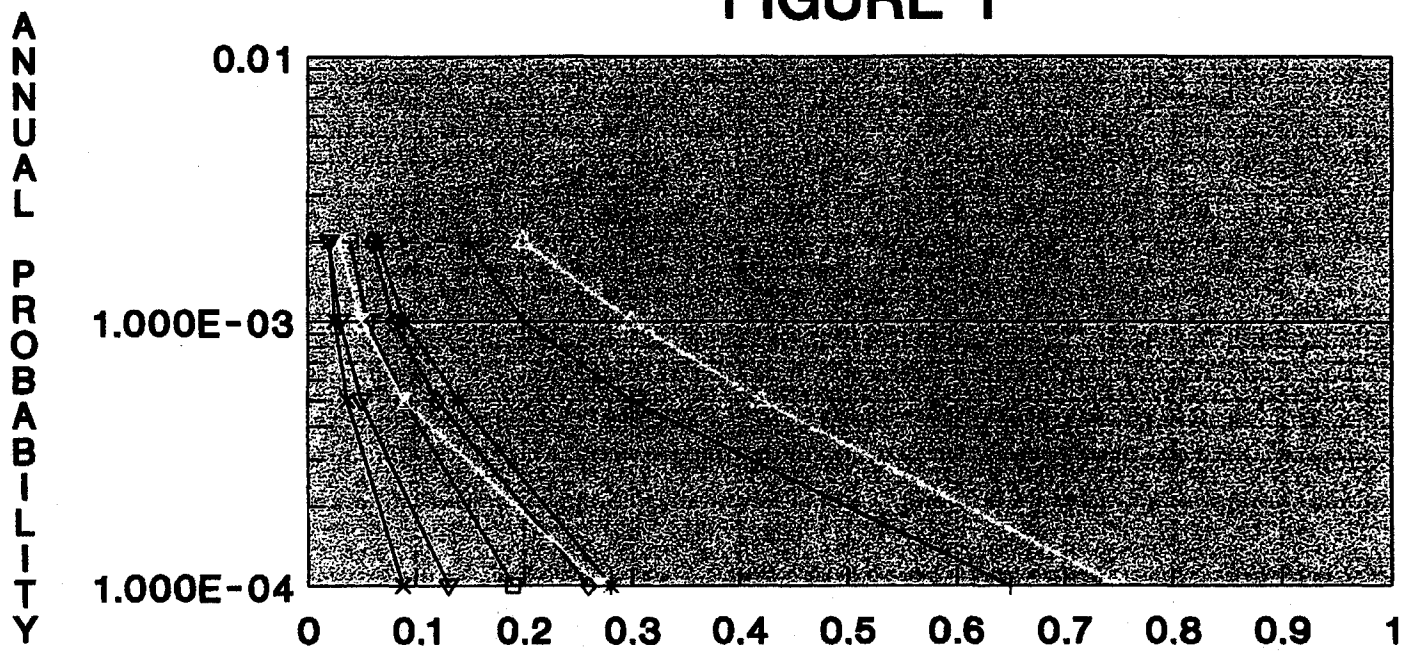
[1] pga = .31 @ prob = 0.1
1 Hz = .24 @ prob = 0.1

[2] Estimate

LLNL - Livermore, California
NTS/YM - Yucca Mountain, Nevada
RF - Rocky Flats, Colorado
LANL - Los Alamos, New Mexico
INEL - Idaho Laboratory, Idaho
(TAN - Test Area North)
(CPP - Chemical Processing Plant)
HAN - Hanford, Washington
(200W - 200 West Area)
(300 = 300 Area)

PROBABILISTIC SEISMIC HAZARD COMPARISONS
DOE EASTERN US SITES (MEAN CURVES)

FIGURE 1

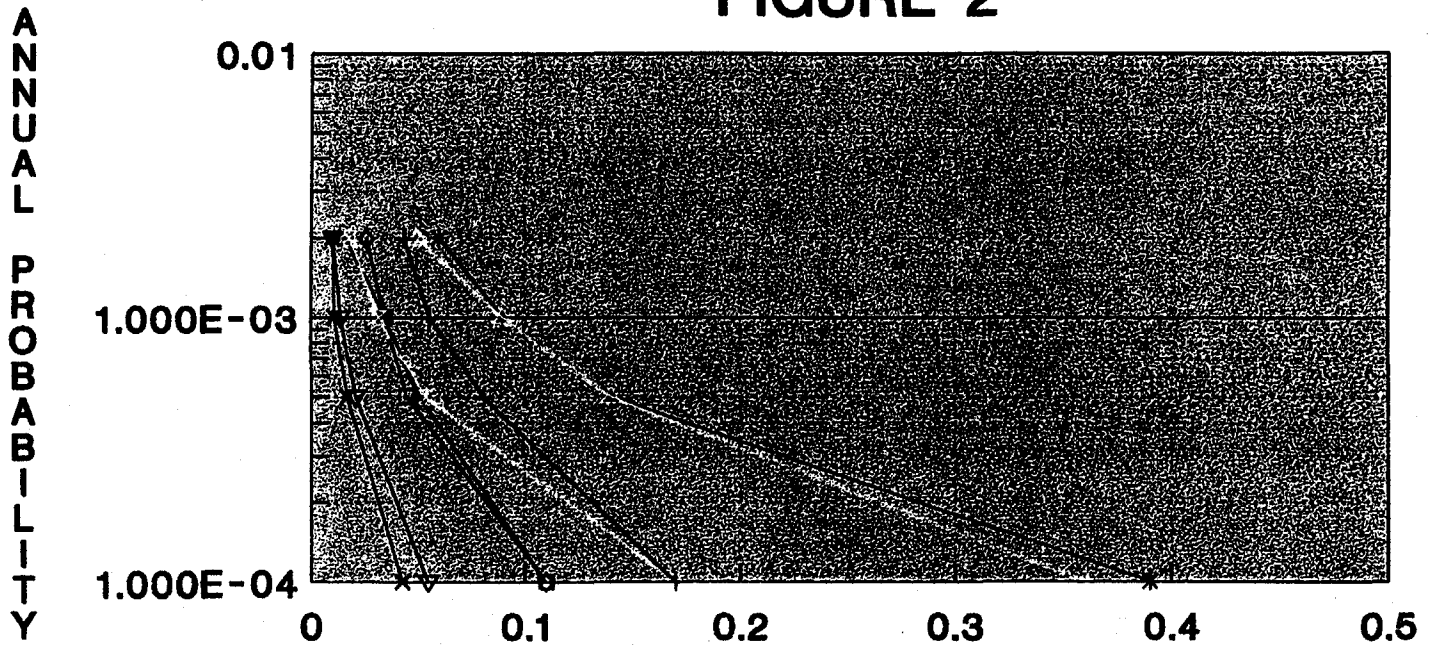


COMPARISON OF PEAK ACCELERATION SEISMIC HAZARD CURVES
FOR DOE EASTERN UNITED STATES SITES

RK=ROCK

PROBABILISTIC SEISMIC HAZARD COMPARISONS
DOE EASTERN US SITES (MEAN CURVES)

FIGURE 2

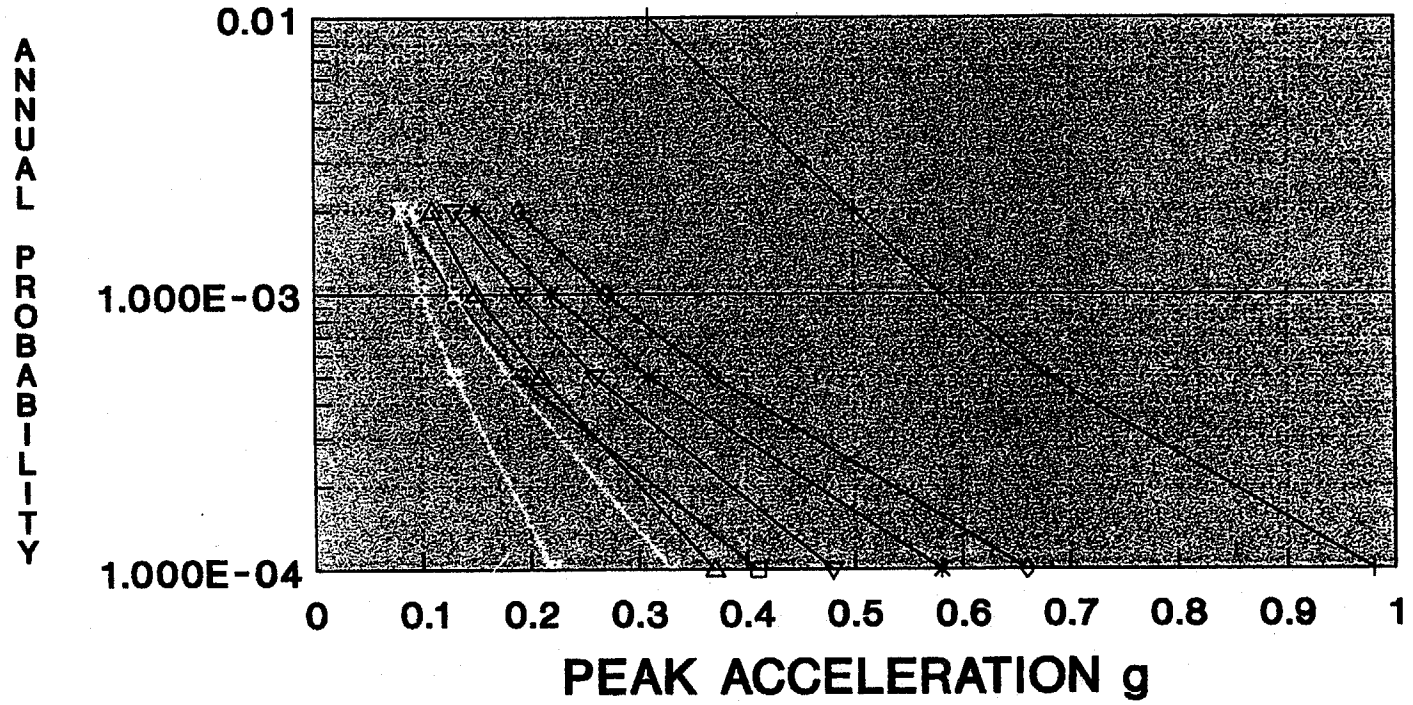


COMPARISON OF 1 HERTZ SPECTRAL ACCELERATION SEISMIC HAZARD CURVES FOR DOE EASTERN UNITED STATES SITES

RK=ROCK

PROBABILISTIC SEISMIC HAZARD COMPARISONS
DOE WESTERN US SITES (MEAN CURVES)

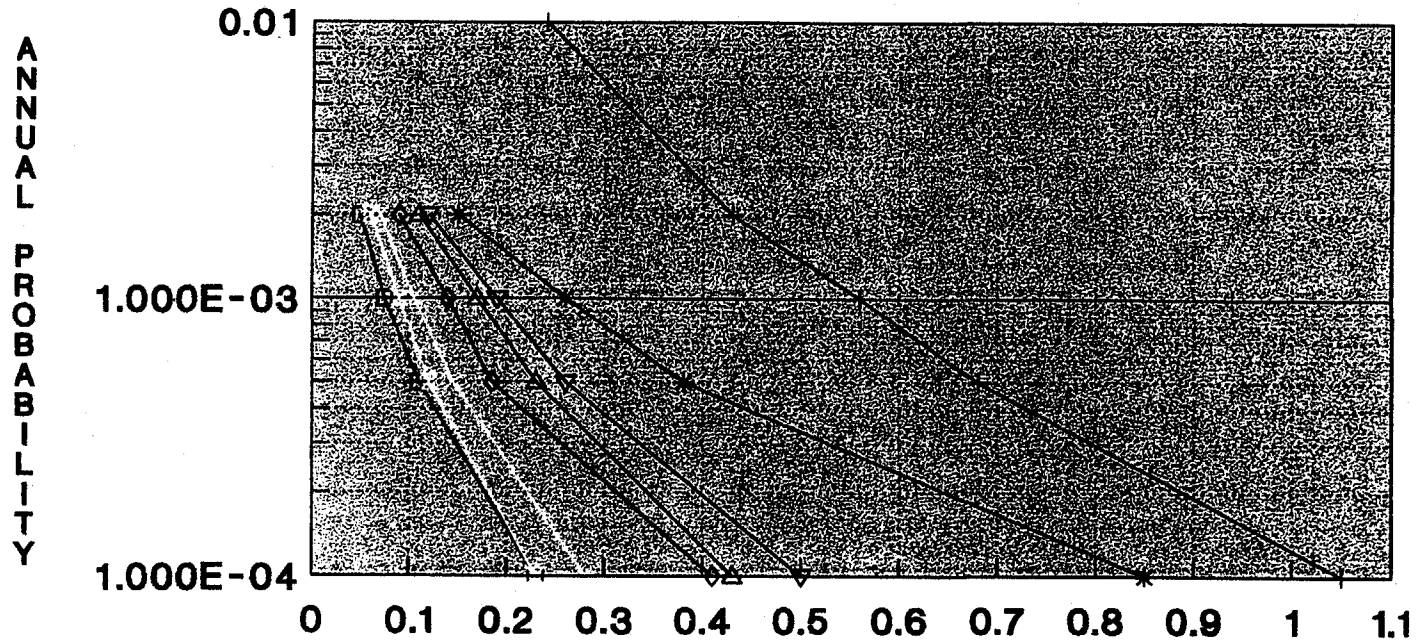
FIGURE 3



PEAK ACCELERATION SEISMIC HAZARD CURVES FOR DOE WESTERN UNITED STATES SITES. WHILE SITE CONDITIONS VARY BETWEEN SITES MOST SITES HAVE STIFF SOIL OR ROCK SITE CONDITIONS

PROBABILISTIC SEISMIC HAZARD COMPARISONS
DOE WESTERN US SITES (MEAN CURVES)

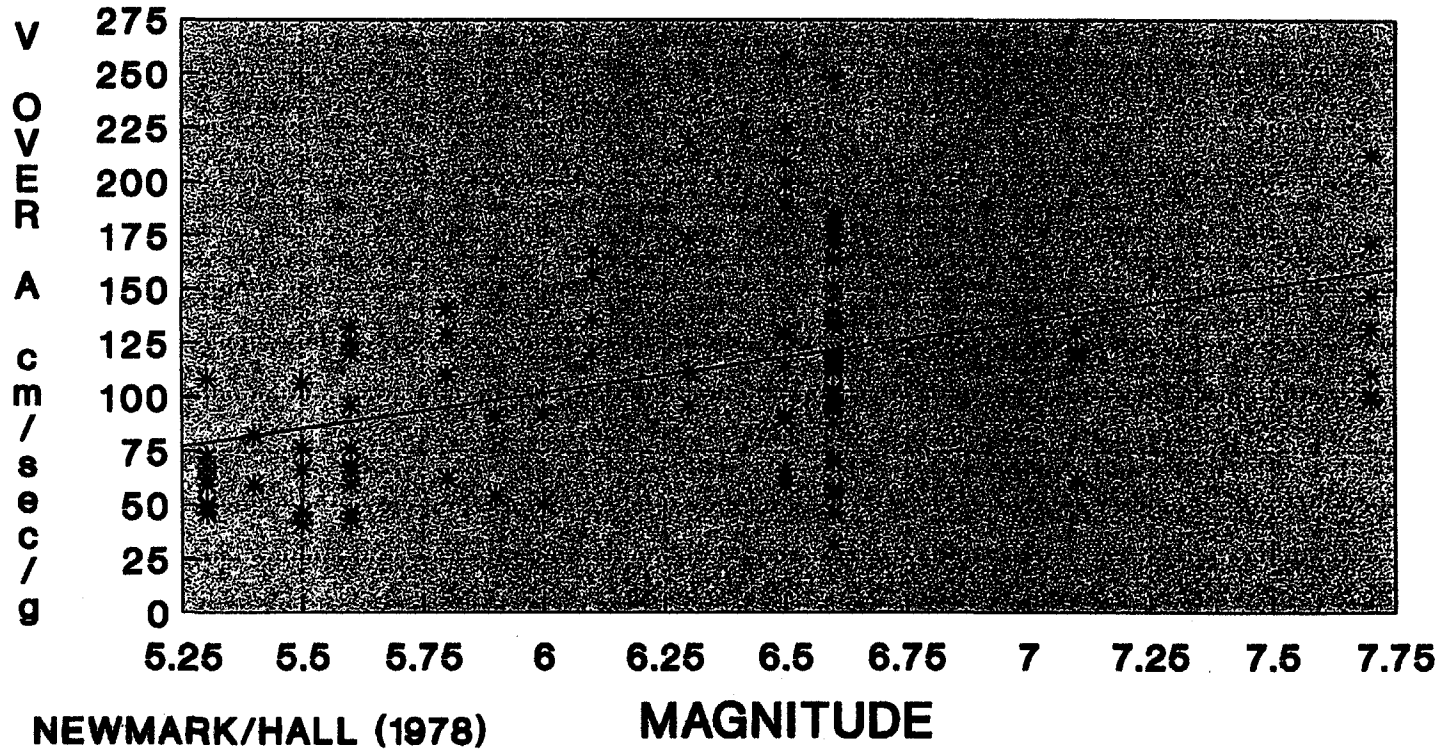
FIGURE 4



1 HZ SPECTRAL ACCEL. SEISMIC HAZARD CURVES FOR DOE WESTERN UNITED STATES SITES. WHILE SITE CONDITIONS VARY BETWEEN SITES MOST SITES HAVE STIFF SOIL OR ROCK SITE CONDITIONS

NEWMARK (1973) STRONG MOTION DATA
VELOCITY/ACCELERATION RATIO

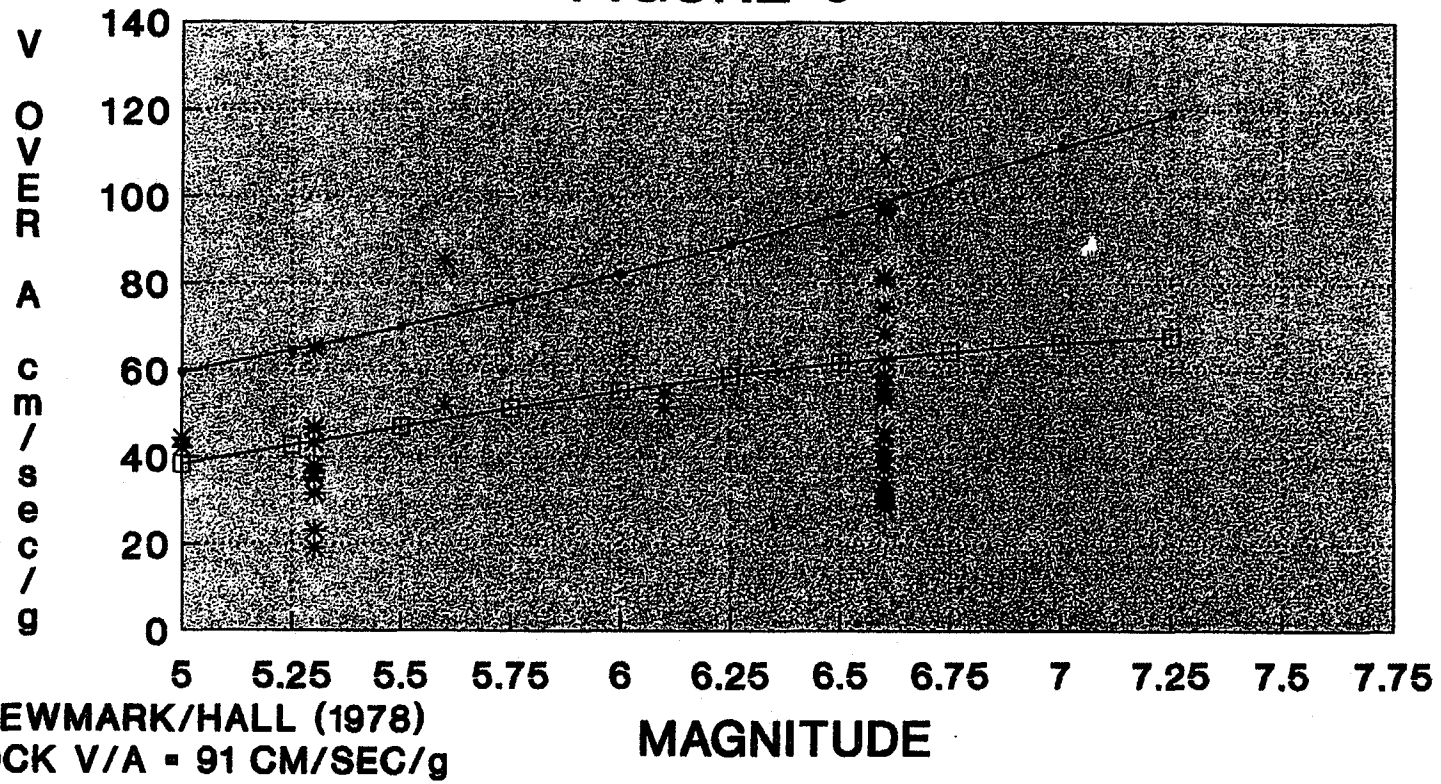
FIGURE 5



PLOT OF INDIVIDUAL DATA POINTS FOR SOIL SITES USING NEWMARK (1973) DATA SET ALONG WITH THE BEST FIT LINEAR RELATIONSHIP SHOWING MAGNITUDE DEPENDENT V/A

VELOCITY/ACCELERATION RATIO'S FROM ROCK PRE-1972 DATA (NEWMARK/HALL LIKE DATA)

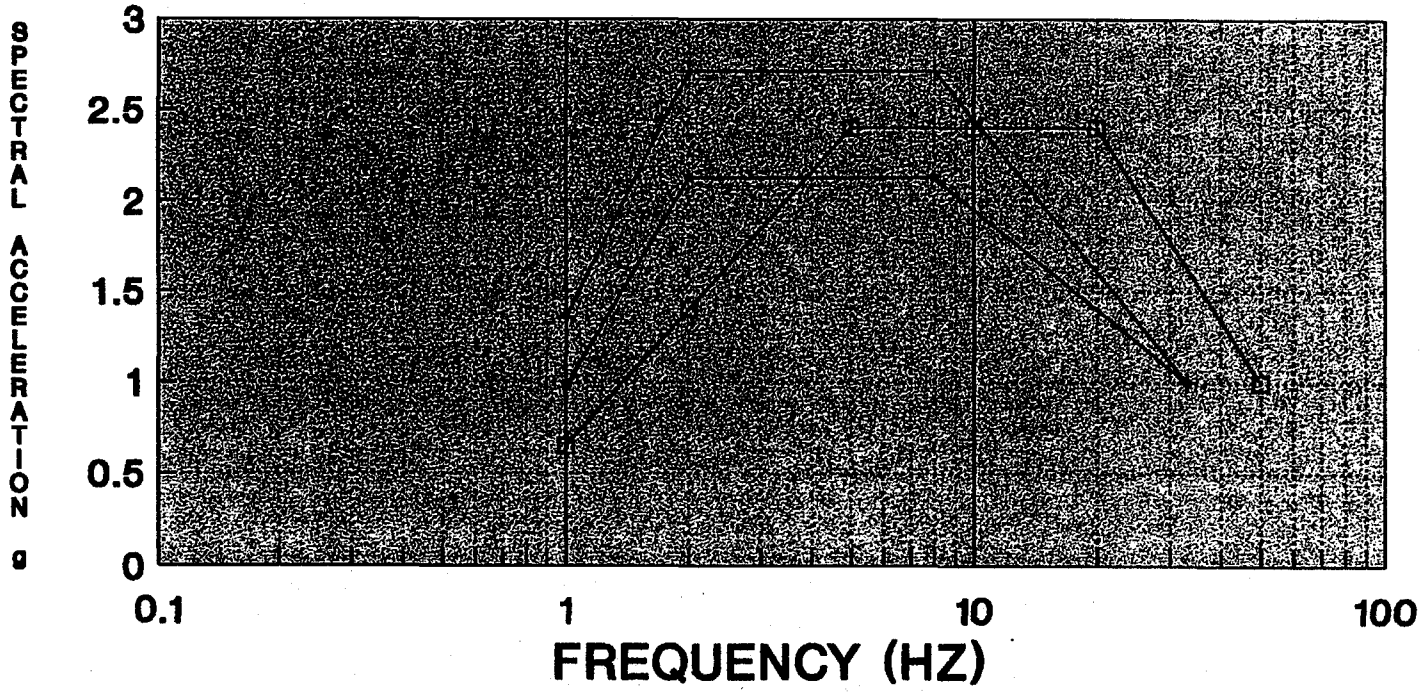
FIGURE 6



PLOT OF INDIVIDUAL DATA POINTS FOR ROCK SITES FOR PRE 1972 STRONG MOTION DATA COMPARED TO V/A BASED ON CAMPBELL 1990 ATTENUATION MODEL - SHOWING MAGNITUDE DEPENDENT V/A

RESPONSE SPECTRA COMPARISONS
SPECTRAL SHAPE ALTERNATIVES

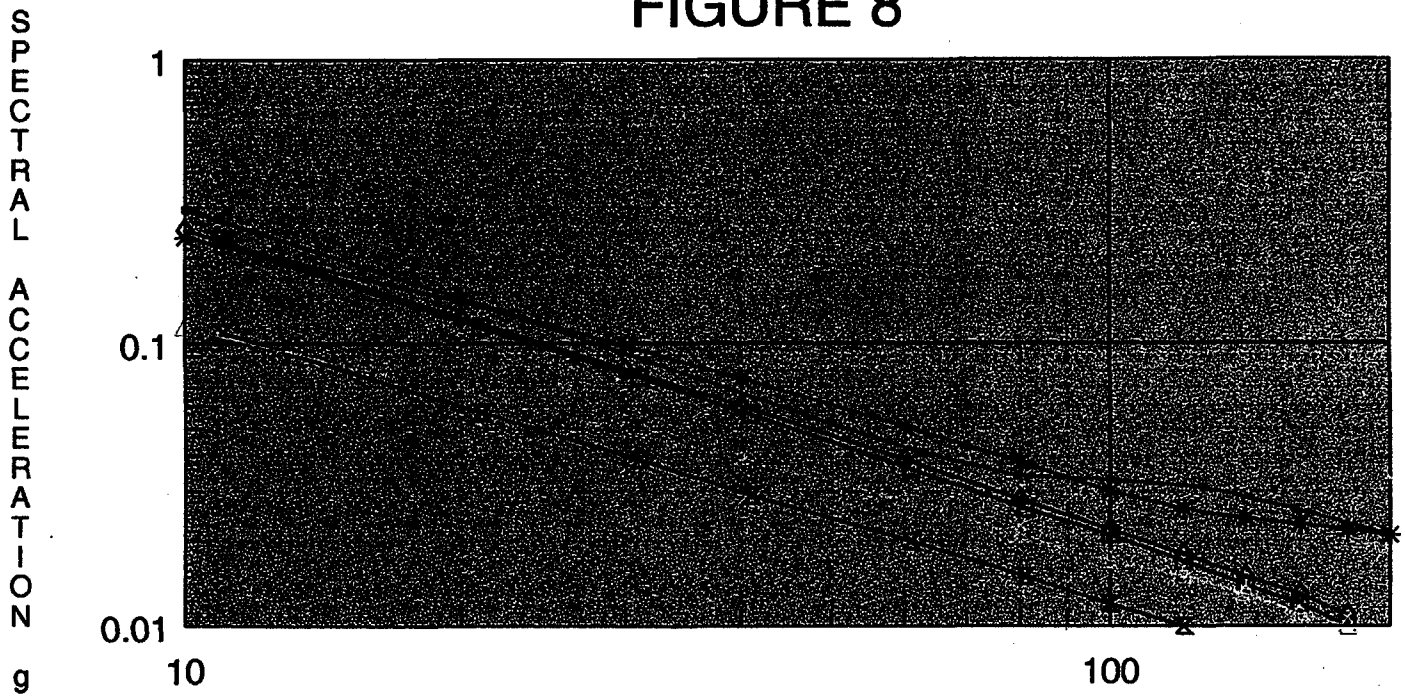
FIGURE 7



ALTERNATIVE RESPONSE SPECTRA DERIVED FROM EUS ATTENUATION MODELS COMPARED TO THE MEDIAN AND 84TH PERCENTILE NEWMARK AND HALL 1978 ROCK SPECTRAL SHAPE

COMPARISON OF 1 HZ SPECTRAL ACCELERATION ATTENUATION MODELS FOR THE EUS

FIGURE 8



A/B 1990, A/B 1995 & USGS 1996 USE Mw = 6.5
EPRI 1987, EPRI 1993 & LLNL COMP USE mb = 6.5

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-0157
Vol. 3

2. TITLE AND SUBTITLE

Proceedings of the Twenty-Fourth Water Reactor Safety Information Meeting

- PRA and HRA
- Probabilistic Seismic Hazard Assessment and Seismic Siting Criteria

3. DATE REPORT PUBLISHED

MONTH	YEAR
February	1997

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 21-23, 1996

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

C. Bonsby, NRC Project Manager. Proceedings prepared by Brookhaven National Laboratory

11. ABSTRACT *(200 words or less)*

This three-volume report contains papers presented at the Twenty-Fourth Water Reactor Safety Information Meeting held at the Bethesda Marriott Hotel, Bethesda, Maryland, October 21-23, 1996. 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, Japan, Norway, Russia and the 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, Nuclear Power Plants - Reactor Safety, PWR Type Reactors - Reactor Safety, Reactor Safety - Meetings, Failure Mode Analysis, Probabilistic Estimation, Reliability, Reactor Accidents, Site Characterization, Seismic Events

13. AVAILABILITY STATEMENT

Unlimited

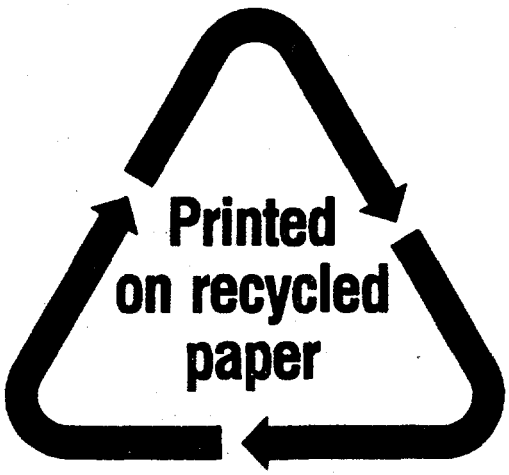
14. SECURITY CLASSIFICATION

(This Page)
Unclassified

(This Report)
Unclassified

15. NUMBER OF PAGES

16. PRICE



Federal Recycling Program