PROCEEDINGS OF

PSAM — II

Volume 1

(Sessions 1 - 36)

An International Conference Devoted to the Advancement of System-based Methods for the Design and Operation of Technological Systems and Processes

San Diego, California, U.S.A.

March 20-25, 1994

PROCEEDINGS OF

PSAM — II

An International Conference Devoted to the Advancement of System-based Methods for the Design and Operation of Technological Systems and Processes

San Diego, California, U.S.A.

March 20-25, 1994

Editors

G.E. Apostolakis and J.S. Wu
University of California, Los Angeles

Contributing Editors

D. Bley, PLG, Inc.
S. Guarro, Aerospace Corp.
V. Ho, PLG, Inc.
R. Mulvihill, PRC, Inc.
D. Orvis, APG, Inc.
N. Sankaran, Unocal Corporation
N. Siu, Idaho National Engineering Laboratory
M. Stamatelatos, Scientech, Inc.

FOREWORD

These volumes contain papers that were presented at the PSAM II Conference. PSAM I was held in February, 1991 and its success led to the present Conference and hopefully many more.

The purpose of the PSAM Conferences is to provide a forum for the presentation of scientific papers covering both methodology and applications of system-based approaches to the design and the effective, safe operation of technological systems and processes. These include nuclear plants, chemical and petroleum facilities, defense systems, aerospace systems, and the treatment and disposal of hazardous wastes. The objective is to share experiences to the benefit of all industries.

We would like to comment on the production of these proceedings, specifically the printing and binding. Unfortunately, the publishers we had contracted to publish the proceedings did not fulfill their obligation to have them available in time for the Conference. Due to our strong belief that the proceedings should be handed out at the Conference, we have done our best to produce these volumes in the very short time available.

The Editors

SPONSORED BY THE

Society for Risk Analysis

European Safety and Reliability Association

COSPONSORED BY THE

American Nuclear Society

American Society of Mechanical Engineers

IEEE Reliability Society

SPONSORING ORGANIZATIONS

Aerospace Corporation

APG, Inc.

ASCA, Inc.

Electric Power Research Institute

Idaho National Engineering Laboratory

Kazarians & Associates

Los Alamos National Laboratory

PLG, Inc.

PRC, Inc.

SAIC

Sandia National Laboratories

Scientech, Inc.

Tenera

Unocal Corporation

University of California, Los Angeles

University of Maryland

US Department of Energy

GENERAL PROGRAM CHAIRMAN

Michael G. Stamatelatos, Scientech, Inc.

ASSOCIATE GENERAL CHAIRMAN

Doug Orvis, Accident Prevention Group

SENIOR ADVISORY BOARD

B.J. Garrick, PLG, Inc., Chairman

A. Amendola, Commission of European Communities
A.H-S. Ang, University of California, Irvine
A.T.D. Butland, SRD, United Kingdom
J.E. Fitzgerald, Jr., US Dept. of Energy
V.L. Grose, Omega Systems Group
D-Y. Hsia, Institute of Nuclear Energy Research, Taiwan
V. Joksimovich, Accident Prevention Group
S. Kondo, University of Tokyo
J. Meltzer, The Aerospace Corporation
N.C. Rasmussen, Massachusetts Institute of Technology
L. Ybarrondo, Scientech, Inc.

CONFERENCE LOCAL ORGANIZING COMMITTEE

A.A. Dykes, PLG, Inc., Chairman

D. Bley, PLG, Inc.
S.Guarro, The Aerospace Corporation
D. Henneke, TENERA
V. Ho, PLG, Inc.
M. Kazarians, Kazarians & Associates
A. Mosleh, University of Maryland
R. Mulvihill, PRC, Inc.
D. Orvis, APG
N. Sankaran, UNOCAL Corporation
N.O. Siu, INEL
M. Stamatelatos, Scientech, Inc.

ORGANIZING STAFF

D. Bell, UCLA
M. Hanna, UCLA
J. George, UCLA
C. Garrett, UCLA
T. Paulos, UCLA

TECHNICAL PROGRAM COMMITTEE

CHAIRMAN

G. Apostolakis, University of California, Los Angeles, USA

ASSOCIATE CHAIR

J.S. Wu, ASCA, Inc.

MEMBERS

D. Aldridge, USA
H.P. Alesso, USA
A. Amendola, Italy
D.R. Anderson, USA
B. Ayyub, USA
R.A. Bari, USA
J.H. Bickel, USA
V.M. Bier, USA
D. Bley, USA
E.J. Bonano, USA
S. Book, USA
B. Bream, USA
D. Brooks, USA
M.L. Brown, UK
B. Buchbinder, USA
R.J. Budnitz, USA
P.C. Cacciabue, Italy
A. Camp, USA
R.M. Cooke, Netherland
R.A. Cox, UK
D. Croucher, USA
G.E. Cummings, USA
D. Cunha, USA
K. Dahlgren, Sweden
J. Devooght, Belgium
A.A. Dykes, USA
T. Eng, USA
D. Frangopol, USA
M.V. Frank, USA
R. Friedman, USA
R.R. Fullwood, USA
W.J. Galyean, USA
D.I. Gertman, USAL.H.J. Goossens, Netherlands
S. Guarro, USA
M. Haim, Israel
G.W. Hannaman, USA
J.C. Helton, USA
D. Henneke, USA
S. Hirschberg, Switzerland
V. Ho, USA
E. Hollnagel, UK
K. Inoue, Japan
K. Jamali, USA
D.H. Johnson, USA
P. Kafka, Germany
G.D. Kaiser, USA
D.M. Karydas, USA
W.E. Kastenberg, USA
M. Kazarians, USA
D.L. Kelly, USA
K. Klein, USA
R.F. Lavelle, USA
C. Lavine, USA
L. Lee, USA
S. Lydersen, Norway
M. Maharik, Israel
D. Majumdar, USA
G. Mancin, Italy
M. Marseguerra, Italy
T. Matsuoka, Japan
M. Modarres, USA
D.A. Moore, USA
A. Mosleh, USA
R. Mulvihill, USA
K. Murphy, USA
D. Okrent, USA
L.F. Oliveira, Brazil
N. Ortiz, USA
D. Orvis, USA
I.A. Papazoglou, Greece
C.K. Park, Korea
G.W. Parry, USA
M.E. Pate-Cornell, USA
P. Prassinos, USA
C. Preyssl, Neth.
D. Rice, USA
L.K. Rudolph, USA
B. Sagar, USA
N. Sankaran, USA
J.C.H. Schuler, Netherland
N.O. Siu, USA
D. Stack, USA
M. Stamatelatos, USA
J-P. Sursock, USA
O. Svenson, Sweden
B. Thompson, U.K.
W. Tosney, USA
L.P. Vestrucci, Italy
J. Wreathall, USA
J. Ziagos, USA

CONTENTS

001 Risk Based Prioritization (I)
Chair: P. Prassinos, USDOE

Qualitative Safety Analysis of Proposed Material Relocation Options
N.G. Cathey, T.L. Foppe (EG&G)

Risk-Based Methods Applicable to Ranking Conceptual Designs
R.J. Breeding, J.T. Ringlnad, K. Ortiz (SNL), J.J. Lim (Lim & Orzechowski)

Process Hazards Assessment Using Risk Matrices
D.H. Henneke, J. Phillips (TENERA)

002 Uncertainties and Sensitivities
Chair: R.M. Cooke, Delft U. Technol

Assessing the Risks and Uncertainties due to Incinerator Toxic Air Pollutants Emission
J. Swider, W.E. Kastenberg (UCLA)

Dependability Through Auditing
J.R. Stone, D.I. Blockley (U. Bristol)

Multi-Level Control Against Uncertainties and Failures Consequences
V.N. Efanov, V.G. Krymsky (Ufa St. Aviation Engineering, Russia)

003 Software Dependability (I)
Chair: C. Lavine, The Aerospace Corporation

Risk Assessment and Management of Safety-Critical, Digital Industrial Controls - Present Practices and Future Challenges
W.R. Dunn (USC); M.V. Frank, S.A. Epstein (Safety Factor Assoc.); L. Doty (NASA)

Reliable Process Execution in FMS by Extended Transactions
U. Schmidt (U. Stuttgart)

004 Dependent Failures

Chair: M. Haim, Rafael

CCDAT, an Automated Tool for Common Cause Failure Data Analysis and Parameter Estimation

F.R. Hubbard (FRH); A. Mosleh (U. Maryland)

Development of a Data Base of Common Cause Failure Events at U.S. Nuclear Power Plants

D. Rasmuson (USNRC); A.Mosleh (U.Maryland); F.Marshall, K. Kvarfordt (EG&G)

005 Advances in Human Reliability Analysis

Chair: G.W. Parry, NUS

A Procedure for the Analysis of Errors of Commission in a PSA

G.W. Parry, J. Julius, E. Jorgenson (NUS); A. Mosleh (U. Maryland)

Human Reliability Analysis for Seismic Events

T.V. Vo, T.M. Mitts (PNL); C.M. van Bujjtenen, E.Wingo (Westinghouse Savannah Rvr.)

Evidence of the Need to Model Errors of Commission in Risk Assessments for Varied Environments

D.I. Gertman, L.N. Haney, L.T. Ostrom (INEL)

Application of HRA in the Commonwealth Edison Individual Plant Examinations

L. Soth (Commonwealth Edison)

006 Uncertainties and Sensitivities in Physical and Chemical Phenomenology--Thermal Phenomenon

Chair: N. Ortiz, SNL

Methodology to Evaluate Uncertainty in Thermalhydraulic Code Calculations

F. D'Auria, G.M. Galassi, S. Belsito (U. Pisa); N. Debrecin (U. Zagreb)

Two Methods for Estimating the Probability of Fuel/Coolant Interactions: Applications to Aluminum/Water

J.A. Close, R.L. Moore, L.G. Blackwood (INEL)

Uncertainties in the Characterization of the Thermal Environment of a Solid Rocket Propellant Fire
J.C. Diaz (LLNL)

Probabilistic Estimates of Hanford Waste Tank Failure due to Hydrogen Burns
R.K. Deremer (PLG), D.R. MacFarlane (LANL)

007 Quantitative Risk Assessment and Process Industry Decision Making
Chair: I.A. Papazoglou, Inst. Nucl. Technol. & Radiat. Protec.

The Use of Quantitative Risk Assessment as a Decision Making Tool
G.N. Pettitt, B. Harvey, D.R.E Worthington (DNV Technica)

008 Choosing Among Alternative Programs or Strategies
Chair: H.F. Martz, LANL

Integrated Regional Risk Assessment and Safety Management: The Experience of Switzerland
A.V. Gheorghe (ETH, Switzerland)

WESVA: A Decision Aid for Comparing Warhead Advanced Surety R&D Options
R.V. Homsy, A. Sicherman, D.R. Stephens (LLNL)

009 Uncertainty in Offsite Consequence Models for Reactor Accidents
Chair: J.C. Helton, Arizona St. U

Modular Analysis of Radiological Consequence Uncertainties and Sensitivities (MARCUS)
L.F. Restrepo (SNL), F.E. Haskin (U. New Mexico)

Summary of Uncertainty Analysis of Dispersion and Deposition Modules of the MACCS and COSYMA Consequence Codes - A Joint USNRC/CEC Study
F.T. Harper, L.A. Miller, M.L. Young (SNL); L.H.J. Goossens, R.M. Cooke (Delft U. Technol.); S.C. Hora (U. Hawaii); J. Pasler-Sauer (KfK, Germany); C. Lui (USNRC), N. Kelly (CEC, Belgium)

A Procedure for Assessing Uncertainty in Models.
M.D. McKay, R.J. Beckman (LANL)

Uncertainty and Sensitivity Analysis of Early Exposure Results with the MACCS Reactor Accident Consequence Model
J.C. Helton (Arizona St. U), J.D. Johnson (GRAM); M.D. McKay (LANL); A.W. Shiver, J.L. Sprung (SNL)

010 Computer-based Systems and Plant Models

Chair: P. Kafka, Gesellschaft für Reaktorsicherheit (GRS)

Use of System Simulation to Support Automated Fault Tree Construction
A. Carpignano (Politecnico Torino, Italy)

Plant Specific PSA Supported and Enhanced by a Computer Based Failure Mode and Effect Analysis (FMEA)
H-P. Balfanz (TUV-Nord)

Identification of Components to Optimize Improvement in System Reliability
L. Painton (Carnegie Mellon U), J. Campbell (SNL)

An Introduction to Dynamic MPLD Model
Y-S. Hu, M. Modarres (U. Maryland)

011 PSA for Dynamic Systems: Modeling Approaches

Chair: M. Marseguerra, Univ. of Milan

A Theoretical Analysis of DYLAM-Type Event Tree Sequences
J. Devooght (U. Libre de Bruxelles); C. Smidts (U. Maryland)

Probabilistic Dynamics: A Numerical Comparison Between a Continuous Event Tree and a DYLAM-Type Event Tree
C. Smidts (U. Maryland); J. Devooght (U. Libre de Bruxelles)

Assessing DYLAM Methodology in the Frame Montecarlo Simulation
G. Cojazzi, P. Vestrucci (CEC- JRC, Ispra)

012 Methods/Data and Applications for Improving Human Reliability in Plant Operations

Chair: G.W. Hannaman, SAIC

Human Reliability Database for In-Plant Application of Industry Data
G.W. Hannaman (SAIC); A. Singh (EPRI)

Risk Management Activities to Address the Impact of Human Errors and Human Error Variability
J.C. Higgins, J.M. O'Hara (BNL)

Generic Event Trees and the Treatment of Dependencies and Non-Procedural Actions in a Low Power and Shutdown Probabilistic Risk Assessment
J. Forester (SAIC); D.W. Whitehead (SNL); J. Darby (S&EA); J. Yakle (SAIC)

013 Nuclear Reactor PSA Applications
Chair: B.O.Y. Lydell, NUS

Application of Petri-Nets-Based Model to Reliability and Risk Analysis of Nuclear Power Plant
G. Petkov (Risk Eng., Bulgaria); S. Doytchinov (Tech. U., Bulgaria)

K Reactor Restart Configuration - Level 1 Internal Events PRA Results (U)
S.P. Tinnes, D.S. Cramer, V.E. Logan, S.V. Topp, J.A. Smith, H.A. Ford, R.T. Bailey, M.D. Brandyberry, B.G. Kingery (Westinghouse Savannah Rvr.)

Predictability Versus Availability High Flux Isotope Reactor
L. Merryman (ORNL), E. Ballon, B. Christie (RAPA)

014 PRA Methodology
Chair: J-P. Sursock, EPRI

How Uncertain We Should be About the Outputs of a PSA: the HMIP Procedure
P. Grindrod, (INTERA); S. Watson (Cambridge Decision Analysts)

Development of a Level 2 PSA Approach to Support Regulatory Evaluation of Severe Accident Management (SAM) Strategies
T. Okkonen, I.M. Niemela, J. Sandberg, R.K. Virolainen (STUK, Finland)

015 Decision Policy Management
Chair: R.S. Strait, LLNL

Risk Based Performance Goals and Probabilistic Source Term in Environmental Restoration and Waste Management Activities
D.A. Reny, T.E. Wierman (TENERA)

Managing Uncertainty in Risk Analysis Decisions
W.D. Rowe, K.J. Beierschmitt (Battelle Pantex)

PRA As A Management Tool: Improving the Safety of the Tiles of the Space Shuttle Orbiter
E. Paté-Cornell (Stanford U.); P. Fischbeck (Carnegie Mellon U.)

Reaching End of License - Big Rock Point
J.R. Schepers, G.C. Withrow (Consumers Pwr. Co.)

A Risk Assessment and Management Tool for the Chemistry and Metallurgy Research (CMR) Building
J.L. LaChance, A. Kolaczkowski, A. Crawford, J. Holderness, (SAIC); G. Medford (LANL)

016 Uncertainty in Performance Assessment

Chair: M.G. Marietta, SNL

Uncertainties in Probabilistic and Non-Probabilistic Risk Assessment
K.E. Petersen (Riso Natl. Lab.)

Management/Technical Assessments on Yucca Mountain
C.P. Gertz (USDOE); S.R. Mattson (SAIC)

Risk Assessment of Coordinate Measuring Machine-Based Dimensional Inspection Technology
Y-L. Shen, X. Zhang (George Washington U.)

The Effect of Uncertainties in Dose-Response Data on Risk Management of Air Toxics
J.C. Huang, W.E. Kastenberg (UCLA)

018 Reliability, Models & PSA

Chair: K. Inoue, Kyoto Univ.

Identification of System States Based on Multistate Model
K. Nakashima (Faculty of Engineering, Japan); H. Matznaga (Toyama Prefectural U., Japan)

Safety Substantiation Analysis for Airplane Systems
B. Zilberman (Israel Aircraft Ind.)

Automatic Construction of Markovian Transition Matrices for the Treatment of Large Size Reliability Problems
B. Tombuyses (U. Libre de Bruxelles); B. Arien, D. Lamy (SCK/CEN, Belgium)

Markovian Models for the Reliability Analysis of Multichanneled Protective Systems
P.F. Frutuoso e Melo (COPPE/UFRJ, Brazil); L.F. Oliveira (PRINCIPIA Ltda. and U. Federal of Bahia, Brazil); R. Youngblood (BNL)

019 Risk Management for Continuous Releases of Airborne Toxics

Chair: W.E. Kastenberg, UCLA

California's Air Toxics "Hot Spots" Law. I. Mechanics of the Law
J.F. Collins, M.A. Marty, , G.V. Alexeeff (Of. Environ. Hlth. Haz. Assmt.)

Uncertainties in the Health Risk Assessment of Fossil-Fueled Electric Power Stations
L.B. Gratt (IWG)

Automated Risk Assessment for California's Air Toxics Hot Spots Act
J.H. Stuhmiller (JAYCOR)

020 Applications for Process Operational Safety

Chair: F. Dombek, NUS

System-Based Approach to Safety Equipment Classification for a Radiochemical Facility
S.T. Almodovar, C.L. Whalen (Jason Assoc.)

A Probabilistic Risk Analysis of a LPE Laboratory
S. Arueti (RAFAEL Reliability Ctr., Israel); M. Mor (SCD, Israel)

Hanford High-Level Waste (HLW) Tank Mixer Pump Safe Operating Envelope Reliability Assessment
S.R. Fischer (LANL); J. Clark (Science & Eng. Assoc.)

021 Management of Risk in Chemical Processes

Chair: G.D. Kaiser, SAIC

Risk Management for Hazardous Materials within the City of Torrance
J.D. Kulluk (Torrance Fire Dept.)

Difficulties in Decision Making without Consideration of Risk
G.D. Kaiser (SAIC)

Risk-Based Regulation Setting Goals for Health and Safety
J. Bacon (HSE, UK)

022 Risk Management in DOE (I)

Chair: K. Murphy, USDOE

Risk Management at the Oak Ridge National Laboratory Research Reactors
G.F. Flanagan, M.A. Linn, L.D. Proctor, D.H. Cook (ORNL)

Risk Management at LLNL
G.E. Cummings, S.R. Strait (LLNL)

Risk Management at Los Alamos National Laboratory
D.G. Brooks (Arizona State U), D.W. Stack (LANL)

023 Environmental Consequence Analysis

Chair: K.R. O'Kula, Westinghouse Savannah Rvr.

MACCS Usage at Rocky Flats Plant for Consequence Analysis of Postulated Accidents
T.L. Foppe, V.L. Peterson (EG&G Rocky Flats)

Practical Application of Probabilistic Risk Analysis for Marine Oil-Spills
D.J. Winfield (AECL Research); D. Dickins (D.F. Dickins & Assoc.)

On the Environmental Risk of Methanol Spills and Leaks
P.T. Katsumata, W.E. Kastenberg (UCLA)

024 Computerized Monitors and Operator Aids (I)

Chair: A.J. Spurgin, Consultant

Object Oriented Plant Models for Off-Line and On-Line Risk Monitoring
A. Poucet (CEC-JRC, Italy); A. Carpignano (Politecnico di Torino, Italy)

Object-Oriented Toolkit for Intelligent Plant Monitoring System: TIPS
T. Ohi, K. Sasaki (Mitsubishi Electric, Japan)

A Computer Aid for Safety Assessment and Configuration Management of Complex Systems Based on PSA Models
P. Kafka, O. Lupas, J. Wu, M. Zimmermann (GRS)

025 PSA for Dynamic Systems: Analysis Techniques

Chair: N.O. Siu, INEL

Improving the Efficiency of Monte Carlo Methods in PSA by Using Neural Networks
M. Marseguerra, E. Zio (Polytechnic of Milan)

Sensitivity Analysis Techniques in Reliability Studies
A. Dubi (Ben Gurion U. Israel); A. Gandini (ENEA, Italy)

Validation of Non-Markov Monte Carlo Calculations of System Reliability
J.D. Lewins, Y. Wu (Cambridge U.)

Variance Reduction Techniques for Dynamic Probabilistic Risk Assessment
N.O. Siu, D.L. Kelly, J.A. Schroeder (INEL)

026 Nuclear Power Safety: Risk Analyses from Engineering and Human Factors Perspectives

Chair: O. Svenson, Stockholm U.

Self-Reported Human Errors in Control Room Work
L. Jacobsson, O. Svenson (Stockholm U., Sweden)

Development of an Orientation Based Approach to Evaluation of Process Operators' Expertise
L. Norros, K. Hukki (Technical Res. Ctr. Finland)

Decision Making under Uncertainty: A Pilot Study on Exemption from Technical Specifications
K. Porn (Studsvik Eco & Safety, Sweden)

027 Hazard Analysis in the Process Industries

Chair: T. Aldemir, Ohio State U.

Hazard Analysis for Compliance with Process Safety Regulations
M. Kazarians (Kazarians & Assoc.)

Ristox, A Toxic Gas Risk Analysis Program
J.M. Hudson, A. See (ACTA)

Case Study of A Quantitative Risk Analysis to Compare Process Alternatives
J.T. Cranefield, D.M. Karydas, P.A. Stavrianidis (Factory Mutual Res.); V. Ley (Texas Instr.)

028 Risk Management in Operations

Chair: M. Stamatelatos, Scientech

Assessing the Risk Impact of Integrating Surveillance Testing and Maintenance
C.L. Smith, P.G. Ellison, J.A. Schroeder (INEL)

Empirical Bayes Estimation of the Average Reliability of Nuclear Power Plant Emergency Diesel Generators to Load-Run Upon Demand
H.F. Martz (LANL); L.R. Abramson (USNRC)

Analyses of Reliability Characteristics of Emergency Diesel Generator Population Using Empirical Bayes Methods
W.E. Vesely (SAIC); S.P. Uryas'ev, P.K. Samanta (BNL)

An Unavailability Model for Errors Made During Surveillance Testing
T.F. Bott (LANL)

029 Determining the Adequacy of Deep Technical Knowledge and Quantifying Its Effect on Risk

Chair: D. Okrent, UCLA

Two Proposed Methods for Incorporating Deep Technical Knowledge Using Behaviorally Anchored Rating Scales into Probabilistic Risk Assessments
E.C. Abbott (ABZ); Y. Xiong , D. Okrent, (UCLA)

Level of Knowledge and Safety
L.J. Reynes (Electricite de France)

Deriving Start-Up Task Descriptions from Functional Models
M.N. Larsen, J.K. Hansen, P.C. Cacciabue (CEC-JRC, Italy)

030 Uncertainities in Chemical and Physical Phenomenology-ConsequenceAnalyses

Chair: M.L. Brown, AEA Technol.

International Assessment of PCA Codes
L. Neymotin (BNL); C. LUI, S. Acharya, J. Glynn (USNRC)

Quantitative Guidelines for Safe Storage of a Reactive Chemical: Ammonium Perchlorate
S.D. Emerson (Kerr-McGee)

Probabilistic Consequence Assessment of Postulated Accidents in the DefenseWaste Processing Facility Using MACCS2 (U)
J.M. East, K.R. O'Kula (Westinghouse Savannah Rvr.)

031 Computerized Monitors and Operator Aids (II)

Chair: L. Norros, VTT Finland

Evaluation of Computerized Emergency Operating Procedure Systems as an Operator Support in Nuclear Power Plants
P. Moieni (Accident Prevention Grp.); A.J. Spurgin

DIMOS: A New Generation of Nuclear Power Plant Process Monitoring Systems
M. De Vlaminck, B. Gilliot (Belgatom, Belgium)

Risk Management Insights from the Development and Use of the San Onofre Safety Monitor
T.A. Morgan (Haliburton NUS); T.G. Hook, R. Lee (S. Cal. Edison)

COSMIC Modelling with Personal Computers
R. Strong (Safety Analysis Sys.)

032 Methodology

Chair: L.R. Abramson, LANL

A Dynamic Goal Tree Approach for Process Safety Management
X. Wang, M.L. Roush (U. Maryland)

Calculating Exact Top Event Probabilities Using ΣΠ-PATREC
A.S. Heger, G. Shamanna (U. New Mexico); D.W. Stack, D.V. Talbott (LANL)

Development of the GO-FLOW Reliability Analysis Methodology - Common Cause Failure Analysis and Uncertainty Analysis
T. Matsuoka, M. Kobayashi (Ship Res. Inst., Japan)

Malfunctioning Evaluation of Pressure Regulating Installation by Integrated Dynamic Decision Analysis
R. Galvagni, I. Ciarambino (SYRECO); N. Piccinini (Politecnico di Torino)

033 Team Skills and Group Processes in Human Reliability

Chair: D. Orvis, Accident Prevention Group

.The Significance of Operator Team Interaction Skills to Nuclear Power Plant Risk
M.S. Harris (PNL)

Root Cause Analysis Methodologies: Trends and Needs
G. Cojazzi, L. Pinola (CEC-JRC, Italy)

034 Reliability/Availability/Maintainability Improvement

Chair: S.H. Levinson, B&W Nucl. Technol.

Improving the Conditional Probability of the Emergency Feedwater System at Arkansas Nuclear One - Unit 2
D. Johnson, J. Miller, D. Nilius (Entergy); B. Christie (RAPA)

Emergency Diesel Generator Conditional Probability Analysis Arkansas Nuclear One - Unit 2
T. Ivy (Entergy); B. Christie (RAPA)

ESFAS Reliability Analysis to Justify Test Interval Extension
S.H. Levinson, R.S. Enzinna (B&W Nucl. Technol.)

035 Regulation and Legal Issues

Chair: C. Guedes Soares, Tech. U. Lisbon

Reliability Certification Methodology of Electronic Systems Used for Protection
P.A. Stavrianidis, D.M. Karydas (Factory Mutual Res.)

Risk Assessment: Overview of Land-Based Tort Liability
J.L. Borrello, M.J. Spansel (Adams and Reese)

Cost-Risk Factor Development Using the Maxwell Risk Criteria Matrix (MRCM) & theAnalytical Hierarcy Process (AHP)
D.R. Graham (SMC/FMCC)

036 Risk Management in DOE (II)

Chair: T. Eng, USDOE

Environment, Safety and Health Decision Process at a DOE Multipurpose Research Laboratory
W.R. Casey, M.S. Davis, J.B. Deitz, O. White (BNL)

Risk Management at Argonne National Laboratory
D.J. Hill, R.D. Hislop (ANL)

Probabilistic Risk Assessment of Manufacturing Activities Within the U.S.Department of Energy
P. Prassinos, P.D. Dilley (USDOE); P. Carrara (Advanced Sciences)

037 Uncertainties and Sensitivities in Physical and Chemical Phenomenology--Explosions and Combustion

Chair: S. Kaplan

Development of Fast-Running Thermal and Structural Response Models for Probabilistic Analyses of Complex Systems
A.S. Benjamin, N.N. Brown (SNL)

The Ignition Temperature of Solid Explosives Exposed to a Fire
J.R. Creighton (LLNL)

Development and Validation of a Vapour Clouds Explosion Blast Model
G. Opschoor, A.C. van den Berg, W.P.M. Mercx (TNO Prins Maurits Lab, Netherlands)

Post-Mortem Risk Modeling of the Mexico City Disaster
G.N. Pettitt, J.D. Harms, J.L. Woodward (DNV Technica)

038 Risk Assessment - Space and Missile Systems

Chair: S. Guarro, The Aerospace Corporation

An Assessment Methodology for SRB Mission Failure Probability
F. Hsu, M.A. Azarm (BNL)

The Development of Risk Profiles for Space and Missile Launch Range Safety Decisions
L.L. Philipson (ACTA)

Risk Assessment Framework for the CASSINI Planetary Mission
S. Guarro (Aerospace Corp.); B. Bream (NASA Lewis)

Risks and Issues in Fire Safety on the Space Station
R. Friedman (NASA Lewis)

039 Expert Judgment

Chair: L.H.J. Goossens, Delft U. Technol.

Method of Expert Judgment Applied to Waste Landfill Performance
Lj. Rodic, L.H.J. Goossens (Delft U. Technol.)

The Acute Toxicity of Hazardous Materials and Expert Judgment
L.H.J. Goossens, R.M. Cooke (Delft U. Technol.); F. Woudenberg, P. van der Torn (Municipal Health Serv., Rotterdam)

A Latent Variable Model in Uncertainty Analysis
A.M.H. Meeuwissen, R.M. Cooke (Delft U. Technol.)

040 Benefits of Understanding Human Errors in Complex Systems

Chair: J. Wreathall, J. Wreathall & Co.

Some Requirements for Designing and Managing Reliable Complex Systems
K.H. Roberts (UC Berkeley); M. Grabowski (Rensselaer Polytechnic U.)

Incorporation of Human Factors into Process Hazard Analysis
D.B. McCafferty, K.A. Borows (DNV Technica)

041 Methods for Improved Operations of Nuclear Units

Chair: K. Jamali, USDOE

The Savannah River Site Component Generic Data Base: Applicable to a Wide Variety of Facilities
C.H. Blanton (Westinghouse Savannah Rvr.); S. A. Eide (LANL)

Risk Based Regulation Configuration Control for the James A. Fitzpatrick Nuclear Power Plant
C.J. Everline, M.G. Stamatelatos, F.M. Quinn (SCIENTECH)

Application of Risk-Based Methods for Inspection of Nuclear Power Plant Systems
S.M. Wong, W.E. Gunther (BNL); J.W. Chung, W.D. Beckner (USNRC)

Assessment of Existing Plant Instrumentation for Severe Accident Management
A.J. Horn, D.E. True (ERIN Eng. & Res.); S. Oh (EPRI)

042 Time Dependent Effects

Chair: D.L. Kelly, INEL

Survey and Evaluation of Aging Risk Assessment Methods and Applications
D. Sanzo, P. Kvam (LANL); G. Apostolakis, J.W. Wu, T. Milici, N. Ghoniem, S. Guarro (ASCA)

Development of High Temperature Metallic Melting Processes Related to the Detritiation of Exhausted Control Rods
G. Modica, H. Dworschak, F. Mannone (CEC-JRC, Ispra); R. Nannicini (ENEA)

Use of Sensitivity Analysis in Selection of Upgrades for Low Seismic Capacity Components for the Advanced Test Reactor
S.T. Khericha, S.A. Atkinson (INEL); D.M. Henry (Tenera); M.K. Ravindra (EQE Intl.)

043 Risk Communication to Professionals

Chair: A.S. Heger, U. New Mexico

How Shall We Measure the Reliability Performance of a Safety System?
P. Hokstad (SINTEF)

The Use of Risk Contours to Clarify Risk Communication
T.E. Fenstermacher (PLG); J.T. Kopecek (Union Oil of Calif.)

Improving NRC Staff Uses of Risk Assessment
M.A. Cunningham, P. Baranowsky, W. Beckner, P. Rathbun (USNRC)

044 Uncertainties and Sensitivities in Physical and Chemical Phenomenology--Radiological Source Terms

Chair: E.J. Bonano, Beta Corp. Intl.

Uncertainties and Sensitivities in Aerosol Calculations - An Analysis of a FIPLOC-M Application to the Experiment VANAM-M2
E. Hofer, B. Krzykacz, J. Langhans, G. Weber (GRS, FRG)

Analysis of Source Term Uncertainty Issues for LWRs
K. Kuramatsu (JAERI)

Source Term Analysis for High Level Waste Storage Accidents
S. Medhekar, J. Kindinger (PLG); D. MacFarlane (LANL)

045 Interactive Fault Detection and Diagnosis--Applications
Chair: M. Modarres, U. Maryland

Applications of Pattern Recognition Techniques to Online Fault Detection
R.M. Singer, K.C. Gross, R.W. King (ANL)

Principal Factor Analysis of the Reactor Coolant Pump System
W.S. Grenzebach (Applied Mgmt. Consultants); T.J. Marx (Marx Soc. Sci. Res.)

FlowSim/FlowRisk - A Code System for Studying Risk Associated with Material Process Flows
A.M. Kaufman (LLNL)

046 Methods for Uncertainty Analysis (I)
Chair: J. Devooght, U. Libre Bruxelles

A New Approach to the Uncertainty Evaluation in Risk Assessment
P. Cecchella, M. Mazzini (U. Pisa)

Uses of Zero-One Sampling in Probabilistic Risk Assessment
A. Camp (SNL)

Coherent Sampling of Multiple Branch Event Tree Questions
A.C. Payne Jr., G.D. Wyss (SNL)

Analysis of Extreme Top Event Frequency Percentiles Based on Fast Probability Integration
B. Staple (SNL); F.E. Haskin (U. New Mexico)

047 Enhancing Safety Culture in Modern Industry
Chair: J. Philley, NUS

Safety Culture: What is it, and How can it be Developed?
D.S. Barnes, S.A. Brearley (AEA Consultancy Services, UK)

Safety Culture and its Reflection in Job and Organizational Design: Total Safety Management
G. Grote, C. Künzler (ETH-Zentrum, Switzerland)

Assessing Organizational Impact on Reactor Safety
W.G. He (PLG)

Concept Safety Review of a Sociotechnical System
G. Wells, C. Phnag (U. of Sheffield, England)

Managing Human Induced Risk Involving Technological Systems and Processes
T.G. Ryan, L.T. Ostrom, D.I. Gertman (INEL)

048 Risk Assessment of Industrial Facilities

Chair: N. Sankaran, UNOCAL

Quantitative Risk Assessment of the Los Alamos National Laboratory TA-55 Plutonium Facility
M.K. Sasser, D. Sanzo (LANL)

Quantitative Risk Analysis of a Butane Storage Facility
L.F.S. Oliveira, J.D.A. Netto, R.A. Pinto (PRINCIPIA Ltda., Brazil); J.C.A. Lima (PETROBRAS, Brazil)

049 External Events

Chair: S.T. Khericha, INEL

Site-Wide Seismic Risk Model for Savannah River Site Nuclear Facilities
S.A. Eide, R.S. Shay (LATA); W.S. Durant (Westinghouse Savannah Rvr.)

Tornado Impact Analysis for Use in Quantitative Risk Assessments
J. Shah (Four Elements Ltd.)

Aircraft Crash Analysis of the Proposed Sizewell B Containment Vessel
Y.F. Al-Obaid (PAAET, Kuwait)

050 Risk Management in DOE (III)

Chair: R.R. Fullwood, BNL

Fully Integrated Risk Management
R.J. Doyle, K. Beierschmitt, (Battelle Pantex)

051 Waste Isolation Pilot Plant--Regulations, Methodology, Modeling and Results

Chair: D.R. Anderson, SNL

Organization of Performance Assessments Conducted for the Waste Isolation Pilot Plant
J.C. Helton (Arizona St. U); D.R. Anderson, M.G. Marietta (SNL)

Using Data and Information to Form Distributions of Model Parameters in Stochastic Simulations of Performance of the Waste Isolation Pilot Plant (WIPP)
M.S. Tierney (SNL)

Modeling System Used for the Performance Assessment for the Waste Isolation Pilot Plant (WIPP)
M.G. Marietta, M.S. Tierney (SNL); J.C. Helton (Arizona St. U.)

Regulatory and Institutional Considerations in Performance Assessment for the Waste Isolation Pilot Plant (WIPP)
D.R. Anderson, M.G. Marietta (SNL)

052 Software Dependability (II)

Chair: R. Mulvihill, PRC

The Dynamic Flowgraph Methodology: A Methodology for Assessing Embedded System Software Safety
C. Garrett, M. Yau, S. Guarro, G. Apostolakis (UCLA)

Determining the Prime Implicants for Multi-State Embedded Systems
E. J. Shields, G. Apostolakis, S.B. Guarro (UCLA)

053 Expert Judgment in Assessment Studies

Chair: M.A. Cunningham, USNRC

An Application of ISPA: Sensitivity Analysis on Complex Engineering Problem
P. McClure, S. Clement, S. Ashbaugh (SAIC)

The Analysis of Competing Failure Modes
R.M. Cooke (Delft U. Technol.)

Practical Problems in Aggregating Expert Opinions
J.M. Booker, R.R. Picard, M.A. Meyer (LANL)

An Application of Expert Opinions Approach in Combining Measurement Results
M. Haim, M. Jaeger, D. Tzidony (RAFAEL, Israel)

054 HRA, the Second Generation (I)

Chair: P.C. Cacciabue, JRC

Some Thoughts on the Requirements for a Second Generation Human Reliability Assessment Process
A.J. Spurgin

The Need for, and a Proposed Structure of, a Second Generation HRA
G.W. Parry (NUS)

055 Instrumentation and Control Reliability

Chair: R. Roberts, Ultramar

Reliability-Based Design of a Safety-Critical Automation System - A Case Study
C.W. Carroll (Boeing); W. Dunn (USC); L. Doty, M. Hulet (NASA); M.V. Frank (Safety Factor Assoc.)

Safeguards Actuation Fault Tree Analysis
M. Cepin, M. Kozuh, B. Mavko (J. Stefan Inst.)

Reliability Assessment of Onsite Emergency Safety Buses at Operating Nuclear Power Plants
G. Martinez-Guridi, M.A. Azarm (BNL)

Optimal Voting Logic of Hydrocarbon Gas Detectors Based on Field Data
L. Bodsberg (SINTEF)

056 Risk Communication

Chair: R.A. Bari, BNL

Risk Assessment - Working with Your Client
K.G. Murphy, J.E. Fitzgerald, Jr. (DOE)

057 Resource Planning and Value-Impact Applications

Chair: K. Klein, USDOE

Environment, Safety & Health Risk Management: Program Planning and Budget Decision-Making
F.E. Tooper (USDOE); J.L. Von Herrmann (CYCLA)

Control Operator Overload: Identification and Prevention
D.A. Strobhar (Beville Eng.)

Probabilistic Cost-Benefit Analysis of Enhanced Safety Features for Strategic Nuclear Weapons at a Representative Location
D.R. Stephens, C.H. Hall, G.S. Holman, K.F. Graham, T.F. Harvey, F.J.D. Serduke (LLNL)

058 Examples of PRA in Design Decisions

Chair: B. Buchbinder, NASA

Examples of the Use of PSA in the Design Process and to Support Modifications at Two Research Reactors
D.H. Johnson, D.C. Bley, J.C. Lin (PLG); C.T. Ramsey, M.A. Linn (ORNL)

Risk Management and Corrective Actions
R.A. Dykes, A.A. Dykes (PLG); J.D. Blodgett (Hughes)

A Risk and Decision Analysis for Choosing Wind Tunnel Turbine Blade Strategies
M.V. Frank, S.A. Epstein (Safety Factor Assoc.)

Investigation Into the Development of A Train-Level Probabilistic Risk Assessment
C.L. Smith, R.D. Fowler, L.M Wolfram (INEL)

059 Use of PRA Models in Assessing Technologies and Device Applications

Chair: M. Zentner, Westinghouse Hanford

The Use of Robotics and Probabilistic Risk Assessment in Environmental Restoration
L.E. Cindel, G. Apostolakis (UCLA)

Risk Evaluation of Medical and Industrial Radiation Devices
E.D. Jones (LLNL), R.E. Cunningham, P.A. Rathbun (USNRC)

Integrated Systems Performance Assessment
C.N. Amos, S.D. Clement (SAIC)

060 HRA, the Second Generation (II)

Chair: E. Hollnagel, Computer Resources Intl.

Reliability of Cognition, Context and Data for a Second Generation HRA
E. Hollnagel (HRA, UK); P.C. Cacciabue (CEC/JRC, Italy)

Elements Of A Model of Operator Problem Solving and Decision Making in Abnormal Conditions
S-H. Shen, C. Smidts, A. Mosleh (U. Maryland)

Human Reliability Analysis Using Simulated Human Model
Y. Fujita, I. Yanagisawa (MAPI, Japan); H. Sakuda (NUPEC/IHF, Japan)

061 Transportation Risk (I)

Chair: T. Altenbach, LLNL

The Cost of Human Error Intervention
C.T. Bennett, W.W. Banks, E.D. Jones (LLNL)

Application of the DOE and NRC Nuclear Safety Policy to Transportation Operations
C.Y. Kimura (LLNL), G.M. Sandquist (U. Utah)

Control of Risk from Explosives Stores Within Mod (UK)
J. Connor, D. Hewkin (Ministry of Defence, UK)

062 Environmental Risk Management--Waste

Chair: C. Peabody, USDOE

The Role of Multimedia, Multi-Pathway Exposure Assessments in Risk-Based Regulations at California Hazardous Wastes Sites
T.E. McKone (LLNL), E.G. Butler, J.J. Wong (Calif. Dept. Toxic Substances Control)

Risk Analysis for New Nuclear Waste Sites - Will It Generate Public Acceptance?
H. Inhaber (Westinghouse Savannah River)

063 Methods for Uncertainty Analysis (II)

Chair: A. Camp, SNL

Development of Smart Searching Algorithms for Vulnerability and Uncertainty Analysis in Probabilistic Risk Assessments
A.S. Benjamin (SNL)

Importance and Sensitivity Analysis in Assessing the System Reliability
Y.-F. Wu (Taiwan Power Co.), J.D. Lewins (Cambridge U.)

Multiple Weight Stepwise Regression
J. Atkins (UC Berkeley); J. Campbell (SNL)

A Software System for Probabilistic Uncertainty and Sensitivity Analysis of Results from Computer Models
B. Krzykacz, E. Hofer, M. Kloos (GRS)

064 Risk Based Prioritization

Chair: G.E. Cummings, LLNL

Prioritizing Risk-Reducing Activities: Integrating Risk Management Into Business Planning
D. Brooks (Arizona St. U)

An Integrated Resource Management System and the Risk-Based Prioritization Model in Use at Martin Marietta Energy Systems
M.I. Sparks (Martin Marietta)

Risk-Based Prioritization: A Comparison of Approaches
R.S. Strait (LLNL)

065 Meaning and Interpretation of Probability

Chair: A. Mosleh, U. Maryland

The Meaning and Use of Probability in Probabilistic Safety Assessment
G.W. Parry (NUS)

Is Probability of Frequency Too Narrow?
H.F. Martz (LANL)

On Bayesian Approaches of Parametric and Modeling Uncertainty
J.S. Wu (ASCA)

On The Objectivity of Subjective Theory of Probability for PSA Applications
A. Mosleh (U. Maryland)

066 Cognitive Modeling and Simulation in Human Reliability Analysis

Chair: Y. Fujita, Mitsubishi Atomic Pwr. Ind.

A Simulation Study of Errors of Commission in Nuclear Accidents
K-S. Hsueh (NUS); L. Soth (Commonwealth Ed.); A. Mosleh (U. Maryland)

Simulating Operator Cognition for Risk Analysis: Current Models and CREWSIM
V.N. Dang (MIT); N.O. Siu (INEL)

Quantification of Multiple Error Expressions in Following Emergency Operating Procedures in Nuclear Power Plant Control Room
A.P. Macwan, P.S. Wieringa (Delft U. Technol.); A. Mosleh (U. Maryland)

067 Comparative Risk Assessment of Complex Technological Systems (I)

Chair: S. Haddad, New South Wales Govt.

Severe Accidents in Comparative Assessment of Energy Sources: Current Issues and Actual Experience Data
S. Hirschberg, C. Parlavantzas (P. Scherrer Inst., Switzerland)

An Analysis of Electricity Generation Health Risks: A United Kingdom Perspective
D.J. Ball, L.R.J. Roberts, A.C.D. Simpson (U. East Anglia, England)

External Costs as an Indicator for Comparative Risk Assessment of Different Energy Systems - A Case Study for Comparing the Nuclear and the Coal Fuel Cycle
W. Krewitt, P. Mayerhofer, R. Friedrich, A. Greβmann (U. Stuttgart, Germany); M. Dreicer (CEPN, France)

The Use of Multi-Attribute Analysis for Comparing the Health and Environmental Impacts of Different Fuel Cycles - A Feasibility Study for the Comparison Between Coal and Nuclear Fuel Cycles
M. Dreicer, P. Kuentzmann, T. Schneider (CEPN, France); W. Krewitt (U. Stuttgart, Germany)

068 Risk Assessment Failure Data Estimation

Chair: C. Fleming, PLG

Advanced Test Reactor Large LOCA Frequency Estimation
S.T. Khericha (INEL); S.A. Eide (LATA)

Component Failure Rate Comparison and Recommendations for Various Processing Fluids
L.C. Cadwallader, J.N. Wilkinson (INEL); S.A. Eide (LATA)

Application of Reliability-Centered-Maintenance to PRA Fault Tree Analysis for a BWR HPCI System
M.A. Feltus, Y.A. Choi (Penn. St. U)

069 Waste Risk Management

Chair: B. Thompson, H.M. Insp. Pollution

The HMIP Research and Development Programme for Post-Closure Risk Assessment
B. Thompson (HMIP, UK)

Risk Analysis In Regulation and Risk Communication
S.M. Stearn (HMIP, UK)

Validation: What Should a Regulator Look for in a Safety Case?
R.D. Wilmot, D.A. Galson (Galson Sciences, England)

Aspects of Review of a Proponent's Post-Closure Safety Assessment on Behalf of the Regulator
T.J. Sumerling (Safety Assessment Mgt.); D. Read (WS Atkins Sci. & Technol.)

070 Reactor PSA Studies

Chair: M. Hitchler, Westinghouse Savannah Rvr.

Probabilistic Safety Analysis of Ignalina NPP, RBMK-1500
G. Johansson (IPS); E. Shiverskly (IPE); E. Söderman (ES-Konsult)

Results and Insights from the Low Power and Shutdown Level 1 PRA of the Grand Gulf Nuclear Power Station
D.W. Whitehead, B.D. Staple, S.L.Daniel (SNL); J. Darby (Sci. & Eng. Assoc.); J. Yakle, S. Miller, J. Forester (SAIC)

Comparative Evaluation of the Performance of Advanced Semi-Passive Pressurized Water Reactors in the Loss of Offsite Power Event
M. Ouyang, M. Golay (MIT)

071 Accident Precurssors

Chair: V.M. Bier, U. Wisc.-Madison

Accident Sequence Precursor Methodology for Maritime Safety
L.H.J. Goossens (Delft U. Technol.); C.C. Glansdorp (Marine Analytics)

Developing Organizational Safety Information System for Monitoring Potential Dangers
M. Tamuz (U. Texas)

The Performance of Precursor-Based Estimator
V.M. Bier, W. Yi (U. Wisc.)

072 Aging Analysis: Methodology & Applications

Chair: D.H. Johnson, PLG

Sensitivity and Uncertainty Analyses in Aging Risk-Based Prioritizations
M. Hassan, S. Uryas'ev (BNL); W.E. Vesely (SAIC)

Bayesian Aging Analysis of Hanford Waste Storage Tank Leak
W.G. He, S.B. Rao (PLG); D.R. MacFarlane (LANL)

Lifetime Prediction and Physical Asset Management
R. Menich (Failure Analysis Assoc.)

073 Human Reliability Applications and Models

Chair: S. Kondo, Tokyo Univ.

Human Reliability Analysis for Surry Midloop Operations
J.C. Lin, D.C. Bley, D.H. Johnson (PLG); T-L. Chu (BNL)

Enhancing Conditions for Correct Human Actions at the Ignalina Nuclear Power Plant in Lithuania
P. Holmgren (RELCON)

Human Error Model Development for Savannah River Site Nonreactor Facilities
R.E. Vail, H.C. Benhardt, J.E. Held, L.M. Olsen (Westinghouse Savannah Rvr.); S.A. Eide (LATA)

Benchmarking an Automated Human Error Analysis Technique
J. Wilson, P. Cloutier, S. Fogarty (Westinghouse Idaho Nucl.)

Assessment of Dependence of Human Errors in Test and Maintenance Activities
L. Reiman (STUK, Finland)

074 Comparative Risk Assessment of Complex Technological Systems (II)

Chair: S. Hirschberg, P. Scherrer Inst.

Comparative Assessment of the Health and Environmental Impacts of Various Energy Systems from Severe Accidents: Issues in Review
A.V. Gheorghe (ETH, Switzerland)

Consideration of Probabilistic Safety Objectives in OECD/NEA Member Countries
M.F. Versteeg (Nucl. Safety Insp., Netherlands)

Risk Assessment of Large Industrial Complexes in Eastern Europe: A Comparative Prospective
A.V. Gheorghe (ETH, Switzerland)

075 Fire Risk Analysis for Enineered Systems

Chair: R. Friedman, NASA Lewis

Risk Analysis of Environmental Hazards at the High Flux Beam Reactor
J.L. Boccio (BNL), V.S. Ho, D.H. Johnson (PLG)

A Model for Fuel Fire Duration and Application to the B-1B Bomber
D.E. Magnoli (LLNL)

Implementation of the FIVE Methodology: Results and Lessons Learned
R.C. Lindquist, M.S. Powell (Arizona Pub. Serv.)

Fire Risk Assessments at Rocky Flats Plant
T.L. Foppe, E. Stahlnecker (EG&G Rocky Flats)

076 Risk-Based Regulation (I)

Chair: V. Joksimovich, Accident Prevention Group

Application and Extension of Formal Decision-Making Methods to Generic Safety Issue Decisions
M.P. Bohn (SNL)

Risk-Based Regulation Using REVEAL
H. Dezfuli, J. Meyer (SCIENTECH); M. Modarres (U. Maryland), H. Specter (RBR Conslts.)

078 Process Safety Management

Chair: R.L. Cummings, Interstate Assessment Technologies

Integrating Compliance Efforts for Process Safety Management Regulations
D.A. Moore (Primatech)

OSHA PSM: Impact on Accident/Incident Investigation
D.A Wetzel, S. Hall (Wetzel, Herron & Drucker); R.E. Rimkus, J.C. Clark (Rimkus Consulting)

079 Impact of Different PRA Methodologies on the Results of Nuclear Power Plant PSAs (I)

Chair: F.R. Hubbard, FRH

Risk Assessment Impacts on Risk Management
K.I. Kiper (N. Atlantic Energy Service)

Comparison of PRA Event Tree Approaches - Some Thoughts and Reflections
D.M. Rasmuson (USNRC)

On Encountering Small Numbers: How Good Models Go Bad
D.C. Bley, D.H. Johnson (PLG)

Completeness and Complexity of PSA: Do They Need it?
A.D. Chambardel, L. Magne (EDF, France)

080 Understanding Organization Factors Through Risk Models

Chair: J.H. Gittus, British Nuclear Industry Forum

An Approach for Incorporation of Organizational Factors into Human Reliability Analysis in PRAs
P. Moieni, D.D. Orvis (Accident Prevention Grp.)

The Work Process Analysis Model (WPAM): An Integrated Approach to the Incorporation of Organizational Performance into Probabilistic Safety Methodology
K. Davoudian, J-S. Wu, G. Apostolakis (UCLA)

Risk Assessment - Including the "CHAOS" Factor
C.T. Kleiner (C.T.K. Enterprises); R.L. Cummings (Interstate Assessment Tech.)

081 DOE Safety Studies

Chair: R.E. Hall, BNL

An SAR Issue for the Savannah River Reactors Resolved with PRA Methods
S.V. Topp (Westinghouse Savannah Rvr.)

Evaluation of Replacement Tritum Facility (RTF) Compliance with DOE Safety Goals Using Probabilistic Consequence Assessment Methodology (U)
K.R. O'Kula, J.M. East, M.L. Moore (Westinghouse Savannah Rvr.)

Fault Tree Analysis on the F&H Canyon Exhaust Systems at the Savannah River Site
J.M. Low, K. Marshall (Westinghouse Savannah Rvr.)

082 Fires, Floods, and Spatial Interactions

Chair: R. Oehlberg, EPRI

Fermi Internal Flood Analysis Using a Component-Based Frequency Calculation Approach
J.C. Lin, Y.M. Hou (PLG); J.V. Ramirez, E.M. Page (Detroit Edison)

Advances in the Methodology for the Analysis of Location-Dependent Hazards for Probabilistic Risk Assessment (PRA)
J.K. Liming, L.A. Bennett (ERIN Eng. & Res.)

Location Transformation for Identification and Screening of Internal Fire and Flood Scenarios
T.A. Thatcher, J.L. Jones (INEL); S.A. Eide (LATA)

EPRI Fire Events Database
K. Bateman, M. Marteeny, B. Najafi, B. Parkinson (SAIC); R. Oehlberg (EPRI)

083 Environmental Restoration Decision Support System

Chair: D. Rice, LLNL

Application of Decision Support Systems to Environmental Restoration Processes
D.W. Rice, J. Ziagos (LLNL); D. Bell (UCLA)

The SEDSS - A Risk Assessment Based Decision Support Tool
R. Knowlton Jr., E. Webb (SNL)

Environmental Decision Support Systems
J. Coleman (USEPA); J. Franco, W. Wee (U. Cincinnati)

084 Reliability Based Design in Structural Engineering

Chair: D. Frangopol, U. Colorado

Time-Dependent Reliability of Rock-Anchored Structrues
M. Chakravorty, J.E. Pytte, D.M. Frangopol (U. Colorado); R.L. Mosher (USAE Waterways Exp. Station)

Reliability Analysis of Redundant Structures by Response Surface Method
Y. Murotsu, S. Shao (U. Osaka, Japan); N. Chiku (Kawasaki Heavy Ind., Japan)

Risk Analysis of Pipeline Systems Based on Structural Reliability Models
M.Sinisi, G.M. Uguccioni, M. Tominez (SIAF, Italy)

085 Transportation Risk (II)

Chair: M. Kazarians, Kazarians & Assoc.

A Zone Model for Determining Atmospheric Contaminant Transport Aboard Human-Crewed Spacecraft
S. Jones, M. Paul, F. Issacci, I. Catton, G. Apostolakis (UCLA)

Commercial Space Transportation Regulation: An Evolution in Risk Management
R.K. Gress, D.E. Lang (USDOT)

System Safety Management in the UK Air Traffic Services
R. Profit (Natl. Air Traffic Services)

086 Impact of Different PRA Methodologies on the Results of Nuclear Power Plant PSAs (II)

Chair: J.H. Bickel, INEL

The Search for Dependencies or How Could Two Current Design Nuclear Power Plants Produce IPE Results Three Orders of Magnitude Different?
F.R. Hubbard (FRH); A. Mosleh (U. Maryland)

Impact of Methodology and Design Changes on Turkey Point IPE Results
C.N. Guey, W.A.Skelley (Florida Pwr. & Lt.)

087 Causal Factors in Human Reliability: Experiments and Databases

Chair: A.A. Dykes, PLG

On the Use of Data Collected During Crew Reliability Experiments at PAKS Nuclear Power Plant - Status Report
A.Bareith, Z. Karsa (Inst. for Electric Pwr. Res.); A.J. Spurgin; I. Kiss (Nucl. Pwr. Plt. of Paks); L. Izso (Tech. U. Budapest)

Causal Identification of Human Errors Towards Intelligent CAI System for Plant Operation
Y. Furuhama, K. Furuta, S. Kondo (U. Tokyo)

Development of a Human Error Data Bank
S.E. Taylor-Adams, B. Kirwan (U. Birmingham, England)

Causal Factors of Operator Unreliability: An Application of Simulator Data
D. Orvis, P. Moieni (Accident Prevention Grp.); A.J. Spurgin

088 Risk Based Methods for Reliability/Availability/Maintainability

Chair: S. Lydersen, Norwegian Inst. Technol.

Some New Measures of Reliability Importance with Applications to Reliability Centred Maintenance
S. Lydersen (Norwegian Inst. Technol.)

"INTEGRIT" - A Parametric Reliability and Maintainability Methodology and Safety Risk Management Tool
R. Vote, T. Barritt, R. Blanchford (ELINTECH)

On-Line VS. Off-Line Maintenance in Nuclear Power Plants - Insights from a Cycle-Wide O&M Cost Model
J.R. Hewitt, L.A. Bennett, R.L. Durling (ERIN Eng. & Res.)

A User-Friendly Program for System and Component Availability Monitoring and Its Potential Application in Maintenance Rule Implementation
D.M. Kapinus (Commonwealth Edison); T.A. Petersen (NUS)

089 Seismic Risk Analysis

Chair: D.A. Moore, Primatech

The Experimental Breeder Reactor II Seismic Probabilistic Risk Assessment
J. Roglans, D.J. Hill (ANL)

Seismic Risk Management Using Earthquake Injury Epidemiology
P.J. Amico, T.A. Haley, S.J. Krill (SAIC)

090 Risk Based Regulation (II)

Chair: G. Apostolakis, UCLA

Regulatory Decision Making by Decision Analysis
J. Holmberg, U. Pulkkinen (Tech. Res. Ctr. Finland); L. Reiman, R. Virolainen (Finnish Ctr. for Radiat. & Nucl. Saf.)

Application of Risk-Based Priortization to QA Requirements
F.J. Rahn, W. Parkinson (EPRI); G.D. Bouchey (SAIC); M. Meisner (Entergy Operations)

091 Management Issues

Chair: D. Cunha, Northrop Corp.

"Risk Index" - A Proposed Concept
S. Chakraborty (Swiss Fed. Nucl. Saf. Insp.); C. Preyssl (European Space Agency)

The Quality Issues of Technologic Risk Assessment
B.O.Y. Lydell (RSA Technologies)

092 Industrial and Transportation Risks

Chair: D. Henneke, TENERA

The ARIPAR Project: Analysis of the Industrial and Transportation Risk Connected with the Ravenna Area

D. Egidi (Civil Protection, Emilia Romagna Region); F. Foraboschi, G. Spadoni (U. Bologna); A. Amendola (CEC-JRC)

Identification and Evaluation of Maritime Exposures

J.L. Borrello, M.J. Spansel (Adams & Reese)

A Decision Model of a Multi-Point Mooring of a Tanker with a Tug Assist

M.L. Eskijian (Calif. St. Lands Commis.)

093 Time Dependence of Equipment Failure Rates-- Models, Data, and Impacts on System Modeling

Chair: D. Bley, PLG

On a Class of Dependent Failures

I. A. Papazoglou (National Center for Scientific Research, Greece)

Statistical Treatment of Time and Demand-Related Failures in the Nordic Reliability Data Book (T-Book)

K. Porn (Studsvik Eco & Safe)

Derivation of Time Dependent Component Unavailability Models and Application to Nordic PSAs

M. Knochenhauer (Logistoca Consult.); G. Johanson (Ind. Process Safety)

094 Applications of Human Reliability Analysis

Chair: D.I. Gertman, INEL

HRA for Explosive Ordinance Disposal

L.N. Haney, R.G. Peatross, D.I. Gertman (INEL)

Nuclear Case Study for A SGTR Sequence

D.I. Gertman,W.J. Reece, M.B. Calley, C.L. Smith (INEL)

Insights into Pilot Situation Awareness Using Verbal Protocol Analysis

H. Blackman, C. Sullivan, K. Seidler (INEL)

095 Risk Methods for Defense Applications

Chair: M.V. Frank, Safety Factor Assoc.

Probabilistic Risk Assessment of Weapon-Systems Field-Testing: Accounting for System's Complexity and Unfamiliarity
S. Feller, M. Maharik (RAFAEL, Israel)

Nuclear Weapon System Risk Assessment
D.D. Carlson (SNL)

Probabilistic Risk Assessment of Disassembly Procedures
D.A. O'Brien, T.R. Bement, B.C. Letellier (LANL)

096 Risk Communication to the Public

Chair: M.E. Paté-Cornell, Stanford U

Effectively Communicating Risk to the Public and to Regulators: Can It Be Accomplished?
G.M. Pilie, G.T. Croxton (Adams & Reese)

Effectively Communicating Risk Assessments to the Public
C. Lambert, M. McDaniel (UNOCAL); S. Santos (FOCUS Grp.)

097 Broad Risk Perspectives Within the DOE Weapon Complex

Chair: H.P. Alesso, LLNL

A Global Overview of Risk Management of the DOE Complex
H.P. Alesso, K.C. Majumdar (LLNL)

The Integration of Human Factors into the Risk Assessment of a Nuclear Device Arming and Firing System
T. Altenbach, W. Ferrell (LLNL)

A Method for Determining Risk to Ground Facilities form Aircraft Accidents
C.Y. Kimura, C.T. Bennett (LLNL)

098 Risk Management - International Space Applications

Chair: C. Preyssl, European Space Agency

Risk Assessment - The European Space Agency Approach
C. Preyssl (European Space Agency)

Risk Management of the Japanese Experiment Module on Space Station Freedom
J.C. Lin, D.H. Johnson, W.R. Fuller (PLG); K. Sakata, H. Suzuki, S. Kojima (Mitsubishi Atomic Pwr. Ind., Japan); H. Himeno (Mitsubishi Heavy Ind., Japan)

Rocky the Rover: PRA Meets ET
M.V. Frank, S.A. Epstein, A.J. Spurgin (Safety Factor Assoc.)

099 Root Cause and Precursor Analysis
Chair: M.G.K. Evans, NUS

The Barseback Incident - A Precursor Challenging Fundamental Safety Principles of LWRs
L. Carlsson, S. Erixon, C. Karlsson, B. Liwang, J. Olsen (SKI); G. Johanson (Ind. Proc. Saf.)

Inferring Safety Trend From The Accident Sequence Precursor Analysis Program
M. Modarres (U. Maryland)

Estimating the Frequency of Electrical Overload Events in the Proposed Space Station
T. Paulos, F. Issacci, I. Catton, G. Apostolakis (UCLA)

100 Reducing Errors through Quality and Design
Chair: T.G. Ryan, INEL

The Pros and Cons of Using Human Reliability Analysis Techniques to Analyze Misadministration Events
L.T. Ostrom (INEL)

Construction Error and Human Reliability for Structural Systems
M.G. Stewart (U. Newcastle)

The Feasibility of Designing Human-Error Backup Systems for Fail-Safe Structures
Y. Sato (Tokyo U.); K. Inoue (Kyoto U)

A Methodology to Support Space System Designer in Minimizing Human Error
M. Ferrante, C. Vivalda (Alenia Spazio); C. Fogli (ESA/ESTEC)

101 Risk Assessment of Nuclear Waste Storage and Processing

Chair: D. Stack, LANL

PSA Results for Hanford High-Level Waste Tank 101-SY
D.R. MacFarlane, T.F. Bott, L.F. Brown, D.W. Stack (LANL); J. Kindinger, R.K. Deremer, S.R. Medhekar, T.J. Mikschl (PLG)

102 Fire Risk

Chair: V. Ho, PLG

Development of the Fire Risk Analysis Methodology for Nuclear Power Plants
T. Matsuoka, K. Miyazaki (Ship Res. Inst., Japan); M. Kondo (JAERI, Japan)

A Methodology for Quantifying Fire Risk On-Board Spacecraft
K.R. Paxton, F. Issacci, G. Apostolakis, I. Catton (UCLA)

103 Risk-Based Regulation (III)

Chair: F. Rahn, EPRI

Where Do We Go from Here in U.S. Nuclear Safety Regulation?
V. Joksimovich (Accident Prevention Grp.)

The Use of Probabilistic Risk Assessment in Satisfaction of the Nuclear Regulatory Commission's Maintenance Rule
R.M. DuBord, M.W. Golay (GE Nuclear Energy); N.C. Rasmussen (MIT)

The Beneficial Use of Risk Analysis in the Regulatory Process
M.V. Bonaca, D.A. Dube, S.D. Weerakkody (Northeast Utilities Serv.)

104 Industrial Risk Management - An EEC Perspective

Chair: D.M. Karydas, Factory Mutual Res. Corp.

Industrial Risk Management: An EEC Perspective
A. Amendola (CEC-JRC, Ispra)

Plant Level Hazard Identification Based on Functional Models
J. Suokas (VTT, Finland)

Decision Making in Process Design - Assessment of Total Safety by Aggregating the Safeties of the Subparts of the Process

R. Koivisto (VTT, Finland), V.J. Pohjola, M.K. Alha (U. Oulu, Finland)

Short Cut Risk Assessment
G. Wells (U. Sheffield, UK); S. Allum (Bowring Marsh & McLennan, UK)

105 Environmental Risk Management--Restoration

Chair: T.E. McKone, LLNL

Scope Definition for the Hanford Tank Farms PRA
J.P. Kindinger (PLG), D.W. Stack (LANL)

Risk Management Applications at the INEL for Advanced Test Reactor Operations and Safety and Environmental Restoration and Waste Management
S.A. Atkinson, R.L. Nitschke (INEL)

Decision Analysis in Environmental Risk Management: Evaluating Multiple Stakeholder/Multiple Objective Decisions
D.C. Bell, G. Apostolakis, W.E. Kastenberg (UCLA)

106 Data Collection and Evaluation

Chair: D. Croucher, EG&G Rocky Flats

Risk Assessment Data Banks at the Savannah River Site (U)
C.S. Townsend, W.S. Durant, D.F. Baughman (Westinghouse Savannah Rvr.)

Data Worth Analysis for Performance Assessment Using Influence Diagrams
J.E. White (INTERA), A.S. Heger (U. New Mexico)

Integrated Risk Management Database Systems
H. Wilhite, J.R. Pearson (CYCLA)

107 Organizational Factors and Nuclear Power Plant Safety

Chair: K. Dahlgren, Swedish Nucl. Pwr. Insp.

Organizational Factors and Nuclear Power Plant Safety: A Process Oriented Approach
K. Dahlgren (SNPI, Sweden); J. Olson (Battelle)

Organizational Assessment of a Maintenance Department at a Nuclear Power Plant
L. Reiman (STUK, Finland), L. Norros (VTT, Finland)

Evaluation of Quality Systems
I. Blom (SNPI, Sweden), B. Melber, N. Durbin (Battelle)

Two Solutions to the Same Problem - Assessing Processes and Their Outcomes
G. Svensson (SNPI, Sweden)

108 Interactive Fault Detection and Diagnosis--Approaches

Chair: A. Poucet, ITER EDA

Development of Diagnosis Systems of Autonomous Operation System for Nuclear Power Plants
A. Saiki, K. Okusa, A. Endou (PR& NFD Corp., Japan)

A Unified Paradigm for Verifying Reliability Requirements in Dynamic Systems
J. Ruiz, M.Roush (U. Maryland)

Towards a Toxanomy of System Failures
J. Ruiz, M. Modarres (U. Maryland)

001 Risk Based Prioritization (I)

Chair: P. Prassinos, USDOE

Qualitative Safety Analysis of Proposed Material Relocation Options
N.G. Cathey, T.L. Foppe (EG&G)

Risk-Based Methods Applicable to Ranking Conceptual Designs
R.J. Breeding, J.T. Ringlnad, K. Ortiz (SNL), J.J. Lim (Lim & Orzechowski)

Process Hazards Assessment Using Risk Matrices
D.H. Henneke, J. Phillips (TENERA)

QUALITATIVE SAFETY ANALYSIS OF PROPOSED MATERIAL RELOCATION OPTIONS

Nathan G. Cathey and Terry L. Foppe

Nuclear Safety Engineering Department
EG&G Rocky Flats, Inc.
P.O. Box 464, Building T886B
Golden, CO 80402-0464

ABSTRACT

This paper presents the methodology used to perform a qualitative safety analysis of various options proposed for the relocation of Special Nuclear Material from its present locations to other areas of the Rocky Flats Plant. This analysis determined the relative risk ranking of various proposed relocation options considering the probability and consequences of accidents associated with the material handling, transportation, and storage locations. Of the five options, two groupings of results were concluded to be significantly different, allowing the decision makers to balance risk issues with their other requirements (e.g., security, schedule, etc.).

INTRODUCTION

The Rocky Flats Plant (RFP) is a government-owned and contractor-operated facility, which is part of the nationwide nuclear weapons production complex managed by the U.S. Department of Energy (DOE). EG&G Rocky Flats, Inc., is the prime operating contractor. RFP is located in Colorado about 16 miles northwest of downtown Denver.

Building 991 at the RFP was designed and built in the early 1950's with underground vaults for interim storage of Special Nuclear Material (SNM). Material stored in areas of the Building 991 complex were to be relocated to other buildings at RFP (e.g., Building 371), or to a highbay area of Building 991 located in the above ground structure. This material relocation was deemed necessary due to seismic structural concerns in the tunnels leading to the vaults, and due to minor water seepage in the vaults.

Based upon the decision to relocate this material, various material relocation options were proposed. Factors such as risk, facility safety envelope issues (i.e., Safety

Analysis Report [SAR] and Operational Safety Requirements [OSR]), personnel radiation exposures, safeguards and security issues, vault upgrading in other locations, and schedule needed to be considered in the decision making process. Five options were identified for evaluation, including four relocation options and the no action alternative of leaving the SNM in place. These issues were considered by the 991 Material Relocation Management Team, senior EG&G Rocky Flats management, and the DOE in selecting the most efficient option to be implemented.

METHODOLOGY

The analysis performed qualitatively addressed the risk (i.e., the probability and consequences of potential accidents) associated with the various options. For this decision making process, detailed quantitative information was not necessary. A qualitative safety analysis providing the relative risk between the options provided sufficient information for presenting the risk related issues.

The risk of an activity or operation is generally determined by analyzing the various accidents that could lead to a release of hazardous material. The hazardous material which could be involved in an accident is primarily plutonium, although uranium, americium, and other hazardous materials could be involved. For each of these accidents, a frequency of occurrence with an associated consequence is determined. The expected value of risk associated with an accident is the product of its frequency and consequence. The total risk associated with a facility is the sum of risk from the various accidents.

For this analysis, a similar process was employed, although at a much more qualitative level. The analysis method was similar to the Delphi procedures used to obtain data from experts. The team was comprised of seven senior nuclear safety personnel experienced in system analysis, safety analysis, accident analysis, fault tree analysis, event tree analysis, component failure rates, radiological consequence assessment, probabilistic risk assessment, criticality analysis, and RFP operations.

For each proposed option, various accident categories as shown in Table 1 were evaluated with regard to frequency of occurrence and associated consequences. The accident categories of general flood, tornado, snow, lighting, and aircraft crash were excluded since they are considered low risk contributors (i.e., they have low frequency and/or low consequence values) per previous risk assessments performed for SARs and the Rocky Flats Plant (RFP) Final Environmental Impact Statement (FEIS).

This evaluation consisted of assigning both a frequency of occurrence and a consequence ranking to an accident category for a specific option. The frequency and consequence for an option were assigned a ranking relative to other material relocation options, as shown in Tables 2 and 3 respectively. The frequency ranking and the consequence ranking were then multiplied together to produce a risk ranking for that accident category for that option. Since the frequency and consequences are relative between the options, the result of this process is a relative risk ranking. The larger the risk ranking product, the greater the risks. It should be noted that the risk rankings presented here do not embody the usual risk units of "consequence per year" such as rem/year or latent cancer fatalities/year.

Table 1. Accident categories considered in qualitative risk analysis.

Transporation	This category considered those accidents which may occur during the transportation of the material from one building to another. This did not consider intra-building movements.
Seismic	Consideration of release of material due to the occurrence of a seismic event. Susceptibility of the material in its temporary location and new location were considered. Also considered was the displacement of material to other locations.
Fire	Consideration of the potential for fire accidents to occur and their associated consequences. Susceptibility of the material in its temporary location and new location were considered. Also considered was any displaced material relocation.
Explosion	Consideration of the potential for explosion related accidents to occur and their associated consequences. Susceptibility of the material in its temporary location and new location were considered. Also considered was any displaced material relocation.
Spill	Consideration of the potential for spill of radioactive material to occur and the associated consequences. Items considered was rupture of the container due to movement and penetration due to an accidental discharge of a weapon by a Security Inspector. Susceptibility of the material in its temporary location and new location were considered. Also considered was any displaced material relocation.
Criticality	Consideration of the potential for an inadvertent criticality to occur either during the movement of material or in its new location. Susceptibility of the material in its temporary location and new location were considered. Also considered was any displaced material relocation.
ALARA	This category considered the estimated person-Rem expended to perform the material relocation for each option.

Table 2. Frequency Ranking Guide.

Rank	Descriptor	Approximate frequency (f) per year
0	Impossible	
1	Incredible	$f < 10^{-6}$
3	Highly Unlikely	$10^{-6} < f < 10^{-4}$
5	Unlikely	$10^{-4} < f < 10^{-2}$
7	Expected	$10^{-2} < f < 1$
9	Routine	$f > 1$

This table is used to assign a frequency ranking based on the assessed accident category frequency. Even number rankings were also assigned if the rating fell between those defined above.

Table 3. Consequence Ranking Guide.

Rank	Descriptor or Ranking Scale Comparison
0	No consequence to worker or public.
1	Consequences comparable to that of a flood or snow accident.
2	Consequences comparable to that expected from a tornado or extreme wind accident.
3	Consequences comparable to a criticality with no workers in the immediate vicinity.
4	Consequences comparable to that associated with a spill in the building or an earthquake which is mitigated by functional safety systems.
6	Consequences comparable to that of a fire in a building that is filtered.
8	Consequences comparable to an in-building explosion that is filtered.
10	Consequences comparable to an unfiltered release such as a dock or truck fire in terms of the consequences to the public.

The assignment of a consequence ranking is subjective. This table was used as a guideline to ensure consistency.

The specific steps performed in this qualitative analysis were:

Step 1. For a specific accident category listed in Table 1, assign a frequency ranking from Table 2 to each option. Consider items such as: building specific initiators, building specific design features, potential for accidents while in temporary storage locations, potential for accidents in new storage locations, and material relocated to other areas (i.e., frequency of transportation accidents). Consider how these factors vary between the proposed options to ensure consistency in the assigned rankings.

Step 2. For the same accident category as in Step 1, assign a consequence ranking from Table 3 to each option. Consider items such as: building specific design features, material-at-risk, release fractions, number of high efficiency particulate air (HEPA) filters, and material relocated to other areas (i.e., potential unfiltered releases during transportation accidents). Consider how these factors vary between the proposed options to ensure consistency in the assigned rankings.

Step 3. Repeat steps 1 and 2 above for each remaining accident category.

RESULTS/CONCLUSIONS

The objective of the analysis was to determine the relative risk of various options as compared to each other. The results of this analysis was presented in terms of a weighted numerical risk ranking as shown in Table 4, and a bar chart as shown

in Figure 1. As can be seen in Figure 1, of the five options, two groupings of results were concluded to be significantly different. This information was presented to the decision makers so that the risk issues could be balanced with their other requirements (e.g., security, schedule, etc.).

Table 4. Risk ranking of proposed options.

Accident category	Option 0 - Leave SNM stored in place	Option 1 - Consolidate in B991 vaults	Option 2 - Consolidate in B991 highbay, then to B371	Option 3 - Immediate move to B371	Option 4 - Consolidate in B991 vaults, then to B371
Transportation risk ranking	0	6	40	40	40
Seismic risk ranking	42	8	30	30	30
Fire risk ranking	8	20	36	36	25
Spill risk ranking	4	18	28	32	18
Explosion risk ranking	30	15	48	30	18
Criticality risk ranking	5	5	12	10	10
ALARA risk ranking	0.2	0.5	11	10.9	10
Total risk ranking	89.2	72.5	205	188.9	151

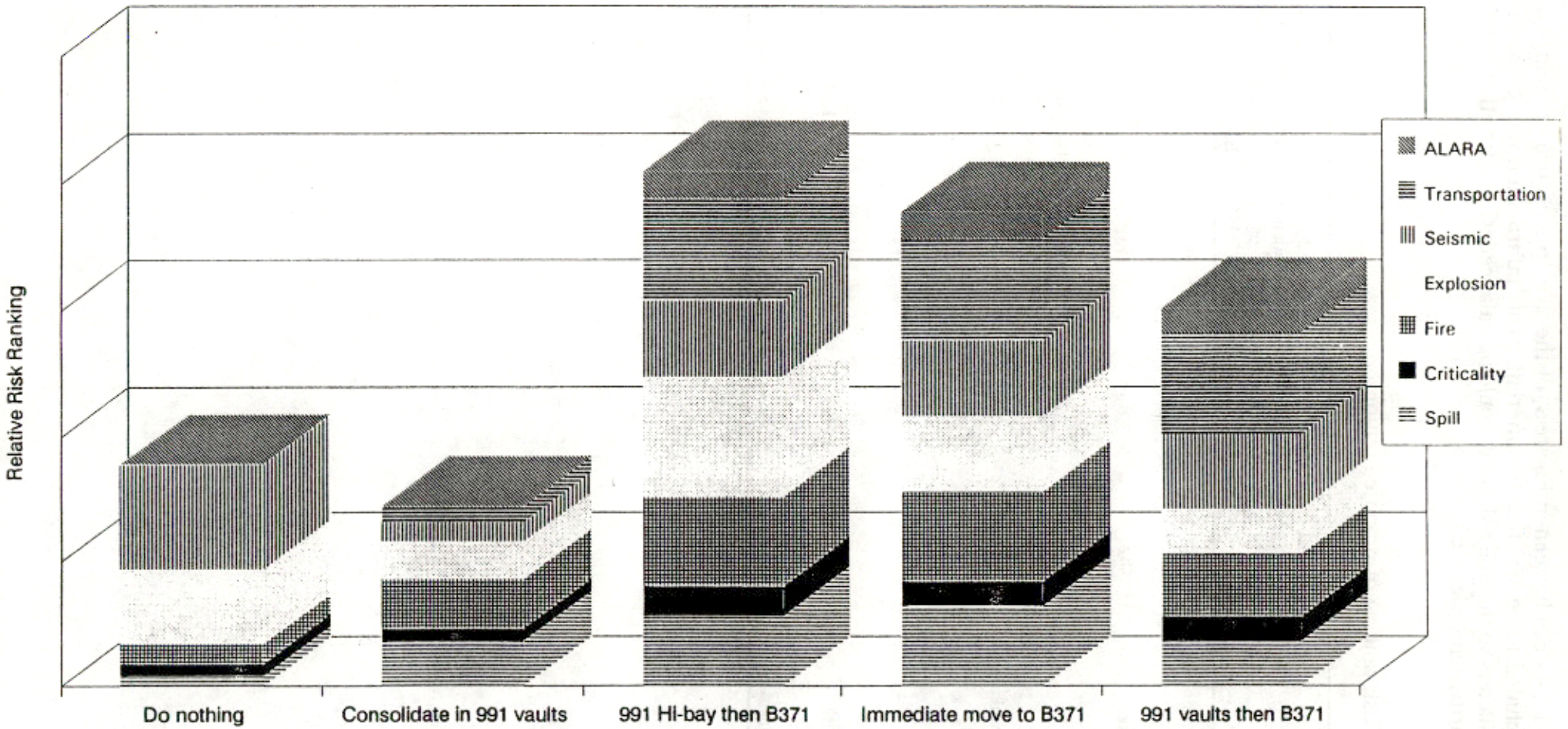


Figure 1. Qualitative Safety Comparison of Options (higher score equals higher risk)

RISK-BASED METHODS APPLICABLE TO RANKING CONCEPTUAL DESIGNS*

R. J. Breeding[1], J. T. Ringland[2], K. Ortiz[3], and J. J. Lim[4]

[1]Dept. 6411, Sandia National Laboratories, Albuquerque, NM 87185
[2]Dept. 8112, Sandia National Laboratories, Livermore, CA 94550
[3]Dept. 5167, Sandia National Laboratories, Albuquerque, NM 87185
[4]Lim & Orzechowski Associates, Alamo, CA 94507

INTRODUCTION

In Ginichi Taguchi's latest book on quality engineering,[1] an emphasis is placed on robust design processes in which quality engineering techniques are brought "upstream," that is, they are utilized as early as possible, preferably in the conceptual design stage. This approach was used in a study of possible future safety system designs for weapons. As an experiment, a method was developed for using probabilistic risk analysis (PRA) techniques to rank conceptual designs for performance against a safety metric for ultimate incorporation into a Pugh matrix evaluation. This represents a high-level trial application of PRA methods to weapons. As with most conceptual designs, details of the implementation were not yet developed; many of the components had never been built, let alone tested. Therefore, our application of risk assessment methods was forced to be at such a high level that the entire evaluation could be performed on a spreadsheet. Nonetheless, the method produced numerical estimates of safety in a manner that was consistent, reproducible, and scrutable. The results enabled us to rank designs to identify areas where returns on research efforts would be the greatest. The numerical estimates were calibrated against what is achievable by current weapon safety systems. The use of expert judgement is inescapable, but these judgements are explicit and the method is easily implemented on any spreadsheet computer program.

Safety in weapon systems is obtained in a fundamentally different fashion than in many other systems. Typically, safety is provided by subsystems that respond when an abnormal situation is sensed to bring the system to a safe state. In an office building, the sprinkler system dispenses water to put out fires when high temperatures are detected. In existing nuclear power reactors, pumps start to flood the core with water when low levels

*This work was performed for the United States Department of Energy under Contract DE-AC04-76DP00789. This paper does not constitute official policy of the Department of Energy or Sandia National Laboratories.

are indicated. Such safety subsystems often operate, at least in part, under normal environmental conditions. In weapons, the safety subsystems are expressly designed to keep the weapon from functioning, e.g., detonating, unless very specific stimuli are present to deactivate the safety subsystems. Thus, we demand that the safety subsystems remain in the safe state in accident conditions. So, instead of an analysis of whether the safety subsystems will operate under normal environmental conditions, an analysis of whether the safety subsystems will remain in the safe state under abnormal conditions is required. The abnormal conditions are a class of "noise" in Taguchi's model, and the "robust tolerance" of the safety devices is our design objective. The engineering tool used to measure tolerance is a very high-level PRA.

Current practice in weapon safety analysis defines failure as the loss of assurance that the safety subsystems are in the safe position and are not bypassed. This is much more conservative than defining failure as the occurrence of the undesired event since it overestimates the probability of the undesired event. This approach greatly simplifies the safety analysis. If we wished to determine the probability of the undesired events accurately, the response of many additional non-safety components would have to be determined for many different severity levels of several single and combined abnormal environments. If failure is defined as the loss of assurance that the safety subsystems are in the safe position and not bypassed, then the safety analysis need determine only the response of a small number of major components in abnormal conditions.

It is difficult to assure that a component designed to keep a weapon system from operating will remain in the safe position for very severe abnormal conditions. Therefore, the systems engineer pairs this component, the strong link, with another component, known as a weak link, whose failure could be guaranteed at lower levels of the abnormal conditions. Every effort is made to have the weak link fail in an irreversibly safe condition through a change of state based on intrinsic physical properties. When the weak link fails, it places the weapon in an irreversible non-functional condition. This strong link – weak link approach requires that the strong link and weak link be located as close together as possible, so that both experience similar conditions. As the abnormal condition increases in severity, then, the weak link changes to a safe position before the conditions reach a level at which the strong link can no longer be guaranteed to remain in the safe position.

Recently, the Department of Energy requested a search for additional or new concepts that would embody revolutionary advances in safety assurance. The diverse designs proposed in response required a consistent, quantitative approach to assess the safety potential at a very early stage of development. The safety features were so different from one design to the next that reliable qualitative comparisons would have been very hard to defend. Additionally, several proposed subsystems had no existing analogs. Thus, consistent application of expert judgement over a range of disparate designs was required by a team with extensive experience in PRA and weapon design and analysis. The assessments were further complicated by designs with two different configurations. In these designs, there is a storage and transportation configuration in which the weapon is intrinsically safe. The configuration is changed to permit use when the weapon is removed from storage or when use appears imminent. This meant that the location and state of the weapon had to be accounted for when performing the safety analysis.

DESCRIPTION OF THE METHOD

The basis of the analysis method is a high-level fault tree that is evaluated for a number of different abnormal environments and for all the stages in the life of the weapon. The aggregation over the abnormal conditions and stages of life is accomplished by the use of weighting factors. The fault tree considers failures and bypasses at the safety

subsystem level and results in six failure paths with fourteen basic events. Such a tree may seem extraordinarily simple, but the designs are at the conceptual level, and the information required for a more detailed tree is not available. Only if the design incorporated a subsystem that has been produced or is about to enter production would there be sufficient information to take the analysis below the subsystem level. Even then, the implementation in the new design is often different enough from the existing implementation that the information is not really applicable. Finally, we were interested in order of magnitude differences in the safety of competing designs; at the conceptual design level, these are the only differences that have meaning. On this scale, when different abnormal environments and phases in the life of the weapon were considered, the six failure paths proved sufficient to discriminate between designs in most cases.

The first step in the analysis for a specific conceptual design was to ascertain if the basic fault tree was appropriate for this design; modification was required to accommodate some designs. The next step was the assignment of probabilities for the basic events for each abnormal environment. This was generally straightforward but was often subjective. Where a similar system has been implemented in like fashion and had been analyzed, the results of that analysis were used. This was seldom the case, so most failure and bypass probabilities were assigned by experts based on analogies with analyzed and tested subsystems. The probability estimates were assigned relative to a benchmark value of 10^{-3} for a well-implemented strong link – weak link pair. This benchmark value was selected so that a system with two independent safety subsystems in series achieved the required undesired event probability of 10^{-6}. In keeping with the level of detail available, probabilities were order-of-magnitude only. Where there were questions about the implementation, optimistic and pessimistic failure probabilities were assigned. The optimistic probability implied that the subsystem is designed and built in such a way that the vulnerabilities are minimized; the pessimistic probability implied that it is not.

For some physical events, such as initiation of insensitive explosive by lightning or the impacts possible in transportation accidents, fairly low probabilities, e.g., 10^{-6} or 10^{-9}, could be assigned because tests had shown that this type of response was precluded by fundamental physical properties of the material. For an engineered safety subsystem, we did not feel that any failure probabilities lower than 10^{-3} were appropriate. There were too many unknowns about the components and the implementation of the subsystem for us to feel confident with lower probabilities.

After the assignment of basic event probabilities for each abnormal condition, the failure paths were evaluated to obtain a system failure probability for each condition. Based on our experience with abnormal environment analyses for different locations where the weapons might be kept for extended periods, and different operations in which the weapons might be involved, we decided that, for the purpose of this study, the ten combinations of abnormal conditions shown in Table 1 covered the accident environments of concern and were likely enough to be considered. We assigned weights that reflect a very approximate relative probability that the abnormal condition will be encountered in an accident.

The bulk of the abnormal environment weight is assigned to three environments: impact alone, fire and low voltage (LV) electricity, and impact, fire, and LV electricity. We considered the presence of high voltage (HV) electricity to be very unlikely. Due to intrinsic design features, electricity with enough potential to set off the detonators would have to come from a power transmission line or substation. We are aware of no data on such accidents. Not only would the accident have to cause failure of the isolation or insulation of the power lines, but the high voltage would have to be available in the immediate area of the weapon. Even the low weight shown may overestimate the probability of weapon exposure to high voltage electricity, but we were unable to justify a lower value.

Table 1. Weighting of Abnormal Environments

Environment	Fractional Weight
Impact	0.33
Fire & LV Electricity	0.33
Impact & Fire & LV Electricity	0.33
Impact & HV Electricity	0.003
Fire & HV Electricity	0.003
Impact & Fire & HV Electricity	0.003
Lightning & anything else	0.0005
Puncture & anything else	0.0005

Lightning and puncture are accidents of concern for which it is difficult to estimate a reliable frequency of occurrence. With today's deployment posture, the weapons considered in this analysis would not be located where they would be exposed to a lightning strike. Further, they would be shielded by one or more containers or structures almost all of the time. In an accident involving a truck or airplane, puncture of the weapon by a structural member is always possible. The probability of it actually happening appears to be very low although there are no good data for the puncture probability.

After estimating the subsystem failure and bypass probabilities for each abnormal environment, the failure paths are evaluated to obtain a system failure probability for each condition. Then aggregation over the environments is performed using the weights assigned to form a weighted average. Finally, there is an aggregation over the stages in the life of the weapon.

Typically a weapon has between five and ten stages in its life: e.g., manufacturing, transport, maintenance, storage, and deployment on alert. A weapon may be in physically different configurations during different stages, and the results of the fault tree evaluation depend on the configuration. The aggregation over the stages of life is also accomplished by means of weighting factors. The weights are assigned on the basis of the expected probability of comparable serious accidents for each stage, that is, on the basis of the product of exposure time and accident frequency. For example, if a weapon spends 50% of its life in location A where the serious accident frequency is 10^{-7}/year, and 5% of its life in location B where the frequency of a comparable accident is 10^{-6}/year, the two locations or stages would be assigned equal weights. Weights for the stages vary greatly with the type of weapon system; one weapon may spend most of its time in storage while another spends most of its life on alert. Table 2 shows the weights for the stages of life for a hypothetical weapon.

Table 2. Weights for the Stages of Life for a Hypothetical Weapon

Stage of Life	Weight	Fractional Weight
Manufacture	1	0.03
Transport	1	0.03
Storage	28	0.84
Maintenance	2	0.06
Training Exercises	0.3	0.01
Alert	1	0.03

A "standard" serious accident, the crash of an aircraft into a structure or vehicle containing the weapon, was used as a baseline for assigning weights to each stage. Crash frequency approximations were taken from previous studies on the likelihood of aircraft crashes at various locations on and around military bases. This accident is the most likely serious accident for many of the stages in the life of the weapon. An accident during transport of a weapon by truck in not considered to be a serious accident in this sense since a highway truck accident very rarely results in accident conditions as severe as an aircraft crash. To develop weights for the stages of life, it was estimated that only one truck accident in one hundred would result in abnormal conditions as severe as a typical aircraft accident, and the truck accident frequency was reduced accordingly. Justification for this factor of 0.01 could not be developed in the course of this project, so the number remains arbitrary, although we believe it to be of the correct order of magnitude.

Storage appears intuitively to be a safe and secure environment. The weapon is in an igloo or bunker protected by heavy doors and several feet of concrete and dirt. Nonetheless, if a weapon spends almost all of its time in storage, the weight for storage may be much higher than for any other stage. The weight reflects the product of the total time in a location and the probability of a serious accident per unit time; and the time in storage is very long. This does not imply that the storage stage is risky, but that the other stages are even less risky than storage.

For a stage such as manufacturing or transport, the time in each stage can be estimated from recent experience with similar weapons. For a stage such as alert, the time spent in the stage must be estimated for future decades. As might be expected, these estimates were subjective with large uncertainties.

Following the aggregation over the different abnormal conditions and over the stages of life, high-level optimistic and pessimistic estimates of weapon failure over the life of the weapon were obtained. These weapon failure probabilities are lower bounds in which we have very high confidence. Because the method of analysis was consistent, these lower bounds can distinguish safety differences between designs and bring out the importance of different environments and design features. We believe that the differences in failure probability estimates between designs reflect real and important differences in actual safety.

The failure estimates derived in this study are far too conservative and approximate to be considered realistic estimates for the failure of the weapon in an accident. Further, as mentioned above, we have defined failure not as the occurrence of the undesired event, but as the loss of assurance that the safety subsystems are in the safe position and are not bypassed.

APPLICATION FOR THE COMPARISON OF CONCEPTUAL DESIGNS

Once this exploratory analysis method had been worked out, which involved several iterations, the application was relatively straightforward. The computations, evaluation of the failure paths, and aggregations, were facilitated by the use of a modern spreadsheet program. The time consuming part of the evaluation was standardizing the criteria for assigning probability estimates to each basic event for the eight abnormal environments. Assignment of the probability estimates went faster than might be expected since some of the failure paths are specific to one abnormal condition, so their evaluation is trivial for all the other conditions.

Once the probability of each basic event is specified for each abnormal condition for a design, the spreadsheet produces an overall failure probability as well as a value relative to the baseline for that design. When all the designs have been evaluated, a substantial amount of time must then be spent in going over the results in detail looking for the

reason that design B is rated better than design A, and how is it that subsystem X appears to increase safety less than was expected intuitively. This in-depth quality check after the initial rating of the subsystems forms a very important consistency check and is crucial for the success of the method. It is during this review process that many of the insights and conclusions are formed. One of the successes of this straightforward approach was the almost immediate feedback we were able to provide to the designers. Preliminary evaluations during the development of the designs allowed the designers to modify and improve their designs. The simplicity of the analysis facilitated understanding of the evaluations by those not familiar with PRA.

Several features of the weapons and environments could not be adequately treated in this initial application of the method. We were not able to take the ordering of combined abnormal conditions into account in a realistic manner. We assumed that the abnormal conditions occurred in the worst possible sequence. In other words, if a design was more robust for fire followed by impact than for impact followed by fire, we assumed that the impact occurred first. We were also not able to treat the time it takes for safety subsystems to function. For designs that employed only subsystems that operated electrically or optically, the assumption that all the subsystems functioned instantaneously appears to be appropriate. For the designs with safety subsystems that operate mechanically, pneumatically, or hydraulically, the time the subsystem takes to operate may be important. This level of complexity could not be accommodated in the initial application of the method. We hope to be able to refine this assessment method in future applications.

CONCLUSIONS

Sandia, other Department of Energy laboratories, and various organizations within the Department of Defense have recently completed an extensive low level risk analysis for some existing weapon systems, considering numerous components in detail. In addition to these efforts, we believe that the high level application of PRA methods early in the design phase has considerable merit. Rapid evaluation made it possible to provide feedback on the efficacy of the safety features of each design during the design phase. This response provided valuable insights to the designers while the designs were in progress. The method provided a consistent, numerical means of comparing divergent approaches to weapon safety. The use of expert judgement was inescapable, but the method makes these judgements explicit and their application uniform and traceable. We were able to consider several abnormal environments and the different stages in the life of the weapon. This method of safety analysis enhanced clarity and understanding among the various disciplines and organizations involved. In sum, this application of PRA methods proved to be a low cost, high value product. It was of demonstrated utility in identifying where scarce resources could be used most effectively.

REFERENCES

1. G. Taguchi, "On Robust Technology Development, Bringing Quality Engineering Upstream," ASME Press, New York (1993).

PROCESS HAZARDS ASSESSMENT USING RISK MATRICES

Dennis Henneke
TENERA, L. P.
One Copley Parkway, Suite 216
Morrisville, NC 27560

Jerry Phillips
TENERA, L.P.
477 Shoup Avenue, Suite 100
Idaho Falls, ID, 83402

SUMMARY

Process Hazards Assessment (PHA) methods have historically provided only qualitative assessments of risk. Many companies are choosing to perform "Semi-Quantitative" PHAs by using a risk matrix ranking scheme during the assessment. Risk Matrices have, in fact, been used in federal and state risk assessment guidelines for a number of years[1,2,3]. These guidelines provide a basis for matrices to be used during PHAs, and even provide basis for acceptance criteria[4] for chemical risks. Two recent studies have included the use of multiple risk matrices. These matrices have been used to compare dissimilar risks such as process upsets, buried wastes, and production losses. The results of this PHA ranking were used to perform subsequent risk analysis normally performed using quantitative results. This subsequent analysis includes the performance of inservice evaluations (Application One), and cost benefit analysis of resulting recommendations (Application Two). The methods used during these two studies are presented here.

RISK MATRIX APPLICATION ONE

The first study using multiple risk matrices was performed at a Department of Energy non-reactor nuclear facility. The focus of this study was to develop technical guidance for performing inservice evaluation (ISE) of components at selected DOE facilities. Part of this project was to develop procedures to identify components whose failures pose a risk to the facility and/or its workers. Several techniques for quantifying component risk were considered. The technique that was selected was a modification of a Hazard and Operability (HAZOP) study. The standard HAZOP technique was supplemented with a risk ranking using risk matrices.

Levels of risk are determined by combining the expected frequency of an occurrence of an event with the level of consequence associated with that event. There are various types of risks associated with a facility operation, including personnel

injury/death, loss of plant equipment, damage to the environment, and others. The specific risks of operation at a given facility depend on many factors such as the type of material processed, process conditions, and concerns with the handling of nuclear fuel. A risk matrix was considered a good tool for use in quantifying the various risks.

Several risk matrices were developed and used during the Application One HAZOP. These risk matrices helped determine the levels of risk posed by failure of various components (e.g., vessels, piping, blowers, pumps, and valves). These matrices were used to estimate the effects and costs associated with equipment failures that resulted in "Plant Loss," "Worker/Public Safety," "Environmental Risk," and "Criticality." The risk matrices are attached as Figures I though IV.

The results of the study included a ranking for all of the components based upon these risk matrices. The component ranking can then be used as the basis for performance of ISE, maintenance or testing. Components that represent a higher risk are subject to more stringent ISE, while components that represent little or no risk are subject to little or no ISE.

RISK MATRIX APPLICATION TWO

Application Two illustrates that risk matrices can be used to compare and rank risks from several processes as well as risks analyzed using multiple PHA techniques. A recent comprehensive PHA performed at non government nuclear fuels plant reviewed all aspects of safety at the plant. The first phase of this study included a six-month review of all systems and plant programs that involved the handling, storage or disposal of hazardous chemicals or nuclear fuel. The PHA methods used were those recommended in the OSHA regulations, 29 CFR 1910.119[5]. This included a Hazard and Operability (HAZOP) study or What If Analysis of all processes containing hazardous materials, Process Hazards Surveys of support systems and waste storage, Program Reviews of important plant programs, and special studies for areas where the risk was either high or not well analyzed by other methods.

The HAZOP and What If studies included approximately five months of review. An independent HAZOP/What IF review team was supplemented with plant operations, maintenance and engineering staff. The team reviewed potential process hazards and made recommendations for plant improvements where necessary. The Process Hazards Surveys were performed by using an independent safety engineer and the responsible system engineer. The team walked down all systems not covered by the HAZOP or What If, reviewed appropriate documentation, and made recommendations for plant improvements where appropriate.

The purpose of the program reviews was to identify potential safety concerns that were a result of a plant program, procedure, or policy. Each program review involved an independent reviewer who was considered an expert in the respective plant program. The reviewer performed plant walk downs, interviewed all key personnel involved in the program, and reviewed applicable plant documents. The reviewer would then make recommendations for program improvements where problems were seen. The programs reviewed under this study included many programs required by OSHA 1910.119, including Emergency Management, Configuration Management, Procedures, Operations and Safety Training, and Maintenance.

reliability analysis and other specialized techniques. Each of these areas analyzed risks that were not fully reviewed by the other PHA reviews.

All of the recommendations that resulted from the HAZOP and What IF studies and individual PHA reviews were ranked during the performance of the study using four risk matrices. The combined risk matrix that was used is attached as Figure V. The risks rankings that were used included Criticality Safety, Environmental Safety, Industrial Loss, and Personnel Safety. Each recommendation was ranked based upon the estimated consequences for any or all of the listed risk areas and the estimated frequency of occurrence. For example, a recommendation in industrial safety may be the result of potential releases from mishandling of gas cylinders. This release may result in either personnel injury or a release to the environment. The recommendation would then be ranked based upon the risk for both environmental safety and personnel safety.

The key to using the risk matrices for the different PHA techniques was the consistent application and ranking using these matrices. Prior to performing each PHA, training on the matrices was performed for all participants. A consistency check was also applied for each risk scenario at the end of the study. The resulting risk ranking was very useful in the implementation phase of the project. Several hundred recommendations resulted from the study and the cost of implementing all of the recommendations was quite large in comparison to the available budget. The facility began to work off these recommendations by sorting the recommendations by risk ranking, then determining the cost and effort that each recommendation would require.

This cost estimate and the risk ranking of each recommendation were used as the basis for a simplified cost-benefit analysis. The implementation of the recommendations was based upon performing the low cost, high risk recommendations first, and the high cost, low risk recommendations last. In this manner, The facility can get the most safety benefit for their money, and reduce the risk at the facility in the shortest time possible.

This method is very useful when the expected cost of recommendations far exceeds the available funding. As expected for a study like this, the plant risk was dominated by a few possible accident scenarios. The recommendations that would reduce the risk from the dominate accident scenarios included both low and high cost plant improvements. It was estimated that by performing approximately 20% of the recommendations (and 20% of the cost), the facility could reduce their known risk by approximately 90%. Additional risk reduction can be achieved by the performance of all of the low cost and some medium cost recommendations.

The results of the PHA showed, as initially expected, that the greatest risk at the facility was not associated with the handling of nuclear fuel, but with the use of hazardous chemicals and disposal/storage of chemical and nuclear wastes. Thus the greatest impact will be felt by the reduction of risks to the workers, public and environment from potential releases of these chemicals.

POTENTIAL APPLICATIONS USING MULTIPLE RISK MATRICES

The two studies above used multiple risk matrices to rank potential plant hazards. In one case, the risk ranking was used to establish ISE of selected components. In the

Reliability Center Maintenance programs. Additionally, by making certain simplifying assumptions, results similar to those provided from a full Quantitative Risk Assessment can be derived. Thus the benefits from using risk matrices during a PHA can be great, and the results are useful for additional potential applications.

The OSHA 1910.119 regulations require many chemical facilities to perform a Process Hazards Analysis. The results from these PHAs are not directly useful for other applications. Use of a risk matrix in ranking potential scenarios will allow the results to be used for future risk assessment applications. Additionally, using a risk matrix during or after the PHA performance has been shown to add little cost to the study.

Risk matrices are typically used to rank "order-of-magnitude" risks. In other words, the approximate order of magnitude for both consequence and likelihood are estimated for each risk scenario. This type of application has been performed using singular risk matrices for years. Use of multiple risk matrices allows a comparison of dissimilar risks, and can even be used to compare risk from dissimilar facilities. One example application could be the prioritization of corporate or government funding allocations for improvements or site cleanup using multiple risk matrices. In this case, order-of-magnitude rankings of risks for each site can be developed based upon site hazards surveys. This results in ranking of sites using any one of a variety of risk matrices, such as potential dollar loss, worker and public safety, and environmental release. This ranking list can then be adjusted based upon deterministic factors, such as the local regulatory and public pressure that may exist for each facility.

The above provide only a sample of applications for risk matrices. With proper application of risk matrices, most application techniques previously applied to quantitative risk assessment results can be applied to PHA results.

REFERENCES

1. U.S. Environmental Protection Agency, "Guidelines for Performing Regulation Impact Analysis," EPA 230/01-84-0003, EPA, Washington DC.

2. U.S. Environmental Protection Agency, Federal Emergency Management Agency, U.S. Department of Transportation, "Technical Guidance for Hazards Analysis, Emergency Planning for Extremely Hazardous Substances," December 1987.

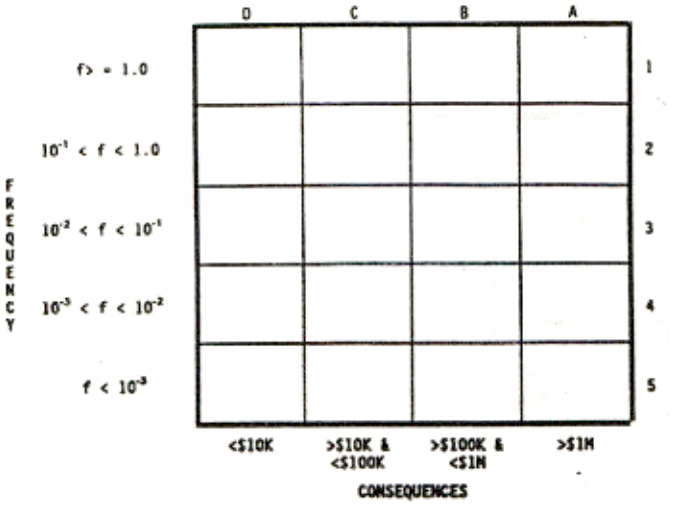
3. State of California, Governor's Office of Emergency Service, "RMPP Guidance for the Preparation of a Risk Management and Prevention Program," November 1989.

4. Henneke, D. W., Dombek, F. S., and Hou, H, "The Use of Acceptance Criteria for Quantitative Risk Assessment in the Chemical Process Industry," Report to Exxon Company, U.S.A., January 1990.

5. U. S. Department of Labor, Occupational Safety and Health Administration, "Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents; Final Rule," 29CFR Part 1910.

6. Blake, C. R., "Quantitative Risk Assessment Matrix Approach for Experiemental Programs," Hazard Prevention, 2nd Quarter, 1990.

Figure I:
Plant Loss Risk Matrix



NOTE: Plant Loss includes costs associated with repair/replacement of components, product losses, and "incentive bonus" losses or "penalty clause" losses due to schedule delays.

Figure II:
Worker/Public Safety Risk Matrix

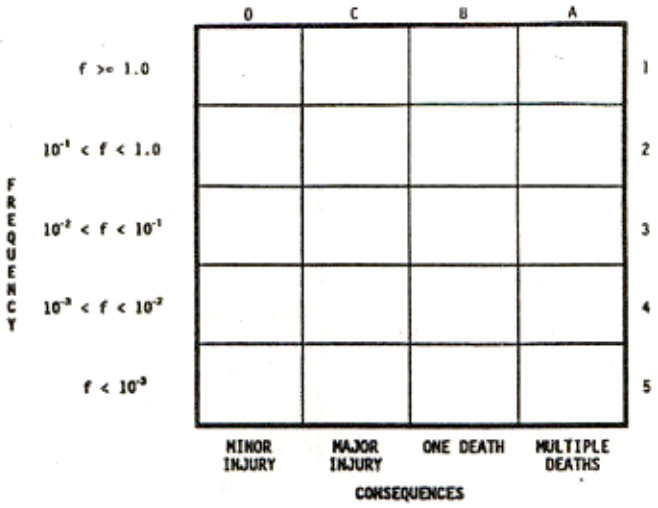


Figure II:
Environmental Risk Matrix

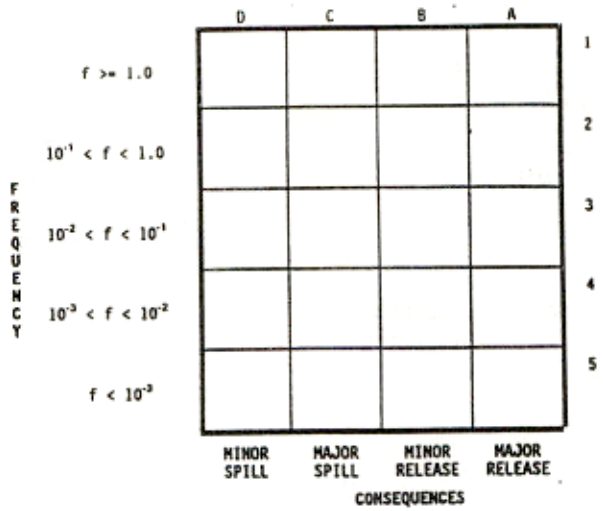


Figure IV:
Criticality Risk Matrix

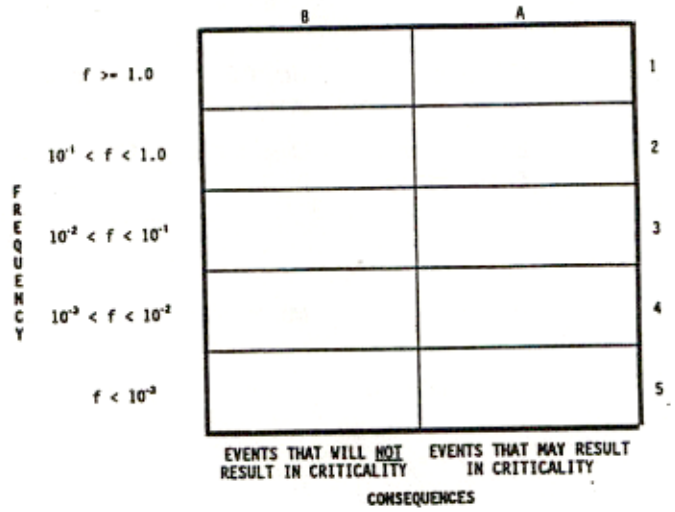


Figure V
Combined Risk Matrix

Frequency (per year)		D	C	B	A	
Frequent	$1.0 < f$	7	5	3	1	1
Likely	$10^{-1} < f < 1.0$	8	6	4	2	2
Occasional	$10^{-2} < f < 10^{-1}$	9	7	5	3	3
Possible	$10^{-3} < f < 10^{-2}$	10	8	6	4	4
Improbable	$f < 10^{-3}$	11	9	7	5	5

	Consequence			
	Notable	Important	Significant	Major
Criticality	Unusual event	Reportable Event	Near criticality	Criticality
Environmental/ Public Safety	On-site minor release	On-site major release	Off-site minor release	Off-site major release
Worker Safety	Minor injury	Major injury	One fatality	Multiple Fatalities
Industrial Loss	< 250K	<2.5M	<25M	>25M

002 Uncertainties and Sensitivities

Chair: R.M. Cooke, Delft U. Technol

Assessing the Risks and Uncertainties due to Incinerator Toxic Air Pollutants Emission
J. Swider, W.E. Kastenberg (UCLA)

Dependability Through Auditing
J.R. Stone, D.I. Blockley (U. Bristol)

Multi-Level Control Against Uncertainties and Failures Consequences
V.N. Efanov, V.G. Krymsky (Ufa St. Aviation Engineering, Russia)

ASSESSING THE RISKS AND UNCERTAINTIES DUE TO INCINERATOR TOXIC AIR POLLUTANTS EMISSION

Jan Swider and William E. Kastenberg

Mechanical, Aerospace and Nuclear Engineering Department
University of California, Los Angeles
Los Angeles, CA 90024-1597

INTRODUCTION

Toxic air pollutants emitted to the atmosphere as a result of human activities have been a significant contributor to the overall public health risk. Estimation of the risks associated with a specific facility is usually carried out by following guidelines published by the Environmental Protection Agency (EPA). However, these guidelines are often composed of conservative assumptions, i.e. they use worst - case input values which lead to point value results having little in common with reality. Any interpretation of the final risk estimates may be limited by these conservative values. There is a need, however, for qualitative as well as quantitative assessment of the results coming from such analyses.

Incineration is a technology that can be a solution for managing municipal solid wastes (MSW) and hazardous wastes. But this technology can also cause adverse effects to the environment and human health. Due to the recent number of extensive studies of incinerator pollutant emissions (EPA, 1984, 1987, 1988), a tremendous amount of data exists. For many of the air toxics risk analysis parameters, one is now able to derive probabilistic distributions. New methodologies for extended uncertainty analysis, especially Monte Carlo techniques, give more confidence in the final results and allow a decision maker to rank the possible outcomes, thus easing the decision making process.

ASSESSING RISKS

The focus of this work is on the risks associated with air toxics emitted from incinerators. Because standard techniques for the quantification of ecological impacts have not been developed as yet, the risk herein quantifies human impacts. In general, the evaluation of public health risks due to air toxic emissions includes the following four steps:

- Hazard identification, where the emission source is characterized and pollutants with potential to cause any type of adverse health effect are recognized.
- Exposure assessment, involves modeling transport and environmental fate to obtain the concentration of pollutants the public can be exposed to, identification of exposure routes, population exposed and time of the exposure.
- Dose-response evaluation, allows one to obtain the population adverse health effects due to the exposure.
- Risk assessment, integrating the exposure and the public health effects in order to obtain the final health risk.

There are significant uncertainties involved in each step of the risk assessment process. These uncertainties stem from a number of sources including, evaluation of the emission source, transport modeling, and health impact studies. Hence, no risk assessment is valid without estimation of the uncertainties.

ASSESSING UNCERTAINTIES

There are two types of uncertainty in any risk assessment: parameter uncertainties and modeling uncertainties. In addition, uncertainties in the degree of completeness as a special type of modeling uncertainty, are sometimes identified (NUREG, 1982). The evaluation of uncertainties embodied in the assessment of risks involves: estimation of uncertainties in the input values; propagation of input uncertainties through the whole analysis; and combination of the uncertainties in the output in order to obtain the final distribution of uncertainties in risk. In this paper, an attempt to provide quantitative estimation of uncertainties in air toxics risk assessment, uncertainty has been treated probabisticaly i.e. by assigning probabilistic distributions to represent uncertainty about the parameter values. For the parameters with negligible uncertainty, point values are applied. Modeling uncertainties can be estimated by comparative calculations of the risk applying different models, and using expert opinion elicitation to quantify them (NUREG, 1990).

There is often a misconception regarding sensitivity and uncertainty analyses. A sensitivity analysis is useful in estimating the effects of varying input parameters, such as emission rates or dispersion coefficients, on the final results. Uncertainty analysis allows one to compare the importance of the input uncertainties with regard to their contributions to uncertainty in the outputs (Morgan and Henrion, 1990). There is a variety of methods for uncertainty propagation and analysis. These methods range from simple analytical approaches based on Taylor series expansions, to computationally extensive models such as Monte Carlo or response surface methods. However, with the rapid progress in the development of personal computers and the flexibility of currently available software, it is possible to run some of these analyses right on an engineer's desk. A method for propagating uncertainties at the screening risk level was shown previously (Swider and Kastenberg, 1993). An example of how these methods can be applied for more complex analysis is presented below.

AN INCINERATOR EMISSION CASE

EPA has conducted a program on waste destruction performance and pollutant emission from municipal solid waste and hazardous waste incinerations. It was designed to estimate the environmental impact of these processes and to collect data on pollutant

emissions. Based on current data, chlorinated dioxin and furan emissions, being in the spotlight of public attention for years, are not significant for hazardous incinerators (Dempsey and Oppelt, 1993). However, metals are of concern in waste incineration because of their presence in many municipal and hazardous wastes, and due to the adverse health effects they pose to human beings. Arsenic, cadmium, chromium and beryllium pose carcinogenic risk while others, like lead and mercury, are non carcinogenic toxics. It was found (ASME, 1988), that the primary exposure pathway of pollutants from incinerators is inhalation via the air route. The indirect exposure pathway may also pose a significant contribution to risk (Lee, 1990). For the purpose of this paper however, we will only consider airborne arsenic, and present a risk assessment due to inhalation for a point source characterized in Table 1. This analysis is based on the methodology presented by EPRI (1985). For simplicity, we are showing only the elementary steps of this methodology.

Table 1. Characteristic of the emission source.

Parameter	Symbol	Value or Distribution
Stack height, m	h_s	30
Stack radius, m	r	1
Emission rate, g/s	q	LN(2.8e-04, 2.0e-05)
Gas exit temperature at stack height, K	T_s	390
Ambient temp. at stack height, K	T_s	293
Stack exit velocity, m/s	v_s	N(15,0.5)
Wind speed at stack top, m/s	u	N(6.5,0.1)

We consider a pollutant injected into the atmosphere through regular emission from an incinerator smokestack. Gases emitted from incinerator stacks are usually hotter than the ambient air and have an initial momentum. Hence, the plume rise is an important factor since the ground level concentration of the emitted pollutant depends on the effective stack height. The effective stack height is the sum of the actual stack height h_s and the plume rise Δh. There are many plume rise formulas available (Zannetti, 1990) with the Briggs method as the most favored,

$$\Delta h = 1.6\, F^{1/3}\, u^{-1}\, x^{2/3} \qquad (1)$$

where the buoyancy flux parameter is given by:

$$F = g\, v_s\, r^2\, (T_s - T_a)/T_s \qquad (2)$$

To estimate exposure, one of the air pollution models is used. In this case, the Gaussian plume model has been chosen. The maximum ground level concentration for the region where the plume has reached its final height can be presented as follow (Seinfeld, 1986),

$$c_{max} = \frac{q\,\alpha^{\alpha/2}\,R_z^{\alpha-1}}{\pi e^{\alpha/2} R_y h^{\alpha} u} \qquad (3)$$

where $\alpha = 1 + r_y / r_z$, and r_y, r_z, R_y, R_z are coefficients depended on the stability class. Surface wind speed at 10 m for stability class D is 5-6 m/s. The wind speed increases with altitude and must be corrected appropriately to the stack height and type of surface.

Exposure due to inhalation of arsenic has been estimated per capita lifetime. In order to translate the ambient ground-level concentration of the pollutant into the inhalated concentration (μg/day), an exposure factor of 22.4 m^3/day, for the adult population, has been applied. Dose-response evaluation is done using three models: one-hit model, multi-stage model, and EPA unit risk factor with parameters for these models intercepted from the airborne pollutants risk assessment study (EPRI, 1985).

To perform the analysis, a Latin Hypercube sampling method was used. A thousand samplings of the random variables was generated from every distribution and propagated through the set of applied models. Comparison of the applied dose-response methods is shown in Figure 1, and the resulting distributions for the maximal ground-level concentration, exposure, and risk are presented in Figure 2. The uncertainty in exposure value is small in comparison with the spread of the dose-response results. The risk values obtained from this analysis are generally in the order of $1x10^{-11}$. The one-hit and multi-hit methods show a good accordance, while the unit risk calculations show one order higher values through the whole range.

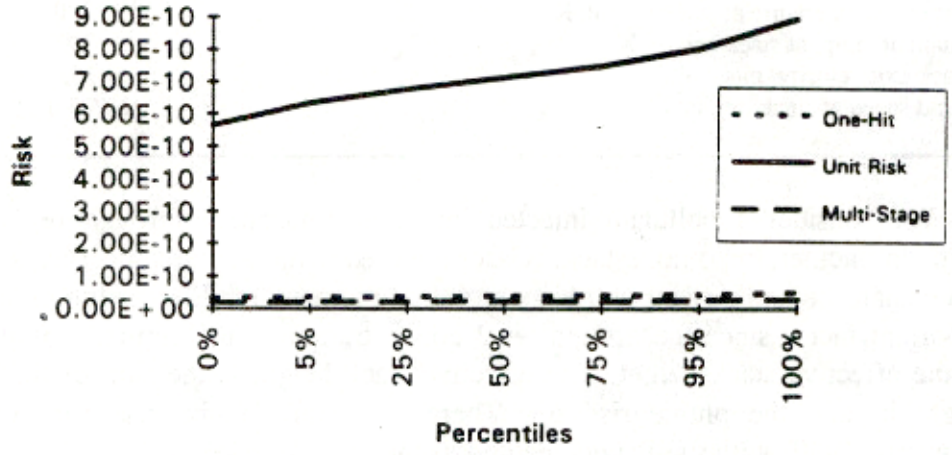


Figure 1. Comparison of Dose-Response Models

CONCLUSIONS

Waste incineration risk assessment provides a means to quantify the impacts of this pollutant destruction process on the public. Conservative assumptions during the risk analysis process are forced by current regulations. Such approach as using the upper bound values do not give a decision maker plausible information. The presented methodology allows a decision maker to rank possible outcomes. Inclusion of the uncertainty analysis gives potential for in-depth comparison of waste incineration options with other disposal methods, thus easing the decision making process. The crucial element of this analysis turns out to be the dose-response calculations. Comparing the final results of this example, one can see that the dose-response uncertainty is dominant. Improving accuracy of dispersion or exposure models has lesser impact on the final risk in this case. Such findings give a basis for a proper action, and allow one to manage the risk in more efficient way.

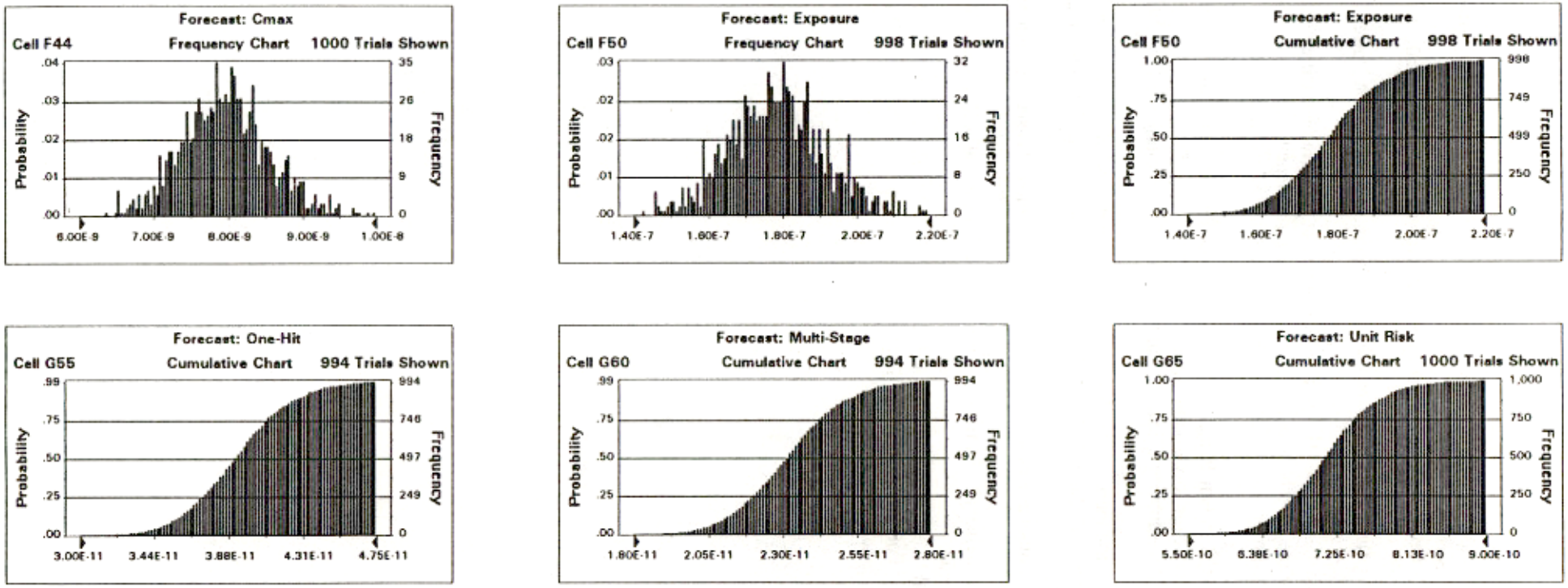


Figure 2. The distributions for the maximum pollutant concentration, exposure, and risk.

REFERENCES

ASME, 1988, "Hazardous Waste Incineration; A Resource Document", The American Society of Mechanical Engineers, New York.

C.R. Demsey and E.T. Oppelt, 1993, Incineration of hazardous waste: a critical review update. *J. Air Waste Manege. Assoc.* 43:25.

EPRI, 1985, "Assessing the Health Risks of Airborne Carcinogens", Electric Power Research Institute, EA-4021.

Lee, J. and W.E. Kastenberg, 1990, Health risk assessment of incinerator stack emissions: trace metals, in: Proceedings of the 1990 National Conference on Environmental Engineering, Washington, D.C.

NUREG, 1982, "PRA Procedure Guide", NUREG/CR-2300, U.S. Nuclear Regulatory Commission, Washington.

NUREG, 1990, "Severe Accident Risks: An Assessment for Five US Nuclear Power Plants", NUREG-1150, U.S. Nuclear Regulatory Commission, Washington.

Seinfeld, J.H., 1986, "Atmospheric Chemistry and Physics of Air Pollution", John Wiley & Sons, New York.

Swider, J. and W.E. Kastenberg, 1993, Propagation of uncertainty in air toxics risk assessment, in: Proceedings of the 1993 Joint CSCE-ASCE National Conference on Environmental Engineering, Montreal, Canada.

U.S. EPA, 1984, "Performance Evaluation of Full-Scale Hazardous Waste Incinerator", NTIS, PB 85-129500.

U.S. EPA, 1988, "Measurement of Particulates, Metals and Organics at a Hazardous Waste Incinerator", NTIS, PB 89-230668.

U.S. EPA, 1987, "Total Mass Emissions from a Hazardous Waste Incinerator", EPA-600/S2-87/064.

Zannetti, P., 1990, "Air Pollution Modeling. Theories, Computational Methods and Available Software", Van Norstrand Reinhold, New York.

DEPENDABILITY THROUGH AUDITING

J R Stone and D I Blockley

Department of Civil Engineering
University of Bristol
Bristol BS8 1TR, U.K.

ABSTRACT

Engineers strive to achieve dependable artefacts. Scientists are seen traditionally seen as seeking for truth. Both groups make extensive use of testing in order to attempt to falsify their theories. Audits are becoming an increasingly used tool in the search for safety. The paper describes the search for dependability through auditing, and compares this approach with the scientific search for truth through testing.

INTRODUCTION

Engineered systems must satisfy a number of separate, often contradictory, criteria, such as safety, initial cost, aesthetic appeal, ease of maintenance and running costs. Each of these criteria will be assessed in some manner and have some greater or lesser 'weighting' applied in accordance with pre-defined sets of values. Depending upon the use for which the system is intended, the balance of the individual weightings influences the final form of the system. The aim of the engineer is (or should be) to deliver 'quality', for which one or more of the above criteria may be necessary (though not sufficient). Safety is clearly a necessary condition of a structure, since quality can not be achieved in its absence. Matousek (1992), for example, has argued the Quality Assurance (QA) view of quality, meaning the meeting of a need and the idea of providing fitness for purpose. Different levels of absolute quality may be thus satisfactory for different purposes, in the same manner that different types of shop exist to serve different sectors of the same market. Many organisations have developed methods of QA to assist them. In the U.K., British Standard BS4778 (BSI, 1987) defines Quality Assurance as "all those planned and systematic actions necessary to provide adequate confidence that a product will satisfy given requirements of quality". One of these necessary actions is the measurement of system dependability through auditing.

DEPENDABILITY

Comerford and Blockley (1993), building upon earlier work by Blockley (1980), have defined dependability as a measure of the safety content of a structure which will be useful in the management of safety, providing evidence of 'fitness for purpose'. It is therefore, as in quality assurance, a relative rather than an absolute attribute. This measure is contrasted with that of 'truth', and they argue that the idea of scientific or engineering theories as 'revealed truth' must be discarded due to the incompleteness and uncertainty inherent in their predictive reliability. The traditional view of science (e.g. as described and criticised by Chalmers, 1978) sees it as a search for truth which is approached through testing.

Experiments are undertaken and a new view of the world emerges, which is believed to be more 'true' in some sense than the previous version. Popper (1959) showed that verification of theories, through the testing of propositions derived from those theories, gives no logical foundation for a belief in future behaviour. He proposed instead the falsification of hypotheses through rigorous and ingenious testing. As theories are falsified they are modified and so knowledge develops. Popper argues that this process of conjecture (the theory) and refutation (the falsification), or trial and error, leads to 'truth'. True knowledge is, in this sense, knowledge which corresponds with the facts.

It is clear that areas of knowledge, such as Newton's Laws, which are not 'true' in this strictest sense (there are situations where they lead to incorrect predictions), are nevertheless extremely useful. They are of enormous practical value because there are many situations where the theories do lead to propositions which do indeed correspond to the facts. This suggests that there is a need to change focus from that of 'truth' to defining the conditions under which theories can be used dependably. Thus true knowledge is clearly dependable whereas dependable knowledge, though useful, may not be true. The desired goal in engineering therefore becomes dependability rather than truth and it involves defining those conditions under which a theory may be relied on for practical decision making.

Comerford and Blockley's use of this idea was to see the process of searching for safety as being analogous to the process of searching for truth. The idea is therefore to test, as ingeniously and rigorously as possible, all aspects of a project to establish an appropriate safety level. The converse of dependability, according to Comerford and Blockleys' interpretation, is vulnerability. Vulnerability is said to accrue if a structure does not pass critical tests, either through the tests not being carried out, or failure to meet the criteria for passing the test.

Dependability need not be a single measure. Comerford and Blockley, in the context of assessing dam safety, envisage a hierarchy of 'dependability indices'. These might include separate indices for stability, structural integrity, operation and human factors. The dependability of the overall system is influenced by the individual components. One rôle of an audit is to establish an appropriate measure of each index.

MEASUREMENT AND TESTING

According to Diekemper and Spartz (1979), "any program, activity, or function which is worthy of continued existence must be designed to permit an objective performance measurement". This search for 'objective' (i.e. measurable) indices is familiar throughout engineering, but is often interpreted in a narrow sense by considering purely quantitative data. Probabilistic Risk Assessment (PRA), for example, is generally concerned with the determination of quantitative measures and the use of probability theory. Probability may, in this context, be seen as a measure of risk. The role of hazard auditing (described below) is to allow the additional incorporation of qualitative data giving a combined measure of 'proneness to failure'.

We may see measurement as allowing a hierarchical ordering of outcomes of a series of tests, becoming progressively nearer to truth / dependability as more tests are successfully

passed. A simple example relating to one definition of 'randomness' illustrates this property of an emergent hierarchy. Popper (*op cit*) considered the process of testing in the context of defining randomness, a concept with several varying interpretations. Using a frequentist interpretation of randomness, in which all substrings of length n have an equal frequency of occurrence in a random string of digits length m ($n < m$), Popper argued that it is possible to construct a hierarchy of 'degree of randomness' by carrying out tests on substrings of increasing length. For example, when testing a given string of digits for randomness, it may perhaps be established that all 2-digit substrings appear an equal number of times. This is a 'low level' pass, giving weak support for the hypothesis that the complete sequence is random. Progressively increasing the test substring length to 3-, 4-, etc., digits results in a series of progressively harder tests to pass, giving progressively stronger evidence of randomness. The 'degree of randomness' of the m-digit string is equivalent to the 'highest level' test passed. A string which fails this test at substring length n is less random than one which fails at length n+1. Randomness, like quality and dependability, is according to this definition a relative rather than an absolute concept.

This analogy with passing a series of increasingly difficult tests can be employed in the assessment of structural dependability. Comerford and Blockley (*op cit*) note that generally in engineering, the word testing usually refers to physical tests carried out in-situ on the structure or perhaps on a scale model. This is widespread in civil and structural engineering, whether it be materials testing of concrete cubes or billets of steel, or in the monitoring of the in-service behaviour of major structures such as dams or suspension bridges. They, however, use the term in a much broader sense to encompass quality, or more specifically hazard, audits carried out to criticise the structure, management, human and organisational factors and the whole project from conception to operation. In many situations, they argue, the threshold of 'pass' or 'fail' when applied to a specific test is fuzzy rather than crisp and that the relative importance of the tests must be reflected in the final measure of dependability. Judgements at the social end of the socio-technical spectrum will generally fall into this fuzzy boundary category.

AUDITING

Audits are one of a range of different and complementary approaches to risk control. Their use has grown dramatically in the past two decades in the wake of well-publicised disasters in high-risk industries, and in the face of growing concern about the control of technology, particularly in the process (petrochemical) and nuclear power industries. Kletz (1992) describes the steps taken by many companies in the process industries, including the use of well developed safety audits in conjunction with specific hazard-spotting techniques such as hazard and operability studies (HAZOP) and hazard analysis (HAZAN). Groeneweg (1992) has described a hazard auditing procedure called Tripod which has been developed for Shell. He argues that analyses based upon future possible event trees of unsafe acts are not possible, as they entail a logical infinity of possibilities, so that audits should be concerned only with giving indications of the current situation. The Tripod audit questions act as evidence towards the assessment of eleven 'General Failure Types', such as poor maintenance procedures, hardware defects and inadequate training, and result in a profile giving a representation of proneness to failure.

A new field of hazard engineering, encompassing hazard auditing and hazard management, has been proposed (Dester and Blockley, 1993, Stone and Blockley, 1993). Dester and Blockley describe the design of a hazard audit in which prior knowledge of factors influencing proneness to failure is structured hierarchically, and where the rôle of an audit is critically to examine a current project in terms of this knowledge. In the same way that probability is a measure of risk, so hazard audits must be able to provide a 'measure' of hazard content, or proneness to failure. This measure is dependability, and is again assessed on a hierarchical

scale through the application of increasingly rigorous audits. The upper, or most rigorous, level of the audit is chosen to be appropriate to the project, so that those whose failure would result in significant loss or damage to life or property would be subjected to more rigorous assessment. Audits can examine not only technical but also social and organisation factors such as operating procedures and environmental and political pressures.

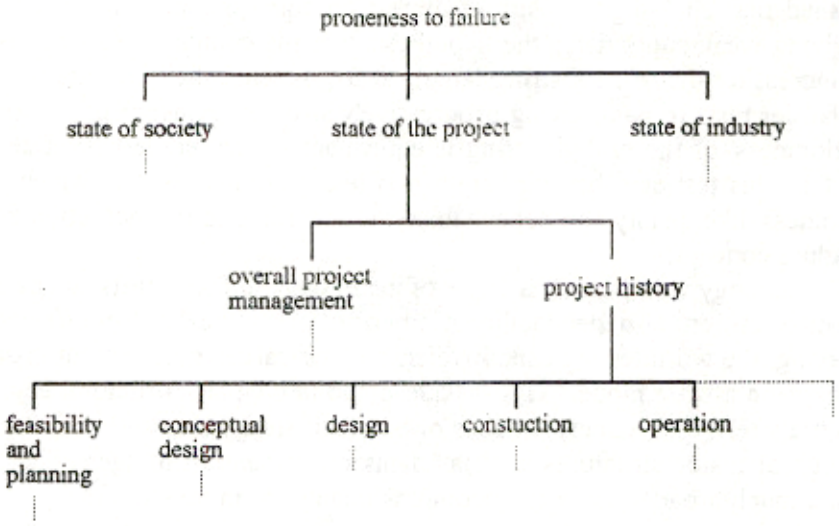


Figure 1. Top levels of the 'proneness to failure' hierarchy. (from Dester, 1992).

Figure 1 illustrates some of the top levels of a proposed 'proneness to failure' hierarchy for use in auditing engineering projects. This would be implemented by constructing a series of questions aimed at establishing the current state of each element of the hierarchy. The overall proneness to failure of the project is made up from contributions from each of the lower levels. It is important to note that the individual components are not factors which might cause failure, but that instead they are indicators of hazard—a set of preconditions with the potential for initiating an accident sequence.

MANAGEMENT

The control of risk through hazard engineering has been described elsewhere (Stone and Blockley, 1993). The two important aspects are the measurement of proneness to failure (through hazard auditing and other means), and the treatment (through hazard management) of exceptional circumstances where hazards exist which need to be controlled by the use of specialist skills.

Comerford and Stone (1992) have discussed developments in the fields of artificial intelligence which have enabled more flexible, open and powerful methods of modelling to be employed in computer systems. These developments include methods for detecting similarities between patterns of factors present in a current project and those accumulated through machine learning from case histories of failures. Similarities found in this way can be used as a part of an overall measure of proneness to failure and so influence dependability. The characteristics of a system for the management of safety through auditing can be realised within new languages and environments resulting from these developments.

CONCLUSIONS

Both science and engineering depend to a large extent upon measurement through testing. Science is often seen as seeking true knowledge whilst engineering is about providing quality and safety through testing for project dependability. The extent to which dependability has been achieved may be found through auditing.

REFERENCES

Blockley D I. 1980, "The Nature of Structural Design and Safety," Ellis Horwood, Chichester.

BSI. 1987, "Quality Vocabulary," (British Standard BS4778), British Standards Institute, London.

Chalmers, A. F., 1978, "What is This Thing Called Science?" Open University Press, Milton Keynes.

Comerford, J. B. and Blockley, D. I. (1993). Managing safety and hazard through dependability. *J. Structural Safety*. 12:1.

Comerford, J. B. and Stone, J. R. (1992). Artificial intelligence in risk control, *in*: "Engineering Safety," D.I. Blockley, ed., McGraw-Hill, London.

Dester, W.S., 1992, "The Development of a Structure for the Design of Hazard Audits,", Ph.D. Thesis, University of Bristol.

Dester, W. S. and Blockley, D. I. (1993). A structure for dependable hazard management. (submitted to *Proc. Inst. Civ. Engrs.*).

Diekemper, R. and Spartz, D., 1979, A quantitative and qualitative measure of industrial safety activities, *in*: "Self-Evaluation of Occupational Safety and Health Programs," National Institute for Occupational Safety, Rockville, MD.

Groeneweg, J., 1992, "Controlling the Controllable," DSWO Press, Leiden.

Kletz, T., 1992, Process industry safety, *in*: "Engineering Safety," D.I. Blockley, ed., McGraw-Hill, London.

Matousek, M., 1992, Quality assurance, *in*: "Engineering Safety," D.I. Blockley, ed., McGraw-Hill, London.

Popper, K., 1959, "The Logic of Scientific Discovery," Hutchinson, London.

Stone, J.R. and Blockley, D.I., 1993, Hazard engineering and the management of risk, *in*: "Proc.ISUMA '93, Second Int.Symp.Uncertainty Modeling and Analysis," B.M. Ayyub, ed., IEEE Computer Society Press, Los Alamitos.

MULTI-LEVEL CONTROL AGAINST UNCERTAINTIES AND FAILURES CONSEQUENCES

V.N.Efanov* and V.G.Krymsky*

*Ufa State Aviation Engineering University
*12 K.Marx Street, Ufa, Bashkortostan, 450000, Russia
*Phone: +7 (347-2) 23-78-36
*Fax: +7 (347-2) 22-99-09

ABSTRACT

In the paper a problem of multi-level control algorithm designing is considered. The offered approach allows to reduce the consequences of the equipment possible failures and also of the uncertainties in the subsystems description. The main idea is based on the redundancy introduction into the system structure.The higher control levels (the levels of coordination) provide system desirable performances by changing its admissible structural states.

INTRODUCTION

Modern control systems oriented toward complex dynamic plants (such as aircrafts and their engines, power stations, etc.) usually have a decentralized structure [1]. The noted type of structure allows to provide the majority of desirable system performances: a rapid response to any change of the controlled process characteristics, an opportunity to satisfy some survivability requirements because of control problems destribution between subsystems, an optimal throughput for the local computers combined into the network.

Meanwhile the solving of decentralized control systems(DCS) design problem is concerned with some specific difficulties consideration. DCS successful functioning can be provided only if the local subsystems coordinated interaction takes place.It means that DCS must include the special higher control levels (the levels for coordination) to influence on the subsystems behavior in the arbitrary situation.

Unfortunately there are many situations when behavior of a concrete subsystem is unknown or imperfectly known. Some of these cases are caused by the uncertainties in the system exploration conditions description. The subsystems abnormal functioning may be also connected with the failures consequences. That is why the necessity in correspondent coordination algorithms properties appears.

The aim of the present paper is to create the methods for design of DCS coordinating levels algorithms reducing the uncertainties and failures consequences. The main idea of the approach to be suggested is based on redundancy introduction into the system initial structure. This action allows to form a

considerable number of DCS states with admissible values of system quality indices. So the coordinating levels(or "coordinators") must provide DCS accident-free functioning by changing the admissible structural states in the cases of possible failures or malfunctions.

THE PROBLEM FORMULATION

The whole DCS is considered to be composed of n local subsystems described by the discrete equations

$$\vec{x}_i(k+1)=A_i\cdot\vec{x}_i(k)+B_i\cdot\vec{u}_i(k)\ ;\quad \vec{y}_i(k)=C_i\cdot\vec{x}_i(k), \tag{1}$$

$$i=1,2,\ldots,n;\quad k=0,1,2,\ldots,$$

where $\vec{u}_i(k),\vec{y}_i(k),\vec{x}_i(k)$-the vectors of i-th subsystem inputs,outputs and phase variables respectively;A_i,B_i,C_i-the real matrices.

Besides

$$A_i=A_i^*+\Delta A_i,\quad B_i=B_i^*+\Delta B_i\ ,\quad C_i=C_i^*+\Delta C_i. \tag{2}$$

Here A_i^*, B_i^*, C^*_i characterize the initial ("nominal") regime of system functioning; $\Delta A_i,\Delta B_i,\Delta C_i$ are the interval matrices [2] which reflect the uncertainties in subsystems behavior description. Only the upper and the lower bounds for each element of the last matrices are assumed to be known.

The interconnections of subsystems can be expressed by

$$\vec{u}_i(k)=\sum_{j=1}^{n}F_{ij}\cdot\vec{y}_j(k)+G_i\cdot\vec{u}(k);\ \vec{y}(k)=\sum_{i=1}^{n}L_i\cdot\vec{y}_i(k),\ k=0,1,\ldots, \tag{3}$$

where $\vec{u}(k)$, $\vec{y}(k)$- the vectors of DCS inputs and outputs; G_i,L_i,F_{ij}-matrices with elements which belong to discrete set $\pi=\{-1,0,+1\}$.

In the cases of possible failures some elements of these matrices become equal to zero.So we can form the special matrices $G^{(r)},L^{(r)},F^{(r)}$ with elements influenced by G_i,L_i,F_{ij}, i,j=1,2,...n, and connected with different system states. Assume upper index r=0 in relation to the faultless DCS state; r=1,2,... in relation to the states caused by the various types of failures.

Then DCS description looks as follow

$$\vec{x}^{(r)}(k+1)=A^{(r)}\cdot\vec{x}^{(r)}(k)+B^{(r)}\cdot\vec{u}^{(r)}(k);\vec{y}^{(r)}(k)=C^{(r)}\cdot\vec{x}^{(r)}(k), \tag{4}$$

$$k=0,1,2,\ldots n\quad r=0,1,2,\ldots,$$

where $A^{(r)}=A+B\cdot F^{(r)}C$; $B^{(r)}=B\cdot G^{(r)}$; $C^{(r)}=L^{(r)}\cdot C$; A=block diag$\{A_i\}$; B=block diag $\{B_i\}$; C=block diag $\{C_i\}$.

Our aim is the designing of the algorithms for the control signals changing in order to satisfy the requirements

$$\vec{x}^{(r)}(k)\in\Omega x\ ,\quad \vec{y}^{(r)}(k)\in\Omega y, \tag{5}$$

for all $r\in\Gamma r$.

Here Γr is the given set with integer elements ; Ωx, Ωy characterize the admissible values of vectors $\vec{x}^{(r)}(k)$, $\vec{y}^{(r)}(k)$ elements respectively.

THE DESIGN PROCEDURE

According to the offered approach the control algorithm $\vec{u}(k)$ is determined as a composition of two parts:

(i) the first part $\vec{u}_{(1)}(k)$ which provides the desirable behavior of the faultless system in relation to the nominal regime;

(ii) the second part $\vec{u}_{(2)}(k)$ which allows to compensate the uncertainties in subsystems description and also to provide the required DCS pole placement in the cases of possible failures.

The second part of the control algorithm

$$\vec{u}(k)=\vec{u}_{(1)}(k)+\vec{u}_{(2)}(k) \tag{6}$$

is realized by the coordinating level.

The item $\vec{u}_{(1)}(k)$ is formed as

$$\vec{u}_{(1)}(k)=H\cdot(\vec{x}^{(0)}(k)\cdot\vec{g}(k))^{\tau}+Q\cdot\vec{\lambda}(k), \tag{7}$$

where $\vec{\lambda}(k)$ is the vector of DCS desirable responses; $\vec{g}(k)$- the vector of coordinator phase variables; H,Q -the real matrices with elements which are to be found; upper index "0" denotes the faultless system state; the analogous index "τ" corresponds to matrix transpose result.

The item $\vec{u}_{(2)}(k)$ is obtained by the following dynamic compensator functioning:

$$\begin{aligned}&\vec{g}(k+1)=\Phi\cdot\vec{g}(k)+\vec{v}(k),\\&\vec{w}(k)=\vec{g}(k)+E\cdot\vec{v}(k),\\&\vec{v}(k)=T\cdot\vec{x}(k),\quad \vec{u}_{(2)}(k)=R\cdot\vec{w}(k).\end{aligned} \tag{8}$$

Here $\vec{v}(k)$, $\vec{w}(k)$ are the vectors of compensator intermediate variables; Φ - special Frobenius matrix; E - matrix with the elements E_{ij} which are equal to "1" if j=1,2,..., dim $\vec{g}(k)$ and i=j+1 or to "0" for all other cases.

Real matrices T,R are also to be found.

The first part of control algorithm is designed by means of the undermentioned statement utilization.

Theorem 1. The vector(7) of control signals which allows to remove the faultless nominal system phase variables to the region given by expression

$$C^{(0)}\cdot\vec{x}^{(0)}(k)=\vec{\lambda}(k) \tag{9}$$

must satisfy the equation

$$\vec{u}_{(1)}(k)=(C^{(0)*}\cdot B^{(0)*})^{\tau}\cdot(C^{(0)*}\cdot B^{(0)*}\cdot(C^{(0)*}\cdot B^{(0)*})^{\tau})\cdot(\vec{\lambda}(k+1)-$$

$$-C^{(0)*}\cdot(A^{(0)*}+B^{(0)*}\cdot R\cdot E\cdot T)\cdot\vec{x}^{(0)}(k)-C^{(0)*}\cdot B^{(0)*}\cdot R\cdot\vec{g}(k)). \tag{10}$$

Here the upper index "*" denotes nominal system regime.

The proof of Theorem 1 includes the estimation of the cost function

$$\rho(k)=|\vec{\lambda}(k)-C^{(0)*}\cdot\vec{x}^{(0)}(k)| \tag{11}$$

and the determination of the conditions which cause $\rho(k)\to 0$.

The second part $\vec{u}_{(2)}(k)$ of the control vector $\vec{u}(k)$ is obtained by means of iterative procedure concerned with compensator (8) decomposition. This procedure gives a possibility

to consider coordinator as a totality of $\mu+1$ dynamic subsystems

$$\vec{g}_l(k+1)=\Phi_l\cdot\vec{g}_l\ k+1)+\vec{v}_l(k),$$
$$\vec{w}_l(k)=\vec{g}_l(k)+E_l\cdot\vec{v}_l(k), \qquad (12)$$
$$\vec{v}_i(k)=T_l\cdot\vec{x}^{(r)}(k), \quad \vec{u}_{(z),l}(k)=R_l\cdot\vec{w}_l(k),$$
$$r=0,1,2,\ldots; \quad l=0,1,2,\ldots,\mu.$$

Here all the vectors and matrices which have denotations with lower index "l" correspond to subsystem under the number "l" and preserve the similar meaning as in (8).

Each l-th stage of the noted iterative procedure deals with the new l-th subsystem introduction into the DCS structure. Besides the initial stage allows to design a basic coordinator subsystem (l=0) which provides DCS required robust control quality level by compensation of the uncertainties (2) consequences. This fact is due to the analysis of feedback control system interval characteristic polynomials $P_l^{(r)}(z)$, where z is the discrete transform variable, l=0 and r=0,1,2,... - the DCS possible states.

Note that

$$P_l^{(r)}(z)=\det(z\cdot I-\Phi_l)\cdot\det(z\cdot I-A_l^{(r)})+\hat{R}_l^{(r)}(z)\cdot D_l^r(z)\cdot\hat{T}_l^{(r)}(z).$$

Here $A_l^{(r)}$ has the similar meaning as $A^{(r)}$ in (4) but in relation to the l-th procedure stage; $D_l^r(z)$ - matrix associated with $(z\cdot I-A_l^{(r)})$; $\hat{R}_l^{(r)}(z)$, $\hat{T}_l^{(r)}(z)$ - matrix-line and matrix-column respectively with elements influenced by R_l, T_l.

In order to fulfil $P_l^{(r)}(z)$ consideration the new (strong) version of Soh result [3] was obtained.

Theorem 2. The roots of m_l^r-th order interval polynomial $P_l^{(r)}(z)$ belong to $[0,\alpha)$, where α - the real number: $0<\alpha<1$, for all the values of subsystems (1) parameters inside the given fields with fixed bounds if the coefficients $P_i^{(r,l)}$, $i=1,2,\ldots,m_l^r$, of the noted characteristic polynomial satisfy the following equations:

$$(\theta_s^{(1)}/\alpha)^{m_l^r}-\underline{P}_i^{(r,l)}\cdot(\theta_s^{(1)}/\alpha)^{m_l^r-1}+\ldots+\gamma=0,$$
$$(\theta_s^{(2)}/\alpha)^{m_l^r}-\underline{P}_i^{(r,l)}\cdot(\theta_s^{(2)}/\alpha)^{m_l^r-1}+\ldots+\delta=0, \qquad (13)$$
$$s=1,2,\ldots,m_l^r.$$

Here $\gamma=(-1)^{m_l^r}\cdot\underline{P}_{m_l^r}^{(r,l)}$ and $\delta=(-1)^{m_l^r}\cdot P_{m_l^r}^{-(r,l)}$ for even m_l^r; $\gamma=(-1)^{m_l^r}\cdot P_{m_l^r}^{-(r,l)}$ and $\delta=(-1)^{m_l^r}\cdot\underline{P}_{m_l^r}^{(r,l)}$ for the contrary case; $\underline{P}_i^{(r,l)}, P_i^{-(r,l)}$ - the lower and the upper bounds for $P_i^{(r,l)}$ respectively; $\theta_s^{(1)}$, $\theta_s^{(2)}$ - the given numbers which belong to $[0,\alpha)$.

The further iterative procedure stages (l=1,2,...) aim to provide the desired DCS pole placements in the states caused by the failures to be considered. The above mentioned Theorem 2 utilization gives a possibility to reduce the problem of additional subsystem design to the search of linear algebraic equations system solution.

The procedure will be finished when the introduction of the last subsystem will provide the expression

$$\sum_{r\in\Gamma_r}\sum_{l=0}^{\mu} m_l^r = æ, \qquad (14)$$

where æ - the resulting number of the poles whose required placement has been provided at all the stages.

In the paper the necessary (structural) conditions for the design problem decidability are investigated. It is shown that the additional subsystems and interconnections introduction allows to reach this purpose. The volume of the redundancy to be introduced can be minimized by consideration of special structural complexity cost function [4].

The offered methods for multi-level control algorithms creation are added by the procedures for their multi-processor realization architectural development. Analysis of the calculating operations sequence realizing the obtained algorithms gives a possibility to form a totality of Abel's groups which unite the actions suitable for parallel fulfilment. The noted result utilization allows to find the required number of processors and memory units, to determine their interconnections.

The main results obtained by the authors are illustrated by the examples of the design of DCS for complex technical plants. It is shown that the created systems remain with allowable performances in the face of uncertainties and possible failure situations. So there is an opportunity to conclude that each the designed DCS posseses the high survivability.

REFERENCES

1. V.I.Vasiliev, Yu.M.Gusev, V.N.Efanov, V.G.Krymsky, V.Yu.Rutkowsky, V.A.Semeran, Multi-Level Control for Dynamic Plants (Nauka, Moscow, 1987).
2. R.E.Moore, Interval Analysis (Englewood Cliffs, N.J., Prentice- Hall, 1966).
3. C.B.Soh, Parameter Space - Approach to Linear Problems (Ph.D. Dissertation, Monash. Univ., Clayton, Victoria, Australia, 1986).
4. V.N.Efanov, V.G.Krymsky, Yu.G.Krymsky, Proc. of PSAM, 1, 741-746 (1991).

003 Software Dependability (I)

Chair: C. Lavine, The Aerospace Corporation

Risk Assessment and Management of Safety-Critical, Digital Industrial Controls - Present Practices and Future Challenges

W.R. Dunn (USC); M.V. Frank, S.A. Epstein (Safety Factor Assoc.); L. Doty (NASA)

Reliable Process Execution in FMS by Extended Transactions

U. Schmidt (U. Stuttgart)

RISK ASSESSMENT AND MANAGEMENT OF SAFETY-CRITICAL, DIGITAL INDUSTRIAL CONTROLS - PRESENT PRACTICES AND FUTURE CHALLENGES

W.R. Dunn[1], M. V. Frank[2], S.A Epstein[2], & L. Doty[3]

[1] University of Southern Colorado, NASA - Ames Research Center, MS 218-6 Moffett Field, CA 94035

[2] Safety Factor Associates, 1410 Vanessa Circle, Encinitas, CA 92024

[3] National Aeronautics and Space Administration, Ames Research Center, MS 218-7, Moffett Field CA 94035

INTRODUCTION

As a result of the low cost and high flexibility of the microprocessor, digital controls are now proliferating in a wide range of safety-critical industrial control applications. Many risk analysts view this trend with concern principally due to a widespread lack of knowledge of digital hardware and software failure modes, a fundamental ignorance brought about by the intractable complexities of digital systems. Risk assessment technology clearly lags implementation technology in this important area.

The paper shows how, in spite of this problem, probabilistic risk assessment (PRA) as used in high-risk nuclear power generation applications can be adapted to the medium-risk digital industrial control problem.

The paper is organized as follows. First, a brief review of the architecture, function, and operation of the digital control system is described. Next, it is shown how probabilistic assessment methodology, as practiced in nuclear applications, is modified to estimate risk in the digital industrial control application. Many gaps nonetheless exist in our knowledge of how to manage and assess risk in these systems. The paper concludes with a discussion of future research directions and a summary.

A GENERIC DIGITAL CONTROL SYSTEM

Figure 1 depicts the basic structure and components that make up a digital industrial system. It represents a variety of available products ranging from the simple programmable logic controller to the multi-computer distributed control system. Referring to the figure, the computer (hardware) and software constitute the "brain" which, via input/output (I/O) electronics, receives operator commands, sends out commands to effectors (motors, valves, actuators, etc.) that drive the process, receives information about the process from sensors (pressures, actuator positions, temperatures, etc.), and communicates needed information about the process to the operator. The operator communicates with the computer with a manual input device which can consist of simple switches, the conventional keyboard, etc. Correspondingly information can be received via indicator lights or in more complex applications a conventional monitor screen. (Some applications combine input and display devices in the form of a "touchscreen").

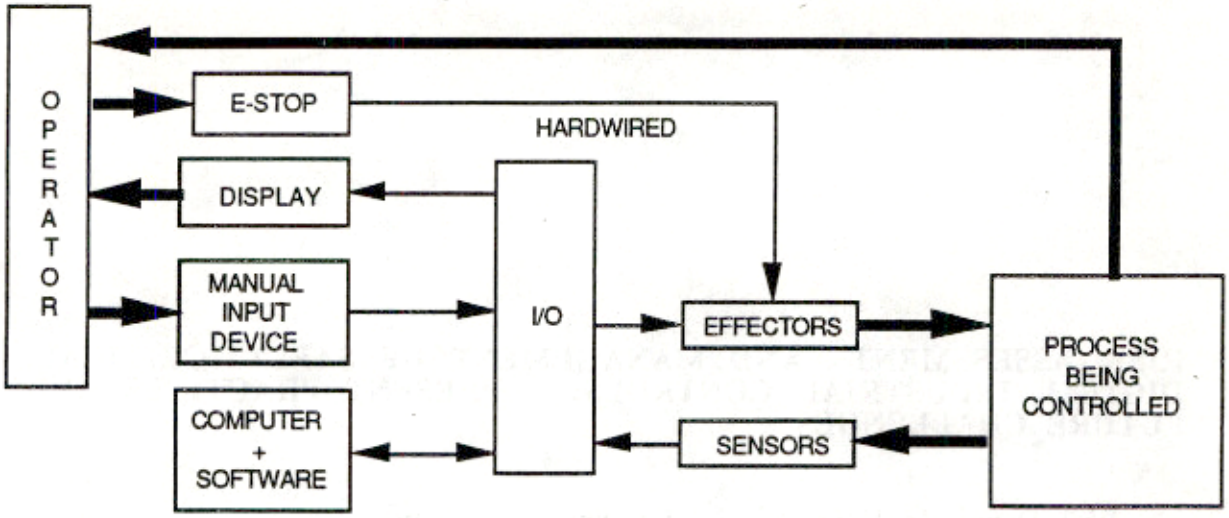


Figure 1. Generic Digital Control System

Software consists of two elements: system software which orchestrates the flow of information between devices attached to I/O electronics and application software consisting of control laws and, as will be discussed in more detail later, diagnostic algorithms.

All safety-critical systems, be they electromechanical, analog, or digital invariably employ an independent hardwired emergency stop (E-stop) circuit as shown in the figure.

RISK ASSESSMENT

Acceptable Risk

Risk in the industrial control applications under discussion is, unlike nuclear power generation or explosive manufacturing, generally concerned with property damage and personnel death/injury on a very limited scale. In the safety assessment work at NASA Ames Research Center, risk of catastrophic or critical failure of a facility control system on the order of 10^{-6} /hour or less is considered acceptable.

Probabilistic Risk Assessment for Industrial Controls

Probabilistic Risk Assessment (PRA) is concerned with scenarios that lead to catastrophic or critical end (damage) states. With the control system, the fundamental scenario begins with loss of control of the process being followed by sequences of (pivotal) events that lead to undesired end states. Control loss invariably manifests itself as inadvertent motion of one or more effectors caused by failure of one or more components in the control system. In our analyses, inadvertent effector motion is the initiating event. Analysis and quantification of the initiating event follows conventional fault tree develpment and cutset equation evaluation as practiced in nuclear-oriented PRA.

The development of scenarios resulting from this initiating event on the other hand is another matter. Our earliest efforts in attempting to adapt PRA to Ames' facility problems focused on the scenario concerning a closed circuit wind tunnel wherein control of the aircraft model being tested was lost (inadvertent model motion), operators failed to effect an E-stop, the model collided with the tunnel wall, debris was generated and travelled down the circuit, impacting and destroying the tunnel's ten million dollar compressor. Once into the effort of developing event trees and attempting to model and quantify pivotal events, it became clear that the engineering effort needed to quantify the scenario would not only exceed available assurance resources but would demand a risk assessment budget rivaling that allocated for the entire design effort.

Quantification of this and similar scenarios was therefore abandoned not only because it was unaffordable, but for the reason that a practical alternative was available: the control system could be readily designed such that probability of the initiating event would be at or

less than the level of acceptable risk. This would guarantee that the risk of any ensuing worst case scenario would be acceptable. As it turns out, these design practices were already a part of NASA Ames System Safety policy.

RISK MANAGEMENT - DESIGNING IN HAZARD CONTROLS

High Level Hazard Controls

The NASA Ames System Safety Office has had the long standing policy that safety-critical control systems should have no single-point-of-failure that can lead to a catastrophic or critical outcome. As a result, past non-digital control systems were designed to incorporate high-level controls intended to arrest inadvertent control motion. The System Safety Office also provides design guidelines that recommend that high level controls be implemented in a hierarchal fashion - the simplest and most reliable ones having the highest priority. The hierarchy is as follows.

1) Physical barriers (e.g. mechanical stops)
2) Static mechanical devices (e.g. burst disks)
3) Moving mechanical devices (e.g. relief valves, check valves)
4) Simple electromechanical system (e.g. limit switches, pressure switches)
5) Simple analog or discrete digital electronic system (e.g. overspeed circuits)
6) Simple software based device (e.g. programmable logic controller)
7) Redundancy (e.g. triple modular redundancy, standby sparing)

With high level controls in place, the probability that unwanted effector motion will occur is now the joint probability of a control system component failing and producing inadvertent motion and the probability of the high level control failing to stop it. Risk of the worst case scenario occurring is clearly reduced.

Low Level Hazard Controls

With a digital system, one can go further in reducing risk of inadvertent effector motion by employing the computer's "intelligence" to diagnose failures within the control system and to arrest inadvertent motion before the effector(s) reach the high level control. To stop the motion, the computer is hardwired via a separate port to a relay in series with emergency stop circuit (Figure 1). The computer opens this relay when it detects a failure, effecting the emergency stop. Three exceedingly simple diagnostic tools are employed to activate this circuit: the wraparound test, continuous built-in self tests, and the watchdog timer - each described as follows.

In the wraparound test the computer verifies, by reading sensor data, that the effector command it sent out to the process was correct. Where it is not correct, the computer commands the emergency stop. This simple function, readily implemented with a few lines of software code, will catch virtually all of the critical failures occurring in the I/O, effector, and sensor subsystems (Figure 1). A wraparound of sorts also applies to the manual input and display devices. Since it is standard practice to display the operator manual commands on the display device, the operator will recognize display or manual input device failures and can effect manual emergency stop.

In the continuous built-in self test, the computer continuously (in background processing) tests memory, central processing unit, and select I/O channels for hardware faults. If a fault is detected, the computer opens the emergency stop relay.

Finally in the watchdog timer function, the computer refreshes a special time-delay circuit (a multivibrator) each time the computer goes through a control computation cycle. The time delay circuit holds the emergency stop relay in the closed position. Should the computer fail, the most likely event is that the time-delay circuit will not be refreshed and it will time out, opening the relay.

These very simple tests have been in use in digital control practice for over a decade. In the risk assessment work at Ames Research Center, it is recommended that all three tests be used. This insures that the majority of possible hardware failures that occur in the

control system will be flagged and result in an E-stop. Additionally, the watchdog timer will catch software failures that result in a "hang up" condition. What remains to be discussed then are those software failures which are not caught by the watchdog timer.

SOFTWARE FAILURES

Software Failure Modes

As noted earlier, software consists of system software and application software. System software is written by the control system manufacturer. Where the control system product has had extensive field exposure (thousands of units running thousands of hours each) and debugging, realtime system software failures do not enter the risk picture. The reason is that the application software, written by the control user, is a new one-of-a-kind item, relatively untested, which can be expected to experience far more failures during operational life than the system software.

Application software can fail in two ways. First, it can fail in a manner wherein it continues to refresh the watch dog timer and at the same time generates an incorrect effector command. Note here that for this type of failure, the previously described diagnostic routines may or may not run. (We assume in our modelling that they will not.) Second, software-implemented diagnostic tests may fail to detect hardware failures when they occur. Note that this type of failure applies not only to the wraparound and self-tests in the control systems computer but to a software-based high-level control (e.g. programmable controller) if one is employed. To do PRA on the digital system, quantitative models for these software failure modes are necessary.

Quantitative Models - Control Software

Concern is with the failure rate at which software continues to refresh the watch dog timer and generates unsafe effector commands. We have no historical data with which to quantify this particular event. It can however be estimated. First, an abundance of data exists which allows estimation (again, in the pre-design phase) of total software failure rate and its uncertainty[1]. What is at issue is the fraction of these software failures that are critical. We know now, in spite of fears about software in the early days of digital control, that the fraction is small. Software-related incidents like the well known Therac-25 accidents[2] are rare when put up against the fact that thousands of properly engineered, critical digital systems have been functioning safely, world wide for over a decade. (The most notable examples are the fleets of civil and military aircraft employing fly-by-wire digital controls which have flown millions of hours without incident.) Data from our studies (based mainly on NASA flight control systems) and those of others[3,4] suggest that the fraction of total software faults that could be "critical" in realtime application can be represented by the discrete probability distribution shown in Table 1.

Table 1. Software Critical Fault Distribution

Fraction f of total software faults that are critical faults	Probability
0.00	0.30
0.10	0.40
0.15	0.15
0.20	0.15

In our own pre-design phase risk modelling, we employ this conservative distribution noting that it can updated using Bayes' Theorem once actual test data become available after the control system has been designed and tested.

Quantitative Models - Diagnostic Software

Turning to diagnostics, the probability that a software diagnostic routine will work

correctly when a failure occurs is referred to as "coverage".[5] Unlike the case for the distribution of critical vs. total software faults, hard data that would permit estimates of coverage based on, say, program size appears not to be available. One can however make coarse, conservative estimates of coverage for preliminary design purposes as follows.

Given diagnostic software of an estimated size (e.g. number of lines of code) of the diagnostic code , it is possible[1] to estimate the total number, N, of software faults we use that will reside in the code when the system enters its operational phase. However only a fraction of these faults, if excited, will lead to unsafe conditions. A conservative working model for estimating diagnostic software coverage is based on two assumptions:

1) The fraction f of the N faults that could lead to catastrophic conditions is given by Table 1 .

2) Over the operational life of the system all N software faults are excited.

The probability that none of the N faults will be catastrophic is therefore $(1-f)^N$. In our analyses, this term is evaluated and used as the coverage figure for the wraparound and high-level control software diagnostic routines.

Finally, coverage for the self-test is not governed by reliability of its diagnostic software but by the fact that the tests do not cover all of the components within the computer hardware . Correspondingly, the watchdog timer will cover most but not all computer hardware failures. In our modelling work, computer hardware failure coverage due to both watchdog timer and self tests is estimated (judgement) to lie somewhere between 0.9 and 0.99 (a uniform distribution is assumed).

CONTROL SYSTEM GENERIC RISK MODEL

Figure 2 shows a generic fault tree for the initiating event "inadvertent effector motion". Note that the top event is "potential" motion since not all control system failures with with no E-stop will necessarily lead to effector motion. Numerical point estimates

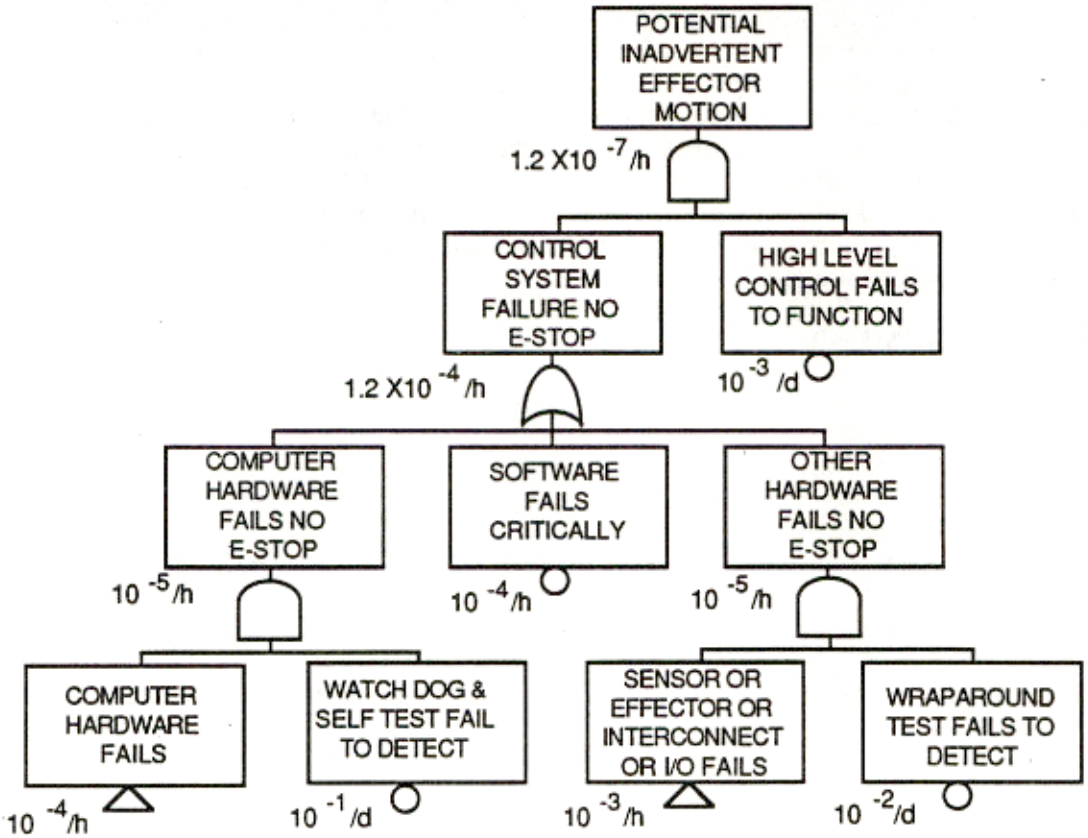


Figure 2. Generic Fault Tree for Control System PRA

shown in Figure 2 are based on an actual Ames application (a model support controller). These show quantitatively how high and low level controls reduce risk of the top event and, therefore, any ensuing worst case scenario to an acceptable level.

Indeed, development and quantification of a fault tree of the form of Figure 2 are all that are needed for PRA of the medium risk controls application.

FUTURE CHALLENGES

While it is clear that digital controls can be safely employed in small-scale, medium risk applications, our primitive models for digital systems, especially the software models, would suggest that it is not possible to engineer safe large-scale systems in high risk applications such as aviation. However, as noted earlier, the development of digital "fly-by-wire" systems and their deployment in both commercial and military aircraft fleets have resulted in millions of hours of safe flight suggesting that good engineering practice, especially in software engineering, can yield a product whose actual risk is much less than our intuition and models would suggest.

A major research challenge therefore is to uncover why, with all the complexities and opportunities for catastrophic failure in large-scale, high risk digital systems (e.g. in aviation) the systems themselves are so reliable. Answers to this question may lead to risk management oriented design and implementation practices that will build, a priori, guaranteed safety into digital control designs design.

Finally, much more research is needed to improve our empirical digital PRA models, especially in the software area.

SUMMARY

The primary concern with the digital control system is that it will generate incorrect control. In our medium risk digital industrial control application, we have found the development of quantified PRA scenarios based on this initiating event is, given available budgets, prohibitively expensive. It is moreover, unnecessary, since the digital designs, like their electromechanical and analog counterparts, require independent, high level controls to arrest the onset of dangerous controls. It is shown that by using the computer's "intelligence" to do low-level system diagnostics, risk of incorrect control is reduced even further. Since the net risk of incorrect control can, through these controls, be driven to or below the acceptable risk for the worst case scenario, PRA for the digital application reduces to the familiar, fault tree analysis. Primative, conservative quantitative models for software are presented to support fault tree quantification. An example of risk computation is presented. Finally, future research directions needed to improve risk assessment and management technology are given.

ACKNOWLEDGEMENT

This work was supported in part by NASA Cooperative Agreements NCC 2-373 and NCC 2-609.

REFERENCES

1. J.D. Musa, A. Iannino, K. Okumoto. "Software Reliability", McGraw Hill, New York, (1990).

2. E. Joyce, Software bugs: a matter of life and liability, "Datamation", (May 15, 1987).

3. R. Rubey, J. Dana, P. Biche, 1975, Quantitative aspects of software validation, *IEEE Transactions on Software Engineering*, Vol. SE-1, No.2:150.

4. R. Selby, 1990, Empirically based analysis of failures in software systems, *IEEE Transactions on Reliability*, Vol 39, No. 4:444.

5. T. Arnold, 1973, The concept of coverage and its effects on the reliability model of a repairable system, *IEEE Transactions on Computers*, Vol. C-22, No. 3:251.

RELIABLE PROCESS EXECUTION IN FMS BY EXTENDED TRANSACTIONS

Ursula Schmidt

University of Stuttgart
Institute for Parallel and Distributed High Performance Systems
Breitwiesenstraße 20 - 22
70565 Stuttgart
Germany

INTRODUCTION

The project "transactional concepts in manufacturing" at the University of Stuttgart explores how manufacturing processes can be performed more reliably with the help of transactional concepts.

When looking into the manufacturing area we find that there are great - and successful - efforts to improve safety and efficiency of the technology of manufacturing processes. Precision is increasing and machine tools become more and more versatile, fast and precise. However, we did not find a common pattern how failures of the technological process are handled. It lies in the responsibility of the programmers of the control system and the NC-programs to care of possible failures. There is no general model how failures are to be handled. Thus, after failures - failures of the machine or, even worse, of components of the control system - the system must be brought back manually to a safe and consistent state. Valuable time is wasted, machines stand still and the operator(s) has to make a lot of important decisions, possibly based on uncertain information.

Our goal is to provide a programming interface that removes failure handling from the application code of both control system and NC-programs. For this, we want to use the concept of transactions, which is well-known and proven in a lot of computer science applications. So, what are these transactions like?

Classical transactions[1] were developed for areas like banking or flight-reservation systems, where data have to be correct and persistent under all circumstances, i.e. where many users resp. processes concurrently access and update data and where system breakdowns must not leave the system in an incorrect state. These transactions are groups of operations on databases, which are executed by the transaction processing system (TPS) *atomically*, i.e. either the group is performed as a whole or, in case of failures or a user-initiated rollback, none of the actions leaves any trace in the system, from the user's view. This is performed by undoing all effects of the failed transaction's operations, whichever reason the failure may have.

So, transactions guarantee data consistency, results are durable and the applications can work in a logical single user mode. These features are provided by the low-level functions of the TPS. Thus, transactions completely remove the burden of failure handling from the application programmer.

These properties motivate us to extend the application areas of transactions:

- when using transactions, failure handling is kept off the application code which in turn will be considerably simplified and thus be more reliable.
- failure handling can be automated in a much higher degree.
- the restart times of a machine or the system will be minimized by guaranteeing consistency of the system state. The defined failure semantics of the transactional model make many of the otherwise required checks superfluous.
- for decisions an operator has to meet in case of urgency situations, he can rely on data which is guaranteed to be correct, i.e. which represents the system state as reported.

FAULT TOLERANCE WITH TRANSACTIONS

Unfortunately, classical transactions cannot simply be applied to processes including operations like manufacturing operations, which have effects on the real world. The point is that the low-level recovery mechanisms for transactions depend on the transactional property of atomicity, which in classical transactions is performed by rolling back data to their original state. This is easy as long as there is enough information about the original values to restore them. Rolling back a physical operation is often enough impossible. These problems have been identified several times[1,2,4] and there was a suggestion to defer the execution of such a physical operation to the end of the enclosing transaction[1]. However, this assumption cannot be made in our environment as requests issued after the completion of a manufacturing operation might refer to results of this operation. An approach for exception handling and replanning in the field of autonomous robots is presented by Meijer[3].

The improvements expected by the use of transactions motivated us to try a new approach and to relax the hard requirement of atomicity as far as necessary while saving as many advantages as possible. For this, a classical transaction processing system must be extended to an extended transaction processing system, or ETPS, in two ways to allow for application dependent failure handling:

First, the executing components' (*Resource Managers*) behavior must be redefined to cover the characteristics of "real actions". Such a redefined component will be called *Physical Resource Manager*, short PRM. It manages the requests from an application to the NC-machines and differs from regular Resource Managers in performing autonomous recovery and in performing a transaction *reset* instead of a transaction rollback. A *reset* means that all nonphysical operations are rolled back (like a classical resource manager does), but for the "undo" of the physical operation there will be only a reset of the machine and unload of the work piece, for the PRM to be ready to process any new incoming transaction.

Second, the way of failure handling must be covered by a separate component, the *Physical Recovery Manager (PRecM)*. In contrast to classical transaction processing applications, failure handling for processes with direct impacts to the real world is application specific. Thus, the PRecM is the entity responsible for *physical recovery* and has to decide how to continue after a failure of a physical operation, trying to finish processing without doing harm to equipment and environment. Both components will be explained later in more detail.

A component which remains unchanged is the *Transaction Manager*. Its main contribution is the management of distributed transactions, i.e. the coordination of resource man-

agers which perform work on behalf of the same transaction. If one resource manager fails irreparably during the execution of a transaction's request, the remaining resource managers involved must be informed so they can reset or rollback their results for this transaction, too, in order to achieve consistency.

The application per se is no integral part of this architecture. In manufacturing, it corresponds to the control system sending requests to the NC-machines resp. to the PRMs representing the machines. However, it must tell the ETPS, which requests should be performed as transaction, i.e. it must know where to set transaction demarcations. This will be briefly described in the next chapter.

The following figure shows the architecture of an extended transaction processing system, designed to cover the needs of a manufacturing environment.

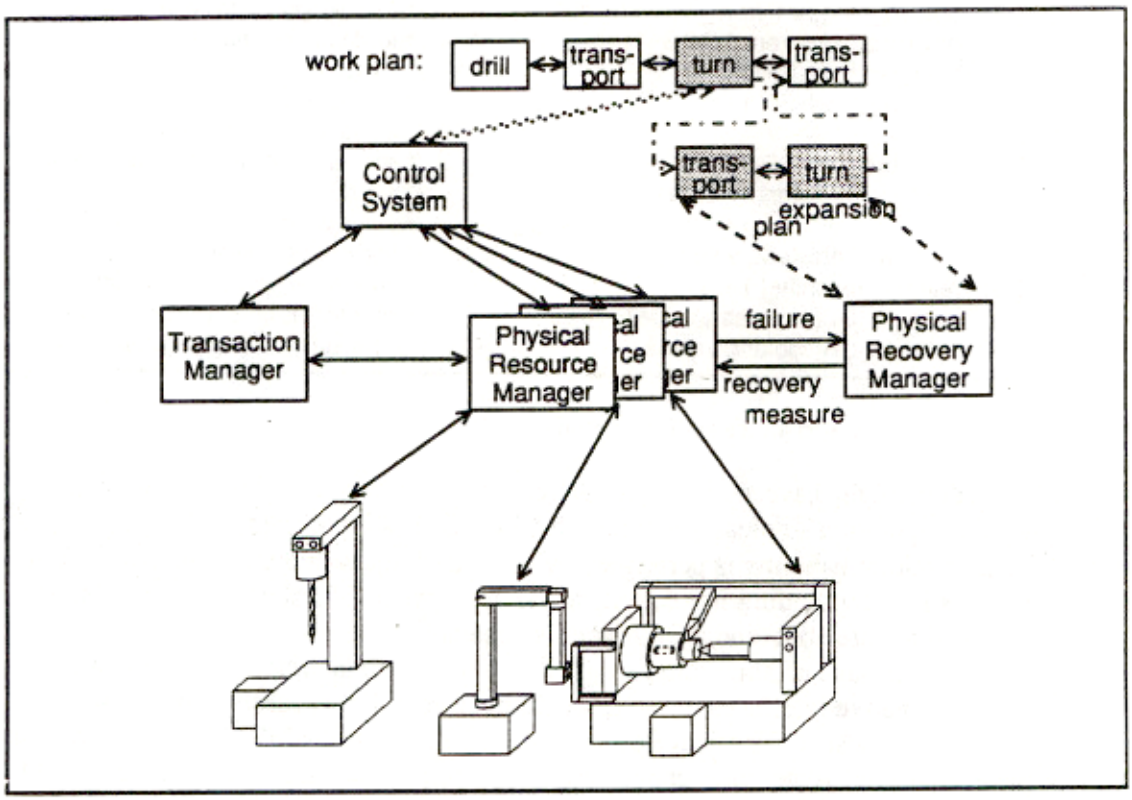


Figure 1. Extended transaction processing system for some sample manufacturing machines.

Here, two questions arise: What does a transaction in manufacturing look like and how are failures handled?

PROGRAMMING TRANSACTIONS

What we want to achieve with transactions in manufacturing is fault-tolerant processing of work pieces. So, where do these transactions come in? In flexible manufacturing systems, a work piece is manufactured by the control system processing the work plan. Besides performing the actual manufacturing operations, preparing and concluding operations like loading programs or providing fixtures are involved. For each physical object in the system - besides work pieces, there are tools, fixtures and pallets to manage - operations must be executed and synchronized with each other. During operation, the ETPS has to manage one separate work plan for each physical object in the system (figure 1 shows just one work plan for one work piece). We assume that the control system, which usually runs

on a dedicated computer, creates so-called "action chains" for each object. An action chain is a sequence of steps to be performed for this object, with each step consisting of related operations. We want to have the nonphysical operations and the manufacturing operation, which comprise the step, performed as a logical unit, i.e. as a transaction. The manufacturing operation is determined from the work piece's work plan und will be performed by running the corresponding NC_ program on the specified machine. The related nonphysical operations will be added by the control system. We explain a transaction's characteristics with the sample step in figure 2:

```
STEP for PROG_1:

1:  upload_program_from_server(PROG_1)   /* load program into control computer      */
2:  download_program(PROG_1)             /* load program into NC-controller        */
3:  bind_program(PROG_1)                 /* something like linking                 */
4:  reserve_machine( )                   /* do this before starting the            */
                                         /* manufacturing operation                */
5:  start_program(PROG_1)                /* start operation and wait for completion */
6:  read_var(register1, value1)          /* register1 contains the actual          */
                                         /* tool wear caused by this operation     */
7:  read_var(register2, value2)          /* register2: consumption of coolant      */
8:  release_machine( )                   /* now, other programs can start          */
9:  write_to_DB(tool wear, value1)       /* save values of tool wear and coolant   */
10: write_to_DB(coolant, value2)         /* consumption for maintenance module     */
```

Figure 2. Sample step for the turning operation

You might have noticed that there is no evidence that this sample step performs a turning operation - unless you know that PROG_1 is a program performing this action. In fact, as failure handling is performed by the underlying system, the control system processing this step by sending its requests to the appropriate (Physical) Resource Managers does not need to care about the NC-program's contents*.

For the sake of simplicity, we used a pseudo-code notation. In reality, a step is coded using the native interfaces of the resource managers. For requests to databases, this will be SQL, for requests to Physical Resource Managers, we use MMS**. For the same reason, we have neglected issues like choosing an appropriate machine - scheduling should be performed by the control system - or establishing connections to the involved (Physical) Resource Managers. This sample step shows several characteristics of a transaction in manufacturing:

- *It contains exactly one manufacturing operation:* We want to make the transaction's outcome depend on the outcome of this operation. If there is more than one manufacturing operation, which one should be the determining one? Allowing transactions to contain more than one NC-program would make the PRM's failure handling algorithm too complex.
- *It is distributed*: operations are executed in various resource managers. In the sample step are involved: a file server containing NC- programs, an NC_machine performing the manufacturing operations, and a database which is used to store process values for evaluation by the control system's maintenance module.

* It should not do that in regular FMS, too. Otherwise it becomes pretty hard to make such a system flexible at all.

** MMS, Manufacturing Message Specification, is designed to allow for open communication in manufacturing and is the application protocol of the Manufacturing Automation Protocol (MAP) profile.

- *It consists of related requests:* The step's requests relate all to the carrying out of the same manufacturing operation - this is why they must be performed as a unit. This characteristic is used both for processing the work plan and for determining recovery measures: It allows to process steps of work plans like independent units of a modular construction kit. Moreover, only related requests should be composed into a transaction. Including unrelated actions would make the outcome of the whole manufacturing operation unnecessarily depend on irrelevant aspects.
- *It deals with temporary values:* A transaction which, after a program run, wants to read from registers which then contain process dependent values must keep other transactions from starting their programs until these values have been read. Otherwise, the registers might be overwritten during the run of the next program. This is what the "reserve_machine" and "release_machine" requests are for. One might want to solve this problem by not allowing interleaving processing of requests of different transactions. Such a *serialization*, however, would cause unnecessary machine idle times.
- *It is sequential:* That is just like manufacturing is - a work piece can be only at one location at a time. If there is any parallelism, it must be contained in the NC-program. For example, there are machines which can perform manufacturing operations on one work piece in parallel. If operations on different work pieces are to be processed in parallel, the corresponding action chains must be synchronized by the control system.
- And what is most important: *There is no failure handling in the application code* - not even hidden in the NC-program. This is what a transaction processing system does for you.

HANDLING FAILURES

In general, failures are handled by the PRM, which might be supported by the PRecM. The PRM tries to hide failures from the application and to perform recovery on its own.

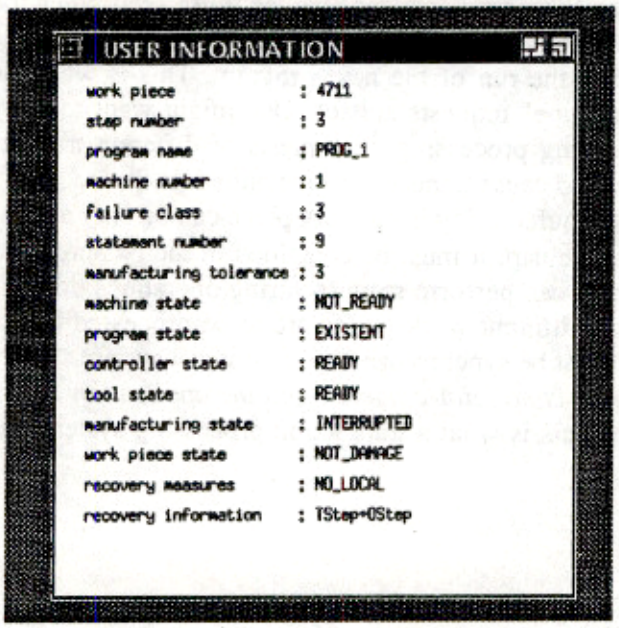
For a failure during a nonphysical operation on the PRM, in most cases it will simply undo and redo the operations performed so far, except for the physical operation, which will be skipped, if there was one already. Then, the PRM can simply continue processing transactions' requests. In order to be able to perform the proper undo- and redo- actions, the PRM must safely store the corresponding information. Additionally, to provide isolation for concurrent transactions, it keeps locks for the managed objects on the NC-machine's controller. (Of course, the operation of the PRM is more complex than it can be described here. A detailed description can be found in a separate paper[5]).

If the failure occurred during a physical operation, the PRM will call the PRecM for help, together with information about the actual system state. To determine the appropriate actions, the PRecM uses facts and rules: *Facts* can be characteristics of machine, tool, work piece, application, and failed operation. They are known in advance (describing static properties), are reported when the failure occurs, or must be explicitly requested. Special attention must be drawn to the features of physical operations. *Rules* incorporate general heuristic strategies to evaluate the available information and find an acceptable solution. These facts and rules must be given to the PRecM at installation time, but they can be selected or modified during operation as well.

If the failure can be handled locally, i.e. on the failed machine, the PRecM simply tells the PRM what to do next (i.e. to restart or to resume the failed program). Otherwise, it will tell the PRM to *reset* the transaction. Then, the control system will stop processing the current transaction. If other steps can be performed, for example, if there is a substitute machine to continue processing of the work piece, the PRecM extends the particular work

piece's work plan (like shown in figure 1), and the control system can continue processing the work piece. If there is no way of failure handling, the PRecM inserts a so-called *abort step* into the work plan, which stops the processing of the work piece[6].

Figure 3 shows the information available to the PRecM and the measures it determined from that information. If it did not receive sufficient information from the calling PRM and could neither get it by interactively interrogating the operator, it assumed, to be on the safe side, the worst case: if, for example, there is no information about the machine's state, the PRecM has to assume that the machine is not operable any longer.



For this instance of failure, local recovery is not possible. Thus, the failed transaction must be reset. However, performing a transport of the work piece to another machine (TStep) and processing the original step (OStep) again will do.

Depending on the encoded rules, more or less strict safety rules can be chosen. It is, for example, possible to restrict failure handling for some actions to certain measures or to require that certain measures have always to be performed.

Figure 3. Recovery measures determined by the Physical Recovery Manager from available information

PROSPECT

A prototypical implementation is currently under development, with PRM-kernel and PRecM already finished. We have been performing functionality tests with a simulation environment and plan to integrate real machine tools, too. We are convinced, that transactions are a mighty means to increase data, and thus process, reliability. Combined with application adaptable failure handling, an operator could be assisted when deciding how to go on with processing a work piece. All in all, a higher degree of automation will be achieved.

REFERENCES

1. J. Gray, The Transaction Concept: Virtues and Limitations, *in*: Proc. 7th Int. Conf. on VLDB, Cannes (1981).
2. S. Jablonski, H. Wedekind and G. Zörntlein, Fehlerbehandlung in Flexiblen Fertigungssystemen (FFS), *Informatik Forsch. Entw.* 3:53-63 (1988).
3. G.R. Meijer. "Autonomous Shopfloor Systems - A study into Exception handling for Robot Control", Ph.D. thesis, University of Amsterdam (1991).
4. R. Pausch. "Adding Input and Output to the Transactional Model, CMU, Ph.D. thesis (1988).
5. U. Schmidt, Transaktionskonzepte in der Fertigung, *in*: Tagungsband Datenbanken in Büro, Technik und Wissenschaft (BTW), 3.-5. März, Braunschweig, S. 104 - 123 (1993).
6. U. Schmidt, Physical Error Recovery for NC-machines. *in*: Proc. 9th CIM-Europe Annual Conference, May 12-14, Amsterdam, pp. 170-179 (1993).

004 Dependent Failures

Chair: M. Haim, Rafael

CCDAT, an Automated Tool for Common Cause Failure Data Analysis and Parameter Estimation

F.R. Hubbard (FRH); A. Mosleh (U. Maryland)

Development of a Data Base of Common Cause Failure Events at U.S. Nuclear Power Plants

D. Rasmuson (USNRC); A.Mosleh (U.Maryland); F.Marshall, K. Kvarfordt (EG&G)

CCDAT, AN AUTOMATED TOOL FOR COMMON CAUSE FAILURE DATA ANALYSIS AND PARAMETER ESTIMATION*

Frank R. Hubbard,[1] Ali Mosleh[2]

[1] FRH, Inc.
P.O. Box 65359
Baltimore, MD 21209

[2]Department of Nuclear Engineering
University of Maryland
College Park, MD

ABSTRACT

This paper describes a computer program, ***CCDAT***, designed to produce plant specific common cause failure parameter values using the data of EPRI report TR-100382[1] and methods of EPRI/NRC common cause guidebook (NUREG/CR-4780[2]) enhanced by adding techniques from the more recent NRC Common Cause Guidebook (NUREG/CR-5801[3]). The tedious process required to tailor the application of the recorded common cause events to the plant being analyzed and producing parameter values for either of the three most well known methods of incorporating common cause failures into risk assessments is automated. In addition, ***CCDAT*** allows the user to keep track, in a consistent way, of his own (plant-specific) common cause events and combine these events with the generic data.

INTRODUCTION

Methodology (see for instance NUREG/CR-4780[2] and NUREG/CR-5801[3]) has existed for several years for producing a common cause failure frequency for use in probabilistic risk assessment (PRA) fault trees from experiential data. The Electric Power Research Institute (EPRI) report TR-100382 ("CC Database report") cataloged a number of common cause events and suggested an impact vector for each using the approach of NUREG/CR-4780[2]. However, for plant specific applications the effort to tailor events from the plant at which it occurred to a plant being analyzed is still

---

* CCDAT was developed under the sponsorship of the Electric Power Research Institute. It is the property of EPRI and its member utilities. Members may obtain a copy of the code and its user's manual by contacting the EPRI Distribution Center, 207 Coggins Drive, Pleasant Hill, CA 94523, (510) 934-4212.

considerable. This process involves adjustment of the event impact vectors for differences in redundancy level ("mapping" process) as well as for differences in design and operating philosophy.

The EPRI CC Database contains 200+ recorded common cause events which can serve as a representative set of common cause failures when taken along with their independent failures.

Previous "generic" lists of common cause parameter values[2] were deliberately set high in order to be used as screening values. Unfortunately to date these values were often used directly without being tailored to the plant being analyzed. This tailoring was necessary to take into account differences in equipment and operating procedures. For instance, a common cause event at a plant with a two train high pressure injection system could produce a different effect in a plant with a three train system. How different this effect is would depend on the likelihood of the same coupling mechanism occurring as well as the different system size (redundancy level). By tailoring each generic event to match the conditions in the plant and system being analyzed., a plant specific version of the generic data base will be produced. To this generic/plant-specific data must be added the events which actually occurred at the plant being analyzed (if they are not among those in the CCF database). Then the impact vectors from all such events can be combined to calculate a plant specific common cause beta factor.

DESCRIPTION OF *CCDAT*

CCDAT eliminates the mathematical tedium involved in tailoring generic common cause data to a particular plant. It does this by automating the process in the EPRI and NRC procedures[1,3] using a Microsoft® EXCEL 4.0 add-in, i.e. a set of linked spreadsheets and macros. It includes the common cause events from the CC Database and the algorithms from the two CCF handbooks. It includes more up-to-date values for the impact vectors in the CC Database report as well as classifications of events in terms of root cause and coupling factor not found in that report.

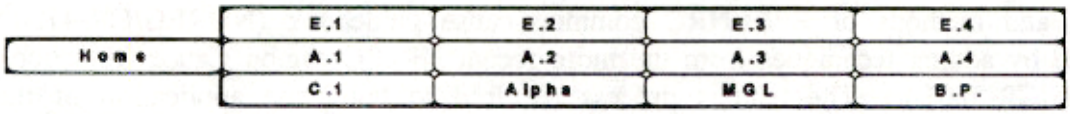


Figure 1. Screen Locator Grid

CCDAT is started by clicking on a Microsoft® Windows™ icon which loads EXCEL and autostarts ***CCDAT***. The add-in files are loaded and the first screen is opened. Navigation through the subsequent screens is done by using mouse actuated buttons on a "screen locator grid" (see Figure 1). Buttons are also used to activate extensive context sensitive help dialog boxes and to open dialog boxes which give choices which are activated by double clicking.

CCDAT was programmed in EXCEL macros and spreadsheets because of EXCEL's capacity to manage a reasonable sized data base and because of the ease with which the programming could be done. Programming was easy because all actions were segmented into small routines started by clicking on buttons. The macro which performed each action was clearly identified by the macro name assigned to a particular button. Evaluations which were to take place immediately were performed in the screen spreadsheet as soon as the enter key was pressed on a data entry cell. Results can either be printed or saved to a spreadsheet which can be read by normally operating EXCEL to form results tables.

CCDAT starts with a Home screen from which the user has a choice of three branches or sets of four screens each:

1. the first set of screens (E.1→E.4) allows the utility to take all the common cause events and choose the ones which are applicable to the plant being analyzed and enter that data into a system and alignment specific data base.
2. the second set of screens (A.1→A.4) allows further modifications to be made to the alignment data bases, for instance, to make the set of events for a particular system to be mapped up to 3 instead of 2 trains.
3. the third set of screens (C.1→B.P.) allows the conversion of failures of different orders into common cause parameter values for either multiple Greek letter (MGL), basic parameter (B.P.), or alpha factor method (Alpha).

DESCRIPTION OF *CCDAT* SCREENS

Figure 2 shows one of the generic data tailoring screens, the one which allows generic assessments of the event data (done by the code authors) to be changed if the user disagrees with their interpretation. Most tailoring will be done in the screen shown in Figure 3.

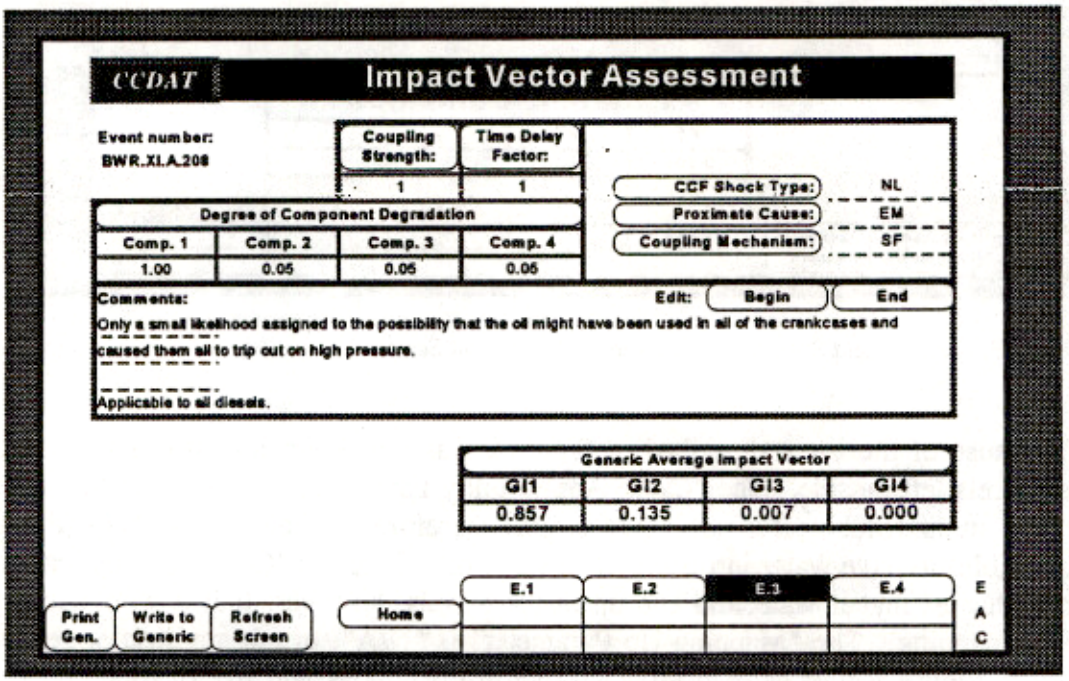


Figure 2. Generic Impact Vector Assessment Screen

In Figure 2 the "Degrees of Component Degradation" fields contain numbers from zero to one which reflect the degree to which each component involved in the event can be said to be failed. (A one means completely failed and a zero means not failed at all.) The "Coupling Strength" and the "Time Delay Factor" fields provide a place to enter fractions which indicate how likely it is that the multiple degraded components failed because of a common cause. The "Average Impact Vector" is calculated by combining the number and degree of failure of each involved component with the coupling and time delay factors. In the example in Figure 2 only one component was judged to be completely failed while the other three were judged only slightly likely to have failed. The time delay was one because the other components if they did fail would have failed

shortly after the first; the coupling strength is one because if more than one component did fail it would have been because of the same cause, similar oil in the crankcase. The average impact vector indicates that there was about 0.86 single failures during this event, 0.135 double failures, 0.01 triple failures, and only a negligibly small chance of four components having failed during this event due to the same cause. (There were four redundant diesels in the system.)

Figure 3 shows the screen on which the average impact vector in Figure 2 is tailored to fit one of the systems (or alignments of a system) at a particular plant. The sample shown is for an emergency power system consisting of two diesel generators (see "Population Exposed in S/L Model").

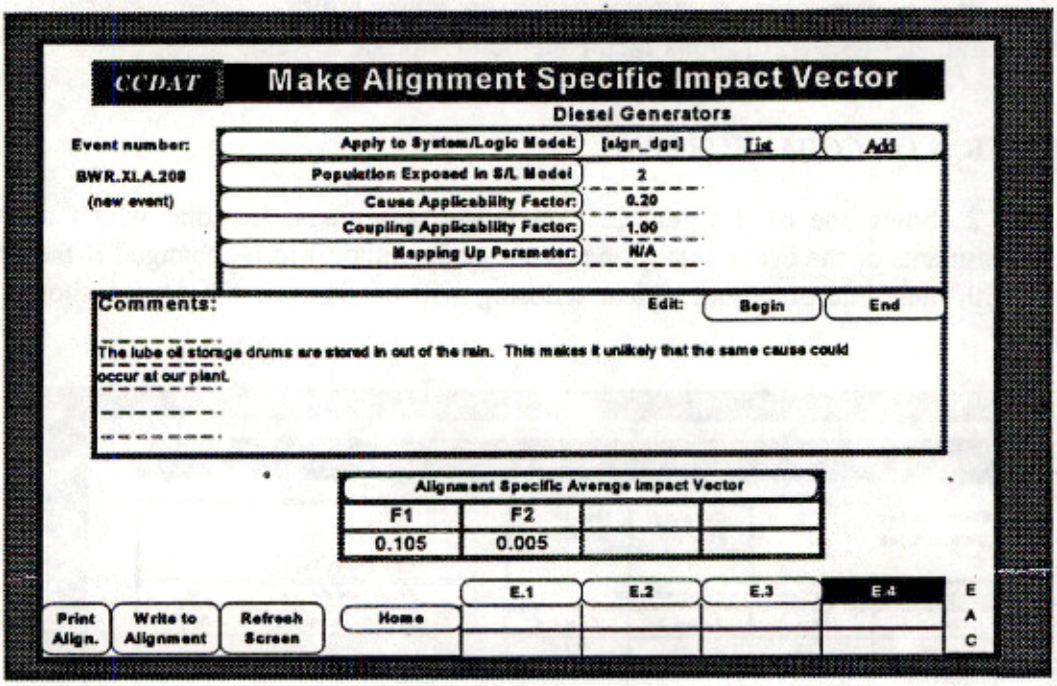


Figure 3. Alignment Specific Impact Vector Assessment Screen

The cause of the event described in Figure 2 was rain water intrusion into lube oil storage barrels left outside. The "Cause Applicability Factor" of 0.2 indicates that at the plant being studied, lube oil is not stored outside therefore it is much less likely (though not impossible) to have water intrusion. The value of 1.0 for the "Coupling Applicability Factor" indicates that if water did end up in the barrels, however, that it would lead to the diesels tripping. The "Mapping Up Parameter" is "N/A", or not applicable, because the event in Figure 2 must be mapped down (not up) from a system size of four to one of two redundant components. The "System Specific Average Impact Vector" is calculated by combining the applicability factors with the mapping down results. The F1 value in Figure 3 is analogous to the GI1 value in Figure 2. It estimates how likely it was that the occurrence of this event at the plant being studied would have resulted in a single failure. F2 indicates the likelihood that the event would result in a failure of both diesels due to the same cause.

After developing a system or alignment specific impact vector for each generic and plant specific event, one of the three screens like the one shown in Figure 4 is used to estimate a plant specific common cause parameter value. The screen shown in Figure 4 is the one for the multiple Greek letter method. *CCDAT* also provides the user with the choice of estimating the basic parameter or alpha-factor parameter values on two other screens.

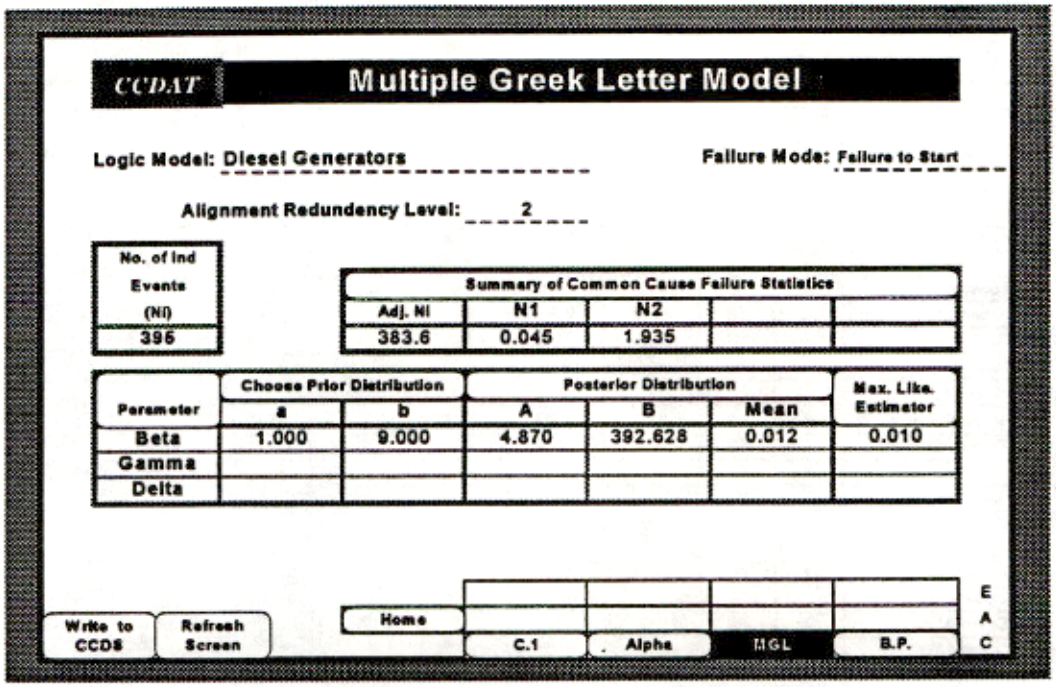


Figure 4. Multiple Greek Letter Parameter Generation Screen

The number of independent failures is required to calculate the CCF parameter values. (The basic parameter model needs the number of successes as well.) The common cause failure fractions, the F1 through F4 values from Figure 3 are summed over all events included in the alignment data base. The "Adjusted NI" value in Figure 4 is the sum of all singles failures (F1 values) and the number of independent events weighted by the generic system size. The N1 value is the sum of all of the single failures, the N2 value the sum of all the doubles, etc.

All three multiple Greek letter model parameters, beta, gamma, and delta, can be calculated using this screen. However, only the factors needed for the specified "Alignment Redundancy Level" will be calculated. For the example shown in Figure 4 of a system redundancy of two, only the beta factor is needed. A prior distribution is provided by the code authors to allow an estimate to be used even when the data is scarce. Little "a" and "b" are the parameters of beta-type distribution suggested for use as a prior. When this prior distribution is combined with the common cause failure statistics, a posterior distribution is generated. Large "A" and large "B" are the parameters of a beta-type distribution for the posterior. The mean value of this posterior is also shown. A maximum likelihood estimator value which does not depend on an estimated prior distribution is also calculated.

Table 1 shows values calculated for one plant using *CCDAT*. It compares these values to those obtained from NUREG/CR-4780 and to the values which would be obtained using non-conservative priors and the assumption that none of the industry or generic events could be tailored to the plant being analyzed. This plant had only a few common cause events of its own which were used to update the non-conservative priors. As can be seen in Table 1, more than half of the NUREG/CR-4780 values were higher than the values calculated by *CCDAT*.

Table 1. Common Cause Parameter Results Produced by *CCDAT* for a Sample Plant

Parameter Type:			Beta			Gamma		Delta	
Component Type	Anal. Pop.	Fail. Mode	Previous Mean	CCDAT Mean	4780 Est.	Previous Mean	CCDAT Mean	Previous Mean	CCDAT Mean
Air Operated Valves	2	FD	0.07	0.063	0.11	0.14	0.07	0.178	0.178
Check Valves	2	FD	0.01	0.067	0.06	0.284		0.14	
Check Valves	4	FD	0.01	0.104	0.06	0.284	0.264	0.14	0.468
Circuit Breakers	2	FD	0.07	0.099		0.178		0.14	
Circuit Breakers	4	FD	0.07	0.107		0.178	0.229	0.14	0.288
Diesel Generators	3	FS	0.001	0.012	0.05		0.133		
Diesel Generators	3	FR	0.01	0.023	0.05		0.122		
HVAC Chillers	2	FS		0.05	0.11				
HVAC Chillers	2	FR		0.071	0.11				
Reactor Trip Breakers	4	FA	0.07	0.084	0.19		0.112		0.155
Motor Operated Valves	4	FD	0.2	0.032	0.08	0.4	0.229	0.24	0.416
Safety Injection	2	FS		0.043	0.17				
Safety Injection	2	FR		0.021	0.17				
LPSI/SDC	2	FS		0.038	0.11				
LPSI/SDC	2	FR		0.03	0.11				
Containment Spray	2	FS		0.251	0.05				
Containment Spray	2	FR		0.107	0.05				
Motor Driven AFW	2	FS		0.195					
Motor Driven AFW	2	FR		0.057					
Turbine-Driven Pumps	2	FS	0.12	0.048	0.03				
Turbine-Driven Pumps	2	FR	0.01	0.034	0.03				

CONCLUSIONS

This method was applied to three plants during the beta-test phase. Each of these plants and its IPE was of a different type and therefore each application produced different relative results.

1. In the first case, making values plant specific showed that the way in which the CCF values were applied in the IPE was not detailed enough to account adequately for the common cause combinations. Even though the values which were produced were sometimes lower, the overall impact was not what was expected.
2. In the second case, the utility had overridden the normal linked fault tree approach and used the CCF guidebook methodology and events and tailored using an analyst's code and by hand to their plant. These values confirmed in general the ***CCDAT*** calculations. However, the extensions contained in ***CCDAT*** made it easier to document the judgments which had to be made about each event.
3. In the third plant analyzed, it was found that ***CCDAT*** helped the utility rationalize values that were both too low and too high, because generic data was used and only updated for those cases where plant specific common cause events existed.

In all cases using ***CCDAT*** allowed the data and the CCF handbook algorithms to be tested in ways that they had never been tested before. It is now much easier to do many calculations using ***CCDAT***. With ***CCDAT*** available there is no longer any reason to use conservative or non-plant specific values for common cause parameters.

REFERENCES

1. **Fleming, et. al., A Database of Common-Cause Events for Risk and Reliability Applications,** EPRI TR-100382, June 1992.

2. **Mosleh, A., et. al., Procedures for Treating Common Cause Failures in Safety and Reliability Studies,** Volumes 1 and 2, NUREG/CR-4780, EPRI NP-5613, 1989.

3. Mosleh, A., **Procedures for Analysis of Common Cause Failures in Safety Assessment of Nuclear Power Plants**, USNRC, NUREG/CR-5801, May 1992.

4 Hubbard, F.R., A. Mosleh, **Common Cause Data Analysis Tool (*CCDAT*) User's Manual**, EPRI TR-102747, August 1993.

DEVELOPMENT OF A DATABASE OF COMMON CAUSE FAILURE EVENTS AT U.S. NUCLEAR POWER PLANTS[1]

Dale M. Rasmuson[2]
Ali Mosleh[3]
Frances Marshall[4]
Kelly Kvarfordt[4]

[2]Division of Safety Programs
Office for Analysis and Evaluation of Operational Data
U.S. Nuclear Regulatory Commission
Washington, D. C. 20555

[3]Department of Materials and Nuclear Engineering
University of Maryland
College Park, Maryland 20742

[4]EG&G Idaho, Inc.
P.O. Box 1625
Idaho Falls, Idaho 83415

INTRODUCTION

A generic conclusion from PRAs of nuclear power plants is that common cause failures (CCFs) are a significant contributor to the unavailability of safety systems. Efforts in the past ten years to improve our ability to understand and model CCFs have produced several models, procedures, computer codes, and databases. In each category, weaknesses and shortcomings have been discussed to various degrees in the literature.

---

[1] The opinions and viewpoints contained in this paper are the author's personal ones and do not necessarily reflect the criteria, requirements, and guidelines of the U.S. Nuclear Regulatory Commission.

Lack of common cause failure event data is still a major problem, though significant progress has been made particularly with the publication of Reference 1. Two of the known problems are: 1) limitation of the database period to approximately before 1982, and 2) the lack of details regarding independent events. In the area of data classification and analysis and model parameter estimation, the detailed procedures of References 2 and 3 have been viewed as too time consuming, despite wide acceptance of the basic approach.

Alleviating these problems is one of the motivations behind an AEOD-sponsored project with the objectives of: 1) developing a comprehensive database of common cause failure events using several data sources such as Licensee Event Reports (LERs), which are contained in the Sequence Coding and Search System maintained by the Oak Ridge National Laboratory, and the Nuclear Plant Reliability Data System (NPRDS), and 2) automation of data analysis and parameter estimation procedures of References 2 and 3. This paper summarizes the achievements of the project in both areas and offers some conclusions based on analysis of a subset of the data. The steps in the CCF event identification process and the LER and NPRDS search strategies are also summarized.

CCF EVENT CLASSIFICATION AND GUIDANCE

The first task, needed for the CCF event database effort, was the development of specific guidance to be used by the data analysts to determine common cause failure events. The basic concepts and characteristics, which had been defined in a PRA context, were translated into engineering terms with examples to illustrate the definitions and concepts. The initial CCF event criteria include similar components, same failure mode, and failure of components involved in a short time interval. These characteristics are necessary for an event to be considered a common cause event. However, they are not sufficient. That is, the failures of the components must involve a shared cause.

The next task was to revise existing classification schemes for use in the engineering review and with the database software. The classification schemes suggested in Reference 1 were picked as a starting point. One criterion used in the modification of the classification schemes was to make them simple and practical. Table 1 contains the modified failure cause/mechanism classification scheme. These coding schemes will help the engineer classify the events in a consistent manner. In addition, they will provide the database user with useful information about the CCF events.

In addition to these efforts, definitions and coding schemes for coding coupling strength (a measure of how closely the coupling factor ties two components together), time delay factor (how close in time the multiple failures occur), and failure mode applicability factor (the likelihood the failure mode will affect multiple components) were also developed and tested. These concepts and definitions are documented in a

Table 1. Event Cause/Mechanism Codes

State of another Component. The cause of the state of the component under consideration is the state of another component. Examples are loss of power and loss of cooling.

Design/Manufacturing/Construction Inadequacy. This category of causes encompasses actions and decisions taken during design or manufacturing or installation of components both before and after the plant is operational.

Procedures Inadequacy. This category refers to ambiguity, incompleteness, or error in procedures for operation and maintenance of equipment. These include inadequacy in construction or modification procedures, and administrative, operational, maintenance, test, and calibration procedures.

Human Actions, Plant Staff Error. represents causes related to errors of omission and commission on the part of plant staff, such as failure to follow a correct procedure. This category includes accidental actions, and failure to follow procedures for construction, modifications, operation, maintenance, calibration, and testing.

Abnormal Environmental Stress. This category includes all causes related to a harsh environment that is not within the components design specifications. Specific mechanisms include: chemical reactions, electromagnetic interference, fire/smoke, impact loads, moisture (sprays, floods, etc.,) radiation, abnormally high or low temperature, vibration load, and acts of nature.

Internal. The component state is due to malfunctioning of something internal to the component as a result of normal wearout or other intrinsic failure mechanism. It includes the influence of the ambient environment of the component. Specific mechanisms include erosion/corrosion, internal contamination, fatigue, and wearout/end of life.

Other. Cause is known, but it is not covered by the other categories in this scheme.

Unknown. The cause of the component state cannot be identified.

report which will be published.

COMMON CAUSE EVENT CLASSIFICATION PROCESS OVERVIEW

Figure 1 contains the major steps in the CCF event classification process. The initial step is to identify those components for which CCF events are desired. The initial list was obtained from identifying the CCF events that are risk-important in several PRAs. The list includes such components as batteries, auxiliary feedwater system pumps, and emergency diesel generators. At this time, only components which are typically modeled in PRAs are being considered.

The next step is to perform CCF searches using available data sources. The main data sources available to the NRC for failures are LERs contained in the SCSS and NPRDS. The search strategies were developed using the basic characteristics of a CCF event described above. The output from the search strategies are "potential" common cause failure events.

The potential CCF events are then screened by engineers to determine when all the criteria for a CCF event are satisfied. The engineers read the failure narrative and cause descriptions of the NPRDS reports of the failures comprising the CCF event. The LER (full-text) is read for the potential CCF events identified by SCSS. Using the developed coding schemes, the time delay factor, coupling strength, failure mode applicability, and component degradation are determined.

The output from the engineering review are coding forms which contain the information related to the total and partial common cause failure events. This information for the events, from NPRDS and SCSS, are coded into the CCF event database for use by the NRC staff.

The database software allows the user to perform searches of the CCF events to meet the specific needs of the analysis. The user then has the choice of using the basic parameter model, the multiple Greek letter model, or the alpha factor model for quantifying the CCF basic event related to the particular component.

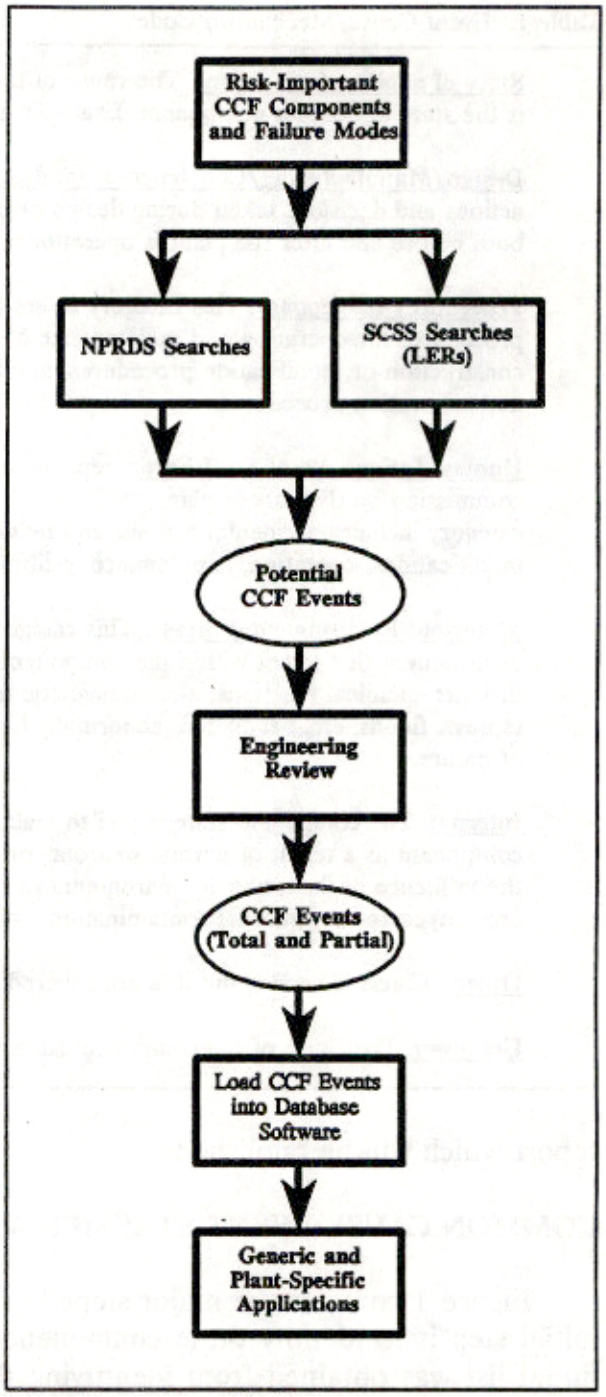


Figure 1. CCF Event Classification Process

NPRDS SEARCH STRATEGIES

In this effort, the NPRDS was the first data source used for identifying common cause failure events. Since each failure record in NPRDS refers to one component only (records are component-based), a set of criteria was developed to identify related component failure events as common cause failure candidates. Among the primary criteria were time proximity and similarity of causes.

Another factor that complicated the identification of CCF events was the definition of the component boundary. Since the primary purpose of the database is

to focus on components used in PRAs and reliability studies, PRA component definitions are used. Thus, the component may be composed of several NPRDS "pieceparts." For example, the auxiliary feedwater (AFW) pump is composed of the pump, the driver (turbine, motor, or diesel), and a circuit breaker (where appropriate).

A computer code was developed to aid in screening the large number of events that can be found in NPRDS for each component category. So far, events involving auxiliary feedwater pumps for the period 1984-1992 have been classified and analyzed. A draft document containing NPRDS search guidelines has been developed.

One qualitative result from analyzing the AFW pump data is that many of the same failure and coupling mechanisms which were identified in Reference 1 for the time period ending about 10 years ago are observed in the new data. This suggests that things have not changed much in the past 10 years as far as AFW pump common cause failures are concerned.

LER SEARCH STRATEGIES

The SCSS search algorithm utilizes the special features of SCSS to help identify potential CCF events. The main criteria are the following: (1) any actual or potential failures within a system of multiple components coded on the same portion of the event, (2) any actual or potential failure of one train of a system that is linked to a failure in another train, (3) any actual or potential failure of a component with at least one additional actual or potential failure of the same type of component coded later in the SCSS matrix, and (4) any fabrication/manufacturing deficiency resulting in an actual or potential failure within the system.

In addition to the above conditions, SCSS has the capability of finding events that occur within a certain time interval of each other. This option, called "windowing," has been combined with the above criteria to aid in the identification of potential CCF events. All searches can be limited to a given time period, system, and/or component type. The results of these searches are then read by engineers to determine which events satisfy all the CCF-event criteria. The full-text LER is utilized for this effort.

CCF COMPUTER CODE

The computer code CCF, which has been developed as part of this activity uses the impact vector method of Reference 2 and the approach introduced in Reference 3 for assessing the event impact vector based on physical characteristics of the event. These include component degradation parameter, time delay factor, and coupling factor strength. In addition, the software allows the user to modify the generic event impact factors for plant-specific applications, including mapping the impact vectors to account for system size difference between the plant in which the event occurred and the plant the data are being modified for. Other features of the software include

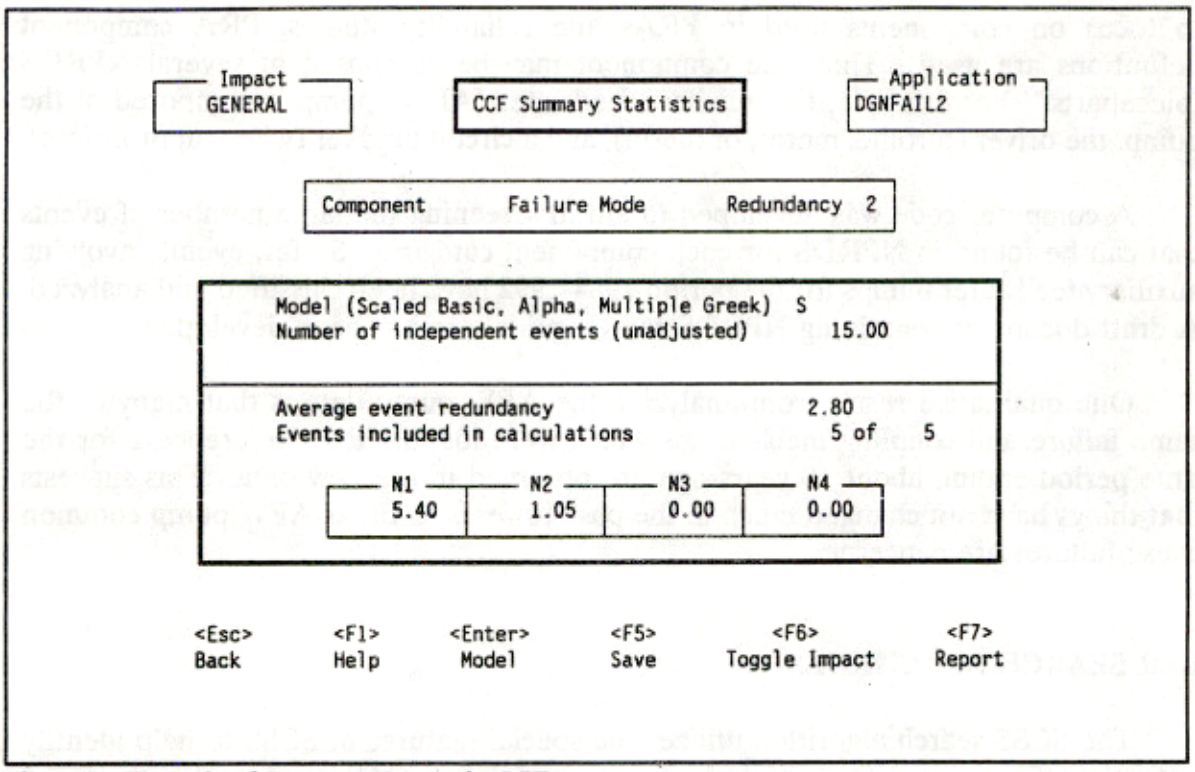


Figure 2. Example of Summary Screen in CCF.

estimation of the parameters of the parametric models including the scaled basic parameter model, the alpha factor model, and the multiple Greek letter model. Figure 2 is an example of one of the screens from the CCF software. This screen shows the final event statistics after event screening analysis for a particular component.

Current efforts are directed toward identifying CCF events and loading them into the database for selected components. The database will be updated on a periodic basis. An uncertainty module is being added to the software in FY 1994.

REFERENCES

1. K. N. Fleming and A. Mosleh, *Classification and Analysis of Reactor Operating Experience Involving Dependent Events*, EPRI NP-3967 (June 1985).

2. A. Mosleh, et al, *Procedures for Treating Common Cause Failures in Safety and Reliability Studies*, NUREG/CR-4780, Volume 1(January 1988) and Volume 2 (January 1989).

3. A. Mosleh, *Procedure for Analysis of Common-Cause Failures in Probabilistic Safety Analysis*, NUREG/CR-5801 (April 1993).

005 Advances in Human Reliability Analysis

Chair: G.W. Parry, NUS

A Procedure for the Analysis of Errors of Commission in a PSA

G.W. Parry, J. Julius, E. Jorgenson (NUS); A. Mosleh (U. Maryland)

Human Reliability Analysis for Seismic Events

T.V. Vo, T.M. Mitts (PNL); C.M. van Bujjtenen, E.Wingo (Westinghouse Savannah Rvr.)

Evidence of the Need to Model Errors of Commission in Risk Assessments for Varied Environments

D.I. Gertman, L.N. Haney, L.T. Ostrom (INEL)

Application of HRA in the Commonwealth Edison Individual Plant Examinations

L. Soth (Commonwealth Edison)

A PROCEDURE FOR THE ANALYSIS OF ERRORS OF COMMISSION IN A PSA

G.W. Parry[1], J.A. Julius[2], E. Jorgenson[2], and A.M. Mosleh[3]

[1]NUS
910 Clopper Road
Gaithersburg, MD 20878
[2]NUS
1303 So. Central Avenue
Kent, WA 98032
[3]University of Maryland
Chemical and Nuclear Engineering Department
College Park, MD 20742

INTRODUCTION

One of the criticisms often leveled at PSAs is that they do not address errors of commission. This is a somewhat imprecise statement, since the classification of an error as one of omission or one of commission is a function of the context in which the error is being modeled, and the same error could be classified differently according to the purpose, scope, and level of detail of the analysis. However, within the context of a PSA, the errors of commission of concern, and those at which the criticism of PSA is leveled, can be defined as those inappropriate acts, performed by the plant personnel, that cause, or increase the likelihood of undesirable scenarios, and are therefore identified by their impact on the success or failure of systems or functions designed to mitigate the impact of transients or accidents.

This paper discusses an approach to the analysis of those errors of commission that may be committed by the control room operating crew following an initiating event, and incorporation of their impact into an existing PSA. It is recognized that the range of possibilities of inappropriate actions is in principle unconstrained, and therefore the spectrum of potential errors of commission is very large. Therefore, a practical approach to the analysis of such errors must involve systematically and logically reducing that number to a manageable set.

The philosophy applied in the work upon which this paper is based is essentially one of a successive and focussed screening of the very large number of scenarios in which operators interact with the plant in order to identify those cases where the likelihood of the scenario involving potential errors of commission with significant

consequences is relatively high. The next section describes the general approach that was adopted, and it is followed by an example analysis procedure for one of the error types recognized.

OVERVIEW OF APPROACH

The first concern in performing an analysis of errors of commission is identification of opportunities for error. In the current work, only rational behavior is considered. Thus, operators are assumed to interact with the plant only when they are required to do so. For modern control rooms, and up to date, symptom based procedures, if the conditions are optimal, the likelihood of significant error is minimal, and therefore a plausible approach to the identification of potential error-inducing scenarios is to search for those scenarios in which conditions are not optimal. Decisions are made by the control room crew on the basis of the information available to them. Therefore, it can be argued that for an error of commission to be made, the crucial factor is that there be something about the scenario that either distorts the available information so that it looks like the signature of another scenario for which the inappropriate action would indeed be appropriate (e.g., instrumentation failure), or conditions are such that the operators are inclined to censor information to match a more familiar scenario signature. These assumptions are consistent with the similarity matching, and, to a lesser extent, frequency gambling processes that are claimed by many (e.g., Reason (1990)), to be the underlying processes that drive human cognitive behavior. The signatures of the different scenarios can be characterized by the values or trends of critical parameters, as those are the cues that the operators rely on to initiate an interaction with the plant.

The likelihood of committing an error is affected by many performance influencing factors. For example, performance influencing factors such as the operators' expectations reinforced by training, and the availability of instrumentation and/or equipment can be taken into account in this initial screening for opportunities for error as characterizing mechanisms that distort information. Ambiguities, or unclear directions in the procedures can be considered as additional distorting mechanisms. When accidents develop slower or faster than the scenarios used to baseline the procedures, annunciators may occur in a different sequence than expected and provide still more ways to create distortion.

Once an opportunity for an error has been identified, the impact or consequence of the error must be evaluated. Only those errors that can significantly impact the mitigation of the plant disturbance need be considered. Another factor that must be taken into account is that, in most circumstances, the inertia of the plant does not lead to immediate failure of a function or specific equipment, but there is an opportunity for recovery. Thus an error only becomes an error in the PSA sense if it is unrecovered before there is irreversible damage. Thus, another important aspect of the screening is the search for opportunities for identification and rectification of errors (see for example, Parry, 1994). The operator's expectations, the strength of diagnosis, and memory of recent actions are all influential in the recovery process.

In the post-initiating event phase, three basic error types are considered:

- Global Misdiagnosis expressed as a selection of an incorrect or inappropriate procedure which has the potential to become the underlying reason for further "errors" or inappropriate actions as the accident develops if it is not recognized and corrected.

- Local Misdiagnosis expressed in the form of a commission error at the level of an interaction with a system (e.g., incorrectly disabling a piece of equipment of a function). This may, if not recognized and recovered, cause an initiator (e.g., loss of a support system), may be an inappropriate act during the course of the accident given an initiator (e.g., activating a system erroneously), or may simply result in the unavailability of the erroneously deactivated equipment.

- Slip (Unintentional Error of Commission) expressed in terms of an error in executing a procedural step and characterized by substitution of an incorrect action for the correct action. If not recoverable in time, this may result in the same results as the local misdiagnosis above.

Different procedures have been developed for the analysis of the three error types, although for local misdiagnosis and slip the method of identifying scenarios that require operator action is the same. The next section summarizes the procedure used to analyze global misdiagnosis errors, for a plant having Westinghouse style emergency operating procedures.

A PROCEDURE FOR ANALYSIS OF GLOBAL MISDIAGNOSIS

In the Westinghouse style procedures, the diagnosis of the accident type is essentially performed in the E-O procedure. Therefore, the potential for global misdiagnosis is evaluated by applying the following steps to the E-O plant procedure, to identify the possibility of transfers to an incorrect procedure.

Initial Screening

1. Screen the initiators based on their frequency. An initiating event having a frequency of 1.0E-7 or smaller is screened out. This is based on an argument that the maximum impact of an error of commission associated with response to the initiator is less then 1% of core damage frequency.

Identification of the Opportunities for Global Misdiagnosis

2. Develop a Procedure Response Matrix (PRM) for all initiating events, or initiator groups that produce significantly different plant responses. This is a table of the trends of the important plant parameters and/or indicators identified in the E-O procedure (e.g., Primary Pressure) for each of the initiator groups. For each of these groups, review the decision points in the procedural path. For each decision point that relates to entering a new procedure (e.g., entering E-1, E-2, E-3A, E-3B, etc.), identify the possible incorrect decisions resulting from either misinterpreting or failure of the plant to provide the correct information used at the decision step, or missing the decision step altogether.

Screening

Screening can be performed on the basis of consequences, on the basis of procedurally guided recovery to the appropriate procedure, or on the basis of likelihood. Step 3 collects the information necessary to screen on likelihood. Step 4 addresses screening on consequence, steps 5 through 7 address long-term recovery (i.e., as a result of procedurally guided re-diagnosis), and step 8 through 10 address screening on likelihood. In practice, steps 4 through 7 are carried out simultaneously, and as suggested by the ordering, in many cases will precede the screening on likelihood.

3. Identify the critical indicators and alarms corresponding to the entries in the PRM developed in step 2 above. For each alarm and indicator catalog the indicator/alarm locations(s), redundancy level, and whether these are diverse indicators or alarms (e.g., alternative methods of verifying the status of the critical parameter). Summarize this information in the form of a Plant Information Matrix (PIM), listing the critical parameters and the above information for each parameter.

Screening on Consequence

4. For each potential error, review the incorrectly chosen procedure and identify whether there exists the potential for failing, not performing, or otherwise making unavailable, any of those functions required to bring the plant to a safe stable state from the actual initiator (the appropriate functions can be identified from the event tree for that initiator). For those errors for which this cannot be excluded unequivocally, proceed to steps 5 through 7.

Screening on Recovery

5. For each global misdiagnosis opportunity review the procedure entered as a result of the misdiagnosis to identify re-diagnosis opportunities based on procedural directions. If there are such opportunities, the case can be screened from further analysis, unless the conditions in 6 and 7 below are met.

6. If the scenarios involve additional hardware failure over and above the initiating events, (e.g., failure of AFW), identify the impact on the operator's ability to make a re-diagnosis. This can be done by considering the impact of the hardware failure on plant response. Specify this in terms of changes in the values of the critical parameters in the PRM matrix that are used to make the re-diagnosis. If the recovery cannot be guaranteed, proceed to frequency screening.

7. Assess the potential for mindset leading to failure of the recovery action. This may, for example, be a function of training bias, or of a commonality of cues. For example, if the information used that resulted in the misdiagnosis in the first place, is not different from that that would be used to provide the opportunity for re-diagnosis, do not claim recovery. If the recovery cannot be guaranteed, proceed to screening on the basis of likelihood.

Screening on Likelihood

Three possibilities are postulated in which a symptom could be perceived to be different than it should be:

(a) instrumentation failure, or unavailability of an indication due to equipment failure, or loss of support system, (b) plant behavior may be modified by other equipment states (e.g., Steam Line Break inside containment may look like a

small LOCA), (c) the step in the procedure that completes the diagnosis may be missed, bypassed, or misinterpreted. For (a) follow step 8 below, for (b) follow step 9 below, and for (c) follow step 10 below.

8. Postulate the appropriate failure mode of instrumentation for the appropriate critical parameter for each case. Only postulate single failures of instrumentation; multiple instrumentation faults have a very low probability because of redundancy.

- Check the possible failure modes (high, low, as-is) to determine if the postulated misinformation is possible.
- For each possible failure mode, using the PIM, determine the possibility of the operators recognizing instrumentation failure, using information on redundancy of instrumentation, standard practices for checking alternate indications, procedural backup, etc.

Retain only those possibilities for which there is no obvious immediate backup to aid recovery from the incorrect information.

9. Identify potential equipment failures that can produce misleading indications by using the following:

- Identify the status of equipment as it should be in response to the initiating event, e.g., PORVs remain closed, Safety Injection(SI) pumps should not start, etc.
- Identify failures that result in violating these conditions and affect the key symptom(s) for decision-making in such a way as to lead to an incorrect decision.
- Identify other symptoms or indications that are triggered by the additional faults and that can lead to an opportunity to correct this misinterpretation.
- Retain those failures than can lead to misinterpretation, and allow no immediate potential for recovery, and which have a non-negligible probability of failure.

10. Assess the possibility of the operator not noticing, or misinterpreting the discriminating information available from the alarms and indicators. To do this list whether the following conditions exist for each initiator:

- Work overload (typically the number of alarms, and the number of parameters to be monitored for the initiator, on a relative basis).
- Perception of time urgency (based on training)
- Whether there is information supplied by an instrument that is known to be unreliable. This is a random hardware failure phenomenon, and the reliability of an instrument can be assessed as high or low for each of the important instruments. Persistent problems with instruments over a long period of time should be noted. This is a problem of desensitization to information.
- Whether there are any negative human factors considerations, e.g., lack of clarity of information, remoteness of recovery equipment, lighting, etc.
- Whether the procedural instruction is unambiguous and clear.
- Whether training has over- or under-emphasized the scenario.

A "High" rating on any of the first four factors or a high negative rating on the either of last two is translated into a "High Likelihood" of ignoring confirming information. Two or more "Moderate" ratings will also translate into "High Likelihood", and other combinations are screened out as "Low Likelihood".

For each alarm or indicator assessed as having a high likelihood of not being noticed by the operator, use the PIM to identify a recovery possibility, that is the potential for the operator to eventually notice the information or learn about the plant condition through other means listed in the PIM.

Assessment of Likelihood

If an error cannot be screened out, it will be required to assess its likelihood. This must be done judgementally. In the project on which this work was based, however, it was not considered necessary to proceed to this next step, hence this part of the procedure remained undeveloped.

PRELIMINARY CONCLUSIONS

The application of this approach to the Borssele nuclear power plant led to the conclusion that the types of adverse consequences that could be envisioned could be grouped into (a) degradation of decay heat removal by unnecessary isolation of a steam generator, (b) creation of a LOCA by inappropriate transfer to feed and bleed, or (c) non-performance of specific actions such as cooldown. However, it was judged that the likelihood of significant errors of commission of this global misdiagnosis type is very low. This is principally due to the forgiving and self-correcting nature of the procedures, the redundant and highly reliable instrumentation, and the good operational practices including use of backup instrumentation as checks on primary indications. The systematic process adopted in the analysis led to identification of one scenario with no clear potential for self-recovery. Mistakenly entering the procedure for a SGTR instead of that for a LOCA would not provide guidance to proceed to cooldown. However, the likelihood of this error is judged to be low, particularly in light of the fact that the transfer to the E-1 procedure (LOCA), occurs before that for the E-3A (SGTR) procedure.

Acknowledgements

This work was performed under a contract with N.V. Elekticiteits - Produktiemaatschappij Zuid - Nederland (EPZ) to study errors of commission for inclusion in the level 1 PSA for the Borssele plant. The authors are particularly grateful to Mario van der Borst for his encouragement and support.

REFERENCES

Parry, G.W., 1994, The need for and a proposed structure of, a second generation HRA methodology, in these proceedings.

Reason, J., 1990, "Human Error", Cambridge University Press.

HUMAN RELIABILITY ANALYSIS FOR SEISMIC EVENTS

Truong V. Vo and Tim M. Mitts
Pacific Northwest Laboratories
P.O. Box 999
Richland, WA 99352

Cindy M. van Bujjtenen and Elwyn Wingo
Westinghouse
Savannah River Company
Aiken, South Carolina

ABSTRACT

This paper presents the human reliability analysis (HRA) for selected post-accident human actions for potential seismic events at the Savannah River Site K-Reactor. This HRA was performed in support of Revision 1 to the probabilistic risk assessment (PRA) for the K-Reactor and provides human error probabilities for use in this PRA. This work was funded by the U.S. Department of Energy and was jointly managed and performed by the Westinghouse Savannah River Company and Pacific Northwest Laboratory.

INTRODUCTION

Under sponsorship from the U.S. Department of Energy, Pacific Northwest Laboratory (PNL)* collaborated with the Westinghouse Savannah River Company (WSRC) to perform a human reliability analysis (HRA) in support of revisions to the K-Reactor probabilistic risk assessment (PRA) for the Savannah River Site (SRS). The overall goal of this effort was to identify and apply a methodology for performing an HRA in the event of a seismic occurrence.

---

*Pacific Northwest Laboratory is operated by Battelle Memorial Institute for the U.S. Department of Energy.

Analysis of human responses to an earthquake raises numerous questions that push the limits of HRA methodology. Modeling human behavior in response to infrequent and extreme circumstances, such as seismic events, requires treatment of very limited quantities of data on human actions performed under high-stress conditions, and a great deal of uncertainty.

In this collaborative study, evaluating HRA methodology related to seismic events included the following activities:

1. Identifying and applying an HRA methodology that is consistent with that used in other recently published PRAs (e.g., NUREG-1150) that have received broad acceptance.

2. Performing and documenting supporting task analyses and data evaluations that provide the bases for obtaining realistic human error probability (HEP) and uncertainty values.

3. Providing HEP values as input to the revised K-Reactor PRA for SRS.

4. Identifying areas that may reduce HEP values and have potential contribution to risk associated with seismic events.

This paper presents results of the human reliability analysis. Details of the evaluation are to be published as a PNL document at a later date.

REVIEW AND SELECT HRA METHODOLOGY

State-of-the-art HRA methodologies were reviewed for the purpose of selecting the methodology best suited for estimating HEPs associated with seismic events (Mitts and Vo 1992). Based on this review, the THERP or ASEP methodologies were the recommended approaches for use in evaluating the HRA to support revisions of the SRS PRA. Test applications of the THERP and ASEP methodologies were also performed in support of this HRA effort (study by van Bujjtenen et al. 1993, to be published). Based on results of test applications, the ASEP methodology was chosen for this study. Use of the ASEP methodology provides the same benefits as using THERP methodology, but requires significantly fewer staff resources to perform.

The following key activities were performed while using the ASEP methodology as the basic approach.

Construct HRA-Event Trees. The HRA-event trees were constructed for selected portions of the SRS seismic event Master Control Procedure DPSOL 105 MC-28-K or MC-28.* Procedure MC-28 is the main procedure used by the central control room

*Internal procedures for the Savannah River Site K-Reactor: DPSOL 105-MC-28-K, MC-28B-K, MC28C-K, MC-28D-K.

(CCR) and others when responding to a seismic event. This activity included a detailed review of the appropriate operating procedures and development of task analyses.

Evaluate Performance-Shaping Factors. This activity involved: 1) evaluation of performance-shaping factors (PSFs) and uncertainty bounds for human actions modeled in the HRA-event trees, and 2) the disposition of judgment issues in assessing HEP values. A seismic intensity level of 0.35G was selected as a threshold value for the analysis. This value was selected based on existing WSRC studies and on recommendations from expe-ri-enced WSRC staff.

Quantify Human Error Probabilities. Completion of the above steps led to quantifying HRA-event trees to obtain the overall HEP values for the human actions evaluated in this study. This effort also included identifying potential improvements, such as potential changes to procedure MC-28, that may reduce HEP values.

ANALYSIS

This section describes the analysis of HRA application for seismic events. Specific details of the analyses can be found in Benhardt et al. (1993, to be published). The analysis includes the following tasks: 1) data collection and evaluation, and 2) application of the methodology.

Data Collection And Evaluation

This task included preparation for data collection and evaluation, desktop procedure review, plant walkdown, and simulator review.

Preparation for Data Collection. One of the first steps in the HRA process was the development of a systematic method for collecting and consolidating information used in the analysis. Second, a task analysis format (or form) was developed that incorporated the information required to support the data collection task. The task analysis approach to HRA development included the following steps:

- identification of a consistent method to identify specific actions throughout the process
- identification of the individual(s) taking the action, and equipment used by the individual when carrying out the action
- description of the action to be taken by the individual
- feedback so the individual knows that the action taken has been completed or is successful
- identification of the exact location where the action takes place, and the time required to perform the action

- assessment of errors that an individual might make in performing the action
- identification of information that may influence the way the individual performs the action.

Desktop Procedure Review. The task analysis began by developing a task list based on the MC-28 procedures (MC-28B, MC-28C, and MC-28D). The individual steps of each procedure were considered as tasks that needed to be performed by an operator. Each of these steps was analyzed to determine if the step actually consisted of multiple tasks or task activities. Based on this analysis, appropriate additions were made to the task list.

Plant Walkdown. The walkdown was a planned and coordinated activity that involved the HRA analysts, personnel familiar with plant operations, and personnel familiar with the design of the systems. Two plant walkdowns were conducted during the course of this study. The walkdowns involved general orientation of the K-Reactor and its systems, as well as visits to the areas where activities described in the MC-28 procedures were performed. Video cassette recordings of plant operators performing the actions of the MC-28 procedures were also reviewed.

Simulator Review. The simulator offered the analyst an opportunity to view details of the procedures that can not normally be observed in the control room. In addition to studying details of control room actions, the simulator staff and training records provided valuable data on operator training and experience levels. A walkdown was conducted in the reactor control room simulator to perform a step-through review of the MC-28 procedures. This walkdown provided data for the task analysis that was used to conduct the ASEP analysis. In addition, other plant relevant, information and site-specific documentation were reviewed.

APPLICATION OF METHODOLOGY

Human actions that impact plant safety, in the event of a seismic occurrence, were selected for HRA evaluation. The following specific actions, as identified in the SRS K-Reactor PRA were selected for the analysis:

- Start of recirculation pumps per MC-28 (Step 14 and MC-28C).
- Trip supplementary safety system (SSS) per MC-27 (step 2) and MC-28 (steps 2 and 3).
- Start of recirculation pump diesel generators (DGs) per MC-28C (steps N8.1 through N8.8).
- Set automatic transfer switch (ATS) for the recirculation pump DGs per MC-28C (Step 13a).

- Operate moderator recovery system (MRS) per MC-28 (step 23 and MC-28D).

- Close heat exchanger isolation valves per MC-28 (steps N30 and N31).

The ASEP approach was used to perform the HRA for these specific operator actions using the task analysis associated with the following procedures: MC-28, MC-28B, MC-28C, and MC-28D. ASEP HRA-tables and HRA-event trees were constructed to model critical human actions for responding to seismic events. Evaluation of individual actions in the task list was performed to assign an HEP values and associated error factors from the tables provided in NUREG/CR-4772. Once the HEP values were assigned, the ASEP tables, and tree models, as well as items in the task list, were reevaluated to include dependencies and PSFs.

The PSFs applied to the tasks included considerations of seismic intensity, location of the action, and availability of personnel to perform the action. Other PSFs were inherent in the conservative values in the ASEP tables. Considerations were evaluated on the basis of the simplified task analysis and with knowledge of human action steps from the governing procedures. Provision to perform a more detailed and thorough HRA for a given human action or subtask exists within the ASEP methodology by applying the THERP methodology. However, additional data and information must be obtained before applying the THERP methodology.

Once HEPs were assigned and modified to reflect the performance environment and the effects of dependence, the individual error probabilities and uncertainty bounds were propagated through the HRA-event trees to determine the final probabilities and uncertainty bounds. Generally, error factors obtained from the ASEP HEP tables (NUREG 4772) were used for the actions considered.

RESULTS AND DISCUSSION

Table 1 summarizes results applicable to the SRS K-Reactor PRA for seismic events. Results show that "Moderator Recovery System (MRS) Activation" has the highest HEP values at seismic intensity levels both less than and greater than 0.35G. These actions are performed under extremely high stress and involve several dynamic tasks with dependence between some actions. In addition, this task requires radio communication and coordinated efforts among personnel in various locations. At seismic intensity levels greater than 0.35G, access to the seismic MRS control stations could be impeded because of equipment damage, jammed doors, etc. This contributes to the highest estimated HEP values.

High HEP values were also found for the action of "Throttling Heat Exchanger Valves." The high values were attributed to the extremely high-stress conditions under which staff operated. The actions are dynamic and require radio communication and coordinated efforts among personnel in various locations. Actions involve manually closing ten 24-inch gate valves to throttle the heat exchanger flow and maintaining the ultimate

Table 1. HRA Results for Selected Human Actions for PRA

Procedure Action	Total HEP[1] @ <0.35G	Total HEP[1] @ >0.35G
MC-28D MRS Activation	3.0E-1	8.8E-1
MC-28 Throttle Heat Exchanger Valves	1.2E-1	6.6E-1
MC-28C Start Recirculation Pumps	6.3E-2	5.0E-1
MC-28C Set ATS for Recirculation Pump Diesel Generators	3.0E-3	1.9E-1
MC-28C Start Recirculation Pump Diesel Generators	1.0E-3	5.0E-2
MC-28 SSS Activation	2.5E-4	2.5E-4

[1] These results present "best estimate" HEP values. Generally, an error factor of 5 is used to address uncertainties for the HEP values.

heat sink (within 4.5 hours). Because of potentially damaged structures and systems, access and personnel availability to perform these actions may be restricted at seismic intensity levels above 0.35G.

The human action with the next highest HEP value was "Start Recirculation Pumps." The high HEP value for this action is driven by the dynamic nature of the situation in the CCR where MC-28C must be assigned and initiated. The HEP value is higher at seismic event intensities greater than 0.35G because the likelihood of visible structural damage and potential failed systems will cause stress levels to be extremely high. The HEP values for "Starting the Recirculation Diesel Generators" and "Setting the Automatic Transfer Switch" are considerably lower because the possibility of failing to initiate MC-28C is already accounted for in the HEP value for "Starting the Recirculation Pump."

The last human action, "Supplementary Safety System Activation," is a simple task that can be completed from the CCR; therefore, the HEP value for MC-28 is relatively low. This HEP value does not change for a seismic intensity level greater than 0.35G because the action is performed within the control room by personnel dedicated to these positions and functions.

The results, as presented in Table 1, are based on "best estimates" with uncertainty estimates based on error factors of 5, except for diagnosis actions, which have an error factor of 10. Analyses were based on assumptions made using plant-specific information and on WSRC staff experience. Thus, these results are plant specific and should be interpreted cautiously.

ACKNOWLEDGMENTS

The authors wish to acknowledge the direction and support provided by Dr. K. Jamali, DOE Project Manager, and Carl E. Beyer, PNL Project Manager. Acknowledgments are also addressed to H. Benhardt, A. Beyrer, K. O'Kula, and S. Topp,

Westinghouse Savannah River Company, B. F. Gore, PNL, and W. Wheeler, Human Affairs Research Center, for their contributions and/or guidance to this work.

REFERENCES

NUREG/CR-4772. 1987. U.S. Nuclear Regulatory Commission, "Accident Sequence Evaluation Program Human Reliability Analysis Procedure." Washington, D.C.

NUREG-1150. 1989. U.S. Nuclear Regulatory Commission, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants." Washington, D.C.

Mitts, T. M., T. V. Vo, W. J. Wheeler, and A. Bittner. 1992. "Selecting the Seismic HRA approach for Savannah River Plant PRA." PNL-8429. Pacific Northwest Laboratory, Richland, Washington.

EVIDENCE OF THE NEED TO MODEL ERRORS OF COMMISSION IN RISK ASSESSMENTS FOR VARIED ENVIRONMENTS

David I. Gertman, Lon N. Haney and Lee T. Ostrom

Human Factors and Systems Analysis Unit
Idaho National Engineering Laboratory
Idaho Falls, Idaho 83415

ABSTRACT

This paper discusses overwhelming evidence that errors of commission are important, occur in a variety of environments, and need to be modeled in risk assessment. Three specialized applications of human reliability analysis are presented where the modeling errors of commission is successfully exploited. Two involve event reconstructions where errors of commission occurred. The third, is a traditional HRA for a generic class of events where the potential for errors of commission is real. A specialized event tree, the cognitive event tree, is presented as a means of representing errors of commission. Findings are discussed in terms of the types of errors of commission identified, the extent to which cognitive event trees aided in the analysis, and what influences (performance shaping factors) were determined to be present surrounding errors of commission.

INTRODUCTION

Commission errors are referred to as either slips, mistakes, or willful violations (see for example, Reason[1]). Most contemporary HRA methods make allowances for quantification of these errors.[2-4] Dynamic evaluation methods (simulation) make provision for them as well.[5] The more interesting commissions are errors in judgment as opposed to simple errors in action execution. Methods for performing integrated probabilistic risk assessment (PRA) such as the sequence proposed in the systematic human action response procedure (SHARP)[6] also make allowance for the representation of errors of commission.

Despite the potential for their representation in PRA, there is general consensus that cognitive errors of commission (other than simple errors in execution, i.e., slips) are underrepresented in PRA/HRAs.

Although this picture is changing, there is need to accelerate the process. Better error models, methods of error detection and means by which to characterize these errors are needed. Reluctance on the part of risk practitioners to model cognitive errors of commission exists because they are overwhelmed by the myriad possibilities for such errors. A model for determining a reasonable subset of these errors based upon how crews communicate, use information resources, and pursue success paths is called for.

This model must be tied to context, i.e., evidence that even small events in non-linear systems seem to be linked (the Perrow[7] approach) or that disasters require latent errors combined with active human error and hardware failure (the Reason[4] approach). On a basic level, studies should also indicate what performance shaping factors (PSFs) influence crew performance.

Error Representation

The HRA event tree framework proposed in Ref. 2 affords, once combined with the Reason taxonomy, a convenient, if not traditional, framework for presenting these errors and supporting PRA event sequence analysis. The rationale for this combined framework, the cognitive event tree (CET), is presented in Ref. 6. The CET approach is used in this paper to determine the range of commissions in real and postulated events.

BACKGROUND

This paper focuses on CET representation of commissions and evaluates: whether there is sufficient evidence that these error types are present in a variety of settings, whether this method is sufficiently robust to represent inter-task and inter-person dependencies and most errors of commission, and whether errors of commission (other than simple slips) need to be represented in risk analysis for human-machine systems. Lastly, it reviews the PSFs that were associated with each event (and the commissions). Three case studies are examined below.

The first analysis (HRA), presents a event sequence reconstruction involving a tanker grounding and subsequent oil spill in the Texas gulf. No loss of life occurred, but considerable environmental damage was present. The second example identifies errors leading to wrong site brachytherapy administration during a cervical cancer treatment incident reported in Puerto Rico. The third HRA reveals errors of commission implicated in altitude deviations, where crews inadvertently deselect the altitude capture navigation system. This latter analysis and evaluation is part of a risk sequence scrutinized for NASA.[8] In each case mentioned above, a CET[6] is used to represent personnel's likely cognitive realm (skill, rule or knowledge) and error mechanisms (slips, lapses, mistakes, and willful violations) involved in each of the errors of commission. It is intended by the review of these sequences to demonstrate that errors of judgment (mistakes and willful violations) play an important role in accident propagation and that their omission severely constrains the generalizability of contemporary risk analysis findings. The contribution of causal factors leading to these errors of commission is discussed in a separate paper.

Case Study Descriptions

Case Study 1. The grounding of the Chandy D in Galveston Harbor was an event with considerable human factors involvement that transpired in 1991 and is described in Ref. 9. On that day, a river pilot on a vessel named the Shinoussa was guilty of a number of "active errors" that included excessive speed (mistake); procedural violations: passing too close to another vessel, failure to notify the coast guard of his position and speed, and failure to request information on other vessel locations and speeds. As a result of this sequence of errors, an oil barge was struck and sunk in the harbor. Latent errors were involved as well. The harbor was being used for tonnage for which it was not designed, and the crew were not aware of the effects of river bottom characteristics upon vessel passings. There may have been some difficulty with coast guard fixed radar positions on that day. After interviews, it was noted that the river pilot's decision not to notify

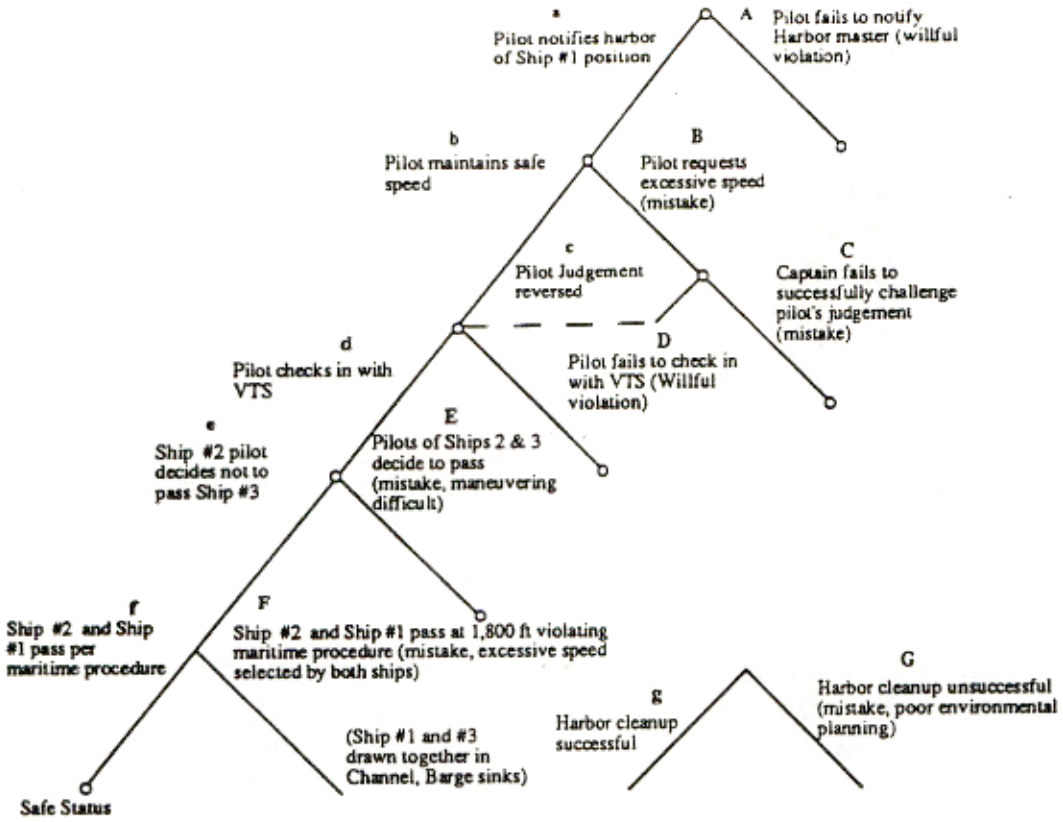


Figure 1. HRA sequence for barge grounding incident.

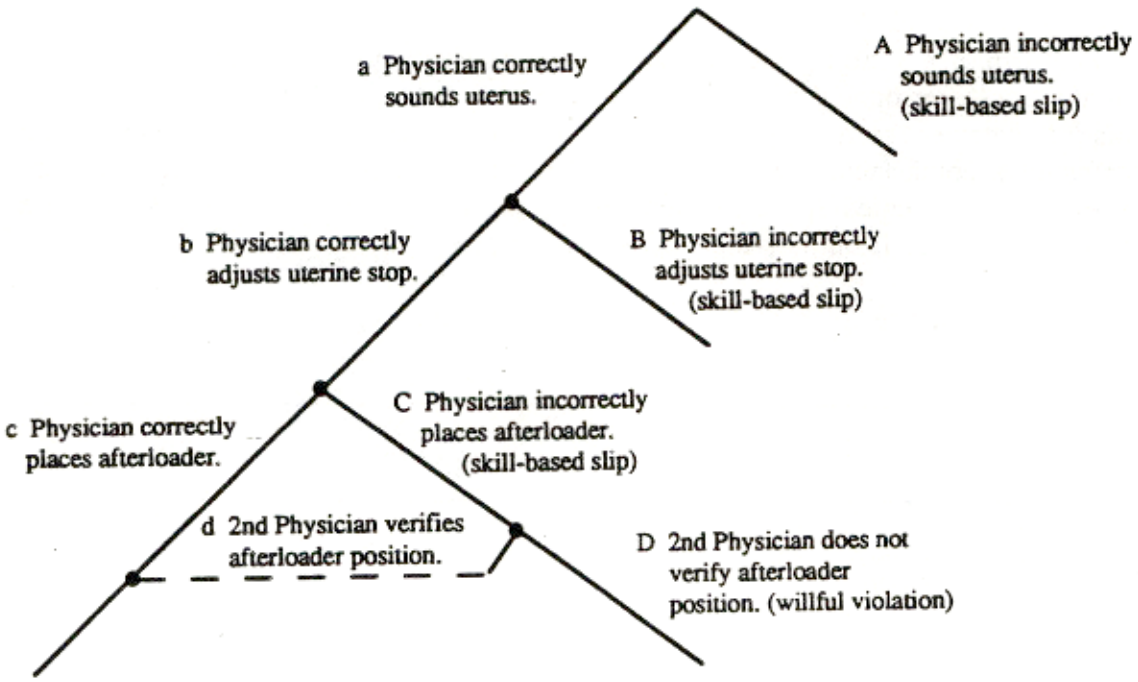


Figure 2. HRA sequence for afterloading applicator placement by physician.

the coast guard of his position was not simply a lapse on his part but indicative of a decision (procedural violation). The Figure 1 CET presents both the successful path that could have been taken and the type of errors that occurred. Because this was an event reconstruction, the multiple errors of commission listed on the right hand side of the tree actually occurred. The most significant error was the failure to reduce speed after viewing and going around the Chandy D. Because of the bottom characteristics, the Chandy D was dragged into a position that made it difficult for that vessel's pilot to return to a parallel heading.

Case Study 2. Figure 2 presents an HRA for a brachytherapy afterloading misplacement that occurred in Puerto Rico in 1992. Three skill-based errors that could be characterized as slips are presented. Upon further analysis, it was determined that the physician's error was due to his violating a procedural step requiring a second physician to verify the radioactive source placement. Thus, what at first seemed to be an skill-based error was really a conditional error, that is the physician had first to commit the skill-based error and then (willfully) violate the verification procedure. Contributing factors seemed to be lack of physician training and overconfidence.

Case Study 3. The HRA for commercial airliner altitude deviation is presented in Figure 3. This scenario can occur because of the nature of the interface, and because of lack of crew awareness that mode changes taken by the crew can disable the altitude capture device (coupled to the flight management system). Although a number of errors are presented in the CET, the actual disabling of the device and subsequent altitude deviation that occurs is due to two primary means: the slip where the altitude capture is "bumped" and drop in altitude occurs, and the mode change that decouples the altitude capture. Simulator studies indicated that pilots were unaware that certain mode changes were capable of decoupling the device. Other deviations could occur from the pilot's overshooting the correct altitude or failure to set the device. Quantification of the sequence indicated that the dominant human error was the commission associated with misunderstanding implications of mode change.

Performance Shaping Factors Information is usually used in order to characterize important task-, personnel- or environment -centered characteristics surrounding error. This is true whether errors of omission or commission are executed. Table 1 presents the performance shaping factors associated with the errors of commission for the three case study examples presented above. Rather than being a predefined list, these PSFs were determined post hoc, from individual events analysis.

Table 1. Performance Shaping Factors Associated With Cognitive Error Analysis for Three Case Studies

PSF	Case Study 1 Chandy D	Case Study 2 Misadministration	Case Study 3 Altitude Deviation
Procedures use	+	+	
Interface design		+	+
Systems knowledge	+	+	+
Teamwork	+		
Training		+	+
Workload			+
Overconfidence	+	+	+

+ indicates that a particular PSF was involved either directly or indirectly in the errors of commission reported in the case studies

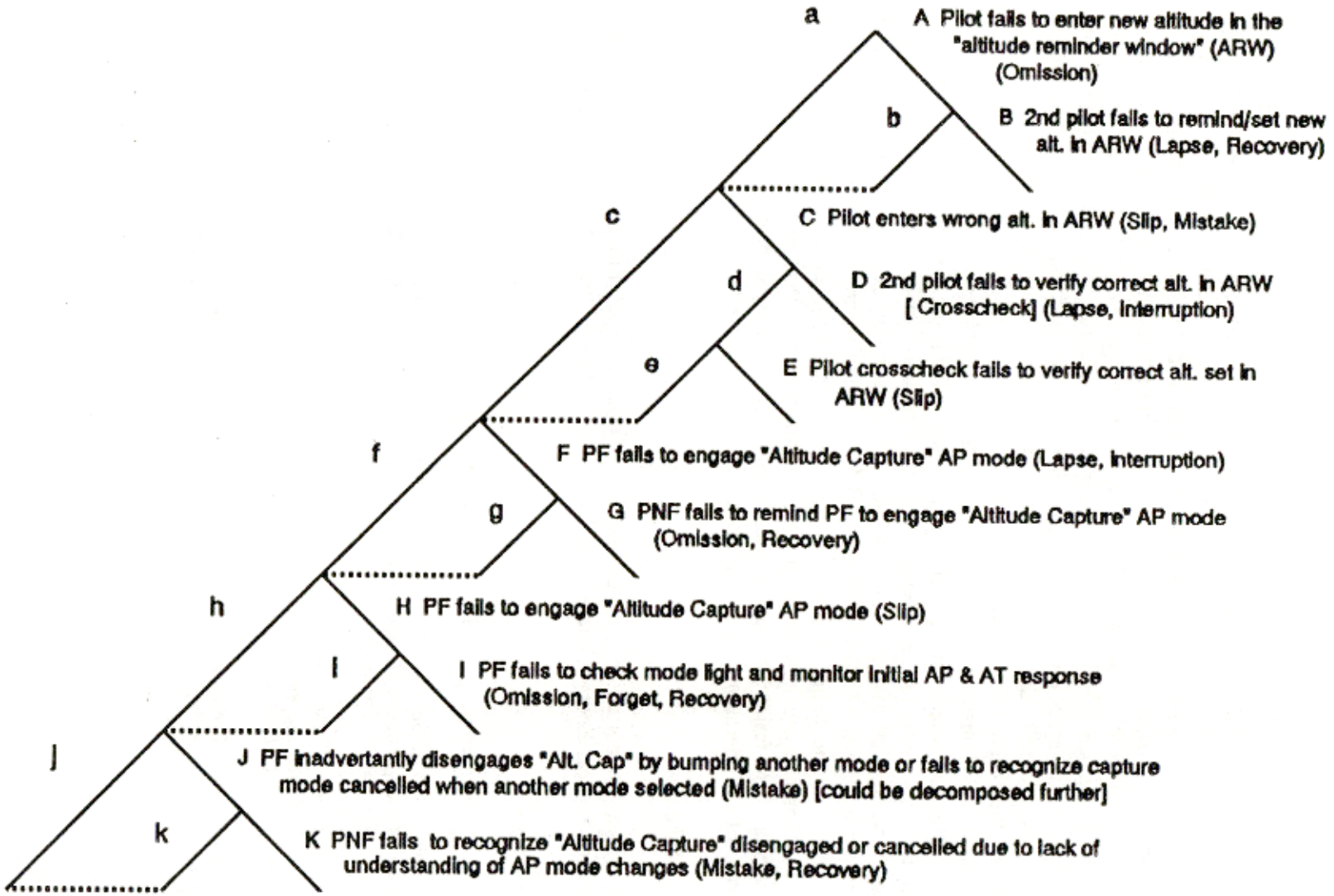


Figure 3. HRA sequence for crew programs and engages auto pilot for altitude change and capture.

SUMMARY AND DISCUSSION

This study supports the notion that a wider range of operator behavior should be included in HRA/PRA. Two event reconstructions and one traditional HRA for a generic category of events (altitude deviation for commercial aircraft) were found to have evidence of errors of commission that involved mistakes and willful violations. CETs were determined a useful means for modeling these commissions (parallel recovery paths are easily shown). Two of the events also involved combinations of hardware and human failure. In Case study 1, hardware failures were evidenced by failure of the Coast Guard Radar (an active failure) and in Case study 2, failure of a minor alarm on the cancer treatment apparatus (an active hardware failure). The third Case study involves a latent error (design error for the altitude capture device interface that allows for easy, inadvertent deactivation) coupled with mistakes and misunderstandings regarding the impact of mode change on current equipment configurations. Additionally, the crew is not prompted that the altitude capture device was disabled (another latent design error).

Case study reconstruction (human error analysis) is different than wholesale modeling of classes of events where one models multiple possibilities and assigns them probabilities. In either case, the need for representing errors of commission is compelling. PSFs were important factors in all of these case studies. The distribution of these PSFs suggests that PSFs are context sensitive elements that need to be identified and evaluated on a scenario-specific basis. In the future, researchers need to determine the extent to which postulated PSFs are orthogonal and how they are best combined. Until that time, PSF lists will be generated a la SLIM fashion through consensus of experts as to what influences are prominent and worthy of consideration. In the absence of something better, this will suffice.

Acknowledgements

This work was supported in part by the U.S. Department of Energy (DOE), Assistant Secretary for Nuclear Energy, under DOE Idaho Field Office Contract DE-AC07-76ID01570.

REFERENCES

1. J. Reason, "Human Error," Cambridge University Press, United Kingdom, (1990).

2. A.D. Swain and H.E. Guttmann "Handbook for Human Reliability Analysis with Emphasis on Nuclear Power Plant Operations: Technique for Human Error Rate Prediction," NUREG/CR 1278, U.S. Nuclear Regulatory Commission, Washington D.C. (1983).

3. D. Embrey et. al., "SLIM-MAUD, An Approach to Assessing Human Error Probabilities Using Structured Expert Judgement," Vol. I, NUREG/CR-3518, U.S. Nuclear Regulatory Commission, Washington D.C. (1987).

4. Moeini, et. al., "The Use of Simulator Data in Human Reliability Analysis: Results form the EPRI Operator Reliability Experiments Program," PSAM II Proceedings, G. A. Apostolakis , ed., Beverly Hills (1991).

5. C. Acosta and N.O. Siu, "Dynamic event trees in accident sequence analysis," *Reliability Engineering and System Safety*, 41, in press (1994).

6. D.I. Gertman, "Representing cognitive activities and errors in HRA trees," *Reliability Engineering and System Safety*, 39, (1993).

7. C. Perrow, "Normal Accidents," Basic Books, New York (1984).

8. W.R. Nelson, et. al., "Lessons Learned from Pilot Errors Using Automated Systems in Advanced Technology Aircraft," IEEE Topical Meeting, Oak Ridge (1993).

9. NTSB/MAR-91/03, Marine Accident Report, Galveston Bay, Texas , NTSB, Washington, DC (1990).

APPLICATION OF HRA IN THE COMMONWEALTH EDISON INDIVIDUAL PLANT EXAMINATIONS

LARRY SOTH, Commonwealth Edison Company

ABSTRACT

The Commonwealth Edison IPEs reflect realistic treatment of operator actions by integration of the emergency procedures into the accident sequences. An extensive HRA based on THERP data was used to quantify the proceduralized operator actions. Some features of the HRA are discussed which highlight the effect of changes in nuclear plant procedures and ergonomics over the past decade.

The detailed HRA produced a comprehensive review of plant emergency procedures and generated several suggested procedure enhancements. Incorporation of selected procedure changes provided a measureable reduction in plant risk.

INTRODUCTION

The Individual Plant Examinations (IPEs) developed by Commonwealth Edison (Edison) in response to Generic Letter 88-20[1] employ best-estimate analyses and realistic treatment of operator action. The intent was to reduce the conservatisms found in traditional PRAs by incorporating several innovative features:

- The Level I event trees and Level II containment event trees were combined into single Plant Response Trees (PRTs) to better evaluate the total plant response to severe accident sequences.
- Realistic success criteria for systems and operator actions were developed based on hundreds of transient computer runs.
- Operator actions prescribed in the Emergency and Abnormal Operating Procedures (EOPs & AOPs) were fully integrated into the PRT sequences.

The node sequence in the Zion Small LOCA PRT illustrates the size of the PRTs and the integration of the operator actions (node designators beginning with **O**).

SLOC1	TK	CCP	SIP	AFW	ORF	CB	MFW	ORS	DS

ODS	LPI	ODP	DP	FC	CSI	OHX	RHX	ONC

NC	ONR	NRC	ORC	LPR	HPR	ORT	RTK	CI

The PRT analysis identified the necessary operator actions (OAs) during the development of the trees represented in the IPE model. These OAs were then analyzed and quantified by HRA. The process was an iterative one to ensure the assumptions made in the PRT analysis and in the HRA were consistent.

THE HRA

The HRA was performed in two phases. In Phase I a detailed Subtask Analysis was used to break down each OA identified in the PRT analyses, including success criteria and time windows, into the specific operator steps which were absolutely necessary for the OA node to be successful. For this analysis, a detailed knowledge of plant systems, operations and procedures was more important than PRA or HRA expertise in identifying and correctly modeling the essential operator tasks. As outlined in G.L. 88-20, only those OAs explicitly proceduralized were modeled.

Quantification was performed using published nominal HEPs from THERP Chapter 20[2] and modifying the HEPs with PSFs. Each modeled step was analyzed based on the requirement of independent, conditional, or joint activities and mathematical expressions were developed for calculations. The resulting HEPs for each step were then added to obtain an overall HEP value for a particular OA node.

In Phase II the assumptions made during Phase I were validated by discussing OAs with experienced operations and training personnel and by observing selected OAs on the plant simulator. For the most part, the Phase II results upheld the general assumptions made in Phase I. However, several differences in operator cues and corrections to procedural step modeling for some of the OAs were identified. Additionally, the emphasis placed on certain parameters or scenarios was conveyed.

The THERP method recommends a screening process to reduce the amount of analysis necessary. This approach was not used in the Edison IPEs since a realistic model of all operator actions was desired. Additionally, different cases were evaluated for several OAs to account for differences in stress, dependency, and recovery factors on a sequence-by-sequence basis. Therefore, the HRA was extensive and represented many man-months of effort.

In the Zion HRA, 29 operator action nodes were quantified for 47 cases. The subtask analyses ranged from 3 to 24 tasks. In the Dresden HRA, 20 OA nodes were quantified for 60 cases. Very few basic HEPs and data elements from THERP Chapter 20 were needed: Zion's HRA only used 17, Dresden's 25.

THERP was chosen for the HRA since it is a relatively straightforward, accepted method for predicting HEPs. But there have been many changes and improvements at nuclear power plants in the 10 years since NUREG/CR-1278 was published:

- Plants now use improved symptom-based Emergency Operating Procedures developed from guidelines provided by the respective Owners Groups.
- The man-machine interface has been improved by applying Human Factors principles to the Control Room design.
- Training has improved and is conducted using plant-specific simulators.
- The Shift Technical Advisor (STA) has been added to the operating crew.

At Edison plants the STA is a licensed SRO named the Station Control Room Engineer or SCRE, and

- The emergency preparedness organization has been expanded to include the Technical Support Center (TSC), Operational Support Center (OSC) and off-site Emergency Operating Facility (EOF) staffs.

These changes allow adjustment of the basic HEPs from THERP. Additionally, differences in such factors as procedure philosophy, and level of detail and use, required differences in HRA modeling between PWRs and BWRs.

Procedures

The PWR EOPs are extremely detailed step-by-step procedures. In contrast, the BWR EOPs are in a flow-chart format, and provide general guidance to follow based on plant symptoms. Systems to be used to fulfill a desired function are specified, but step-by-step proceduralized actions are not included. Therefore, lineup of systems directed by the BWR EOPs is accomplished from memory by the operators, without initial reliance on procedures. [It must be emphasized that these activities are well within the skill of the operators and are the ones on which they receive the most training.]

Since the PWR procedures are detailed, THERP Table 20-7 (Errors of Omission Per Item of Instruction When Use of Written Procedures Is Specified) was used in assigning HEPs for errors of omission. In the BWR case, since the operators rely on memory to perform the detailed actions, Table 20-8 (Estimated Probabilities of Errors in Recalling Oral Instruction Items Not Written Down) was used. The resulting HEPs are higher than those obtained through the use of Table 20-7.

In addition to having very detailed procedures, at the PWR plants the EOPs and related procedures are read to the Control Board Operators. This is a formal, practiced, reader-worker routine. For this reason, the commission error HEP values from THERP were reduced by a factor of 10 in the PWR IPEs. Since the BWR procedures do not specify detailed lineups and the actions are performed from memory, the factor of 10 reduction was not applied.

Recovery Modeling

Both the PWR and BWR HRAs utilized recovery models, with differences.

For the PWRs no recovery credit was given for OAs which require action within 5 minutes. A HEP reduction was not considered justifiable because with such a short time, all operator actions are time dependent and the availabilty of an operator for checking another's activities is almost nonexistent.

After 5 minutes into an event, the SCRE is available in the Control Room to help recover errors. The PWR EOPs provide numerous redundant steps and verifications, including Critical Safety Function Status Trees, all of which support recovery. Additionally, the Control Room crew is trained as, and functions as, a team to perform the actions necessary to mitigate a transient. Therefore, if greater than 5 minutes were available for the operators to perform the action, a general recovery factor of 0.1 was applied.

The BWR recovery model was somewhat different due to the differences noted above. Because of these differences, only specific, identifiable recoveries were credited during the first hour. Some of the recovery opportunities include:

- a procedure step directing the operator to verify that the system is performing its intended function,
- a second alarm at another location in the control room that a different crew member may acknowledge, and
- an alarm that would indicate that the action had not been performed correctly.

For actions that take place greater than one hour after an initiating event, a slack time recovery factor was applied to both PWRs and BWRs. This recovery is based on review of the event progression by personnel who had not been intimately involved up to that point. Recoveries of this type include manning of the TSC, arrival of off-duty personnel to assist in accident mitigation and recovery, or arrival of a relieving crew. A recovery factor of .21 was applied to account for this extra assistance. This was derived from THERP Table 20-22 (Estimated Probabilities That a Checker Will Fail to Detect Errors by Others) Item (3): Special Short-Term, 1-of-a-kind Checking with Alerting Factors, which has a mean HEP of .081. A moderate dependence (Table 20-17) was assumed to provide the resulting 0.21 factor.

Stress

The stress factors used were taken from THERP Table 20-16 (Modification of Estimated HEPs for the Effects of Stress and Experience) and were taken to be either optimal (PSF = 1), moderate (x 2), or high (x 5). In most cases, a higher stress multiplier was adopted in general to compensate for uncertainty of stress assumptions, less-than-perfect training as well as the failure of plant instrumentation to present useable information. During the Zion operator discussions it was noted that there were no significant stress differences which affect the HRA quantification for LOCA events of different sizes (large or small). The reason for this is that with the symptom-based EOPs the operators respond to event symptom(s) rather than making knowledge-based diagnosis.

IPE RESULTS AND HRA SENSITIVITY

The bottom line results of the Zion and Dresden IPEs were that there were no severe accident concerns requiring remedial actions within the context of the NRC's safety goals. For Zion, the Total CDF over all (15) initiators was 4.0E-6/yr. For Dresden, the result was 1.86E-5/yr (10 initiators).

Since the EOPs were mapped to the accident sequences, it was to be expected that OA node failures would be represented in the dominant sequences. For Zion 70% of the CDF is attributable to sequences containing one or more failed OA nodes. For Dresden the contribution was 33%. The Zion top 100 accident sequences included only 9 different OA node failures (out of 29 analyzed) in 14 sequence specific cases, three of which were defined failures (HEP = 1.0).

To examine the sensitivity of the IPE models to the HRA, OA nodes which were significant contributors to the total CDF were varied by an order of magnitude and the model requantified.

In the Zion study, three OAs were significant contributors to CDF:

ORT: Refill the RWST
ORC: Establish ECC Recirculation
ODS: Depressurize the Steam Generators

For the Dresden IPE the significant OAs were:

OSPC: Establish Suppression Pool Cooling
OAD: Depressurize the Reactor Vessel
OMUP: Supply Makeup to the Isolation Condenser

The results of the sensitivity analysis may be summarized as follows:

	PRT NODE	CONTRIBUTION TO TOTAL CDF	% CHANGE IN TOTAL CDF NODE X 10	NODE X .10
Zion:	ORT	34%	+ 250%	- 15%
	ORC	20%	+ 275%	- 17.5%
	ODS	17%	+ 250%	- 15%
Dresden:	OSPC	15%	+ 135%	- 14%
	OAD	12%	+ 68%	- 8%
	OMUP	7.5%	+ 111%	- 8%

Thus, for both plants, increasing the HEP by a factor of ten does result in some ial change in the CDF. Although the change appears significant at first look, it is important to note that the CDFs associated with the sensitivity cases are still low in an absolute sense. Nevertheless, this does highlight the importance of maintaining the quality of the procedures and the effectiveness of operator training.

Decreasing the HEPs by an order of magnitude did not result in any significant decrease in plant risk. The conclusion here is that improvements in procedures or training associated with the dominant OA nodes (without accompanying improvements in hardware) would provide only a small improvement in plant risk.

INSIGHTS AND REQUANTIFICATION

One of the NRC's objectives for the IPEs was to identify potential enhancements which could reduce risk, based on reviewing the dominant sequences. At Edison, the search for insights was conducted during each stage of the IPE, rather than at the end - looking backwards from the IPE results. This process has several benefits, primarily the ability to discover many more insights (over 300 at Zion) by searching at the same time system performance, system interaction, operator actions, and accident progression are under study.

The HRA resulted in a comprehensive review of the plant EOPs and, as expected, a significant number of procedural insights were developed, primarily to improve clarity and increase the chances for appropriate operator response to plant parameters. For Zion, about 25% of the insights dealt with procedure enhancements; for Dresden about 40%.

Evaluation of the Zion IPE showed that failure to successfully refill the Refueling Water Storage Tank (RWST) in a timely manner for sequences with loss of ECCS recirculation capability contributed substantially to the overall CDF. Several insights had been identified to improve the chances of successful RWST refill. These included:

- more timely diagnosis of the need for RWST refill,
- more timely reduction in RWST water usage during an event,
- explicit approval for the use of unborated water makeup sources, and
- more detailed instruction on the necessary system alignments.

These procedure change recommendations result in two changes to the IPE model:

- requantification of the HRA for node ORT, and
- requantification of the fault tree for node RTK (Equipment to Refill the RWST).

These changes were made and the Zion IPE model requantified with the revised ORT and RTK included.

The results were a five fold decrease in total CDF from 4.00E- 06/yr to 7.1E-07/yr. Also, the Uncontrolled Release Frequency dropped from 1.46E-06/yr to 2.78E-07/yr, showing that the loss of containment function was also favorably impacted by the changes to the RWST refill procedure.

In the Dresden IPE, a similar application of insights relating to the operator action (OSPC) and equipment (SPC) for Suppression Pool Cooling produced a reduction in total CDF from 1.85E-05/yr to 3.75E-6/yr.

CONCLUDING DISCUSSION

The results of an HRA are valid only if they are borne-out by real world events. For an HRA performed as part of a PRA, this form of confirmation is to say the least, undesirable. However, the results of an HRA are valuable because they provide a reference point for understanding operator performance during the improbable events that would occur during a postulated plant accident.

The detailed HRAs performed for the Edison IPEs were extensive, time consuming, and labor intensive. The resulting HEPs are generally lower than those found in previous PRAs due to the additional detail. The many procedural insights developed during the HRA also make the effort justifiable. A number of such insights with generic applicability have been forwarded to the respective Owners Groups for consideration as improvements to their Emergency Response Guidelines.

The recommended RWST refill procedure changes, as well as several other procedure changes suggested by the insight process, have already been implemented at Zion. Similarly, the recommended procedure changes at Dresden are also under way. With these changes, both stations meet the NUMARC Severe Accident Closure Guidelines [3].

---

1. NRC Letter to All Licenses Holding Operating Licenses and Construction Permits for Nuclear Power Reactor Facilities, "Individual Plant Examination for Severe Accident Vulnerabilities, -10CFR-50.54(f)," Generic Letter No. 88-20, November 23, 1988.

2. Swain, A. D. & Guttman, H. E., "Handbook of Human Reliability Analysis With Emphasis on Nuclear Plant Applications," NUREC/CR-1278, USNRC, Washington, D. C., 1983.

3. - Severe Accident Issue Closure Guidelines, NUMARC 91-04, Nuclear Management & Resources Council, Inc., Washington, DC, January 1992.

006 Uncertainties and Sensitivities in Physical and Chemical Phenomenology--Thermal Phenomenon

Chair: N. Ortiz, SNL

Methodology to Evaluate Uncertainty in Thermalhydraulic Code Calculations
F. D'Auria, G.M. Galassi, S. Belsito (U. Pisa); N. Debrecin (U. Zagreb)

Two Methods for Estimating the Probability of Fuel/Coolant Interactions: Applications to Aluminum/Water
J.A. Close, R.L. Moore, L.G. Blackwood (INEL)

Uncertainties in the Characterization of the Thermal Environment of a Solid Rocket Propellant Fire
J.C. Diaz (LLNL)

Probabilistic Estimates of Hanford Waste Tank Failure due to Hydrogen Burns
R.K. Deremer (PLG), D.R. MacFarlane (LANL)

METHODOLOGY TO EVALUATE UNCERTAINTY IN THERMALHYDRAULIC CODE CALCULATIONS

D'Auria F.,[1] Debrecin N.,[2] Galassi G.M.,[1] Belsito S.[1]

[1] University of Pisa - Via Diotisalvi 2 - 56100 Pisa - Italy
[2] University of Zagreb - Croatia

ABSTRACT

The present paper deals with the description of a few aspects of the UMAE (Uncertainty Methodology based on Extrapolation of Accuracy) methodology suitable to evaluate the uncertainty in the prediction, by thermalhydraulic system codes, of the transient scenarios in nuclear reactors. The methodology is based upon the extrapolation of the accuracy resulting from the comparison between code results and relevant experimental data obtained in small scale facilities.

Emphasis is given in this paper to the statistical treatment of data obtained from experiments and code calculations. Some results related to the full application of the UMAE to a small break Loss of Coolant Accident in a PWR, including core uncovery, are reported.

1. INTRODUCTION

Evaluating nuclear power plant performance during transient conditions has been the main issue of safety researches in the thermalhydraulic area carried out all over the world since the beginning of the exploitation of nuclear energy for producing electricity in the 50's (e.g. State of the Art Report by CSNI and Compendium of ECCS Researches by US NRC, both issued in 1989[1,2]).

A huge amount of experimental data has been made available from very simple loops (Basic Test Facilities and Separate Effect Test Facilities) and from very complex Integral Test Facilities simulating all the relevant parts of a Light Water Reactor. On the other hand, sophisticated computer codes like Athlet, Cathare, Relap and Trac have been developed in Europe and United States and are widely in use at present. These are able to calculate time trends of any interesting quantity during any transient in LWRs with assigned boundary and initial conditions. The reliability of the predictions cannot be directly assessed owing to the lack of suitable measurements in the plants. So, the capabilities of the codes can be evaluated only from the comparison between calculation results and experimental data recorded in small scale facilities. In order to evaluate the applicability of a code in predicting a plant situation, one must be sure, at least, that the experimental data used for qualifying the codes are representative of phenomena expected in the plant and, subsequently that codes are able to reproduce qualitatively and quantitatively these data.

The (unknown) error made in predicting plant behaviour is called uncertainty, while the discrepancies between measured and calculated trends related to experimental facilities, are included in the accuracy of the prediction. The methodology here proposed aims at evaluating uncertainty from accuracy data[3,4].

The purpose of this paper is to show some features of the UMAE (Uncertainty Methodology based on Accuracy Extrapolation)[5] giving emphasis to the statistical treatment of the data.

2. BASIS AND DEVELOPMENT OF THE METHODOLOGY

The fundaments of the methodology have been discussed in previous papers[6,7] and can be drawn from the considerations 1 to 6 below, related to the test facilities and the codes. It is assumed that both of these are representative of the actual state of the art: i.e. facilities are "simulators" of a reference LWR and codes are based on the "six balance equations model" and must be intended as generically "qualified"[8].

1. The direct extrapolation of experimental data is not feasible; nevertheless, the time trends of significant variables measured during counterpart tests in differently scaled facilities are quite similar: this fact must be exploited.
2. Phenomena and transient scenarios occurring in larger facilities, being nearly constant the other conditions (e.g. design criteria, quality of instrumentation, etc.), are more close to plant conditions than those recorded from smaller facilities.
3. "Qualified" codes are indispensable tools to predict plant behaviour during nominal and off-nominal conditions.
4. The confidence in predicting a given phenomenon by the code, must increase when increasing the number of experiments analyzed dealing with that phenomenon.
5. The uncertainty in the prediction of plant behaviour cannot be smaller than the accuracy resulting from the comparison between measured and calculated trends; furthermore, accuracy (uncertainty) must be connected with the complexity of the facility (plant) and of the considered transient.
6. The effects of user and of nodalization must be included in the methodology.

The basic idea is to get the uncertainty from considering the accuracy. The main problems to achieve this are connected with the availability of experimental data that must be 'representative' of plants, with the quantification of accuracy and with the justification of any relationship between accuracy obtained in small dimensions loops with accuracy of the plant calculation, i.e. uncertainty.

The use of data base from counterpart and similar tests in Integral Test Facilities was of large help in this context, with main reference to the last mentioned problem. In particular, similar tests are those experiments performed in differently scaled facilities that are characterized by the occurrence of the same thermalhydraulic phenomena; counterpart tests are similar tests where boundary and initial conditions are imposed following a scaling analysis.

Two main aspects have been considered at a preliminary level to judge the realism of the accuracy extrapolation[5]: from the experimental side, the design of the facilities, the boundary and initial conditions of the experiments, the suitability of the instrumentation, the quality of the recorded data have been evaluated together with the similarity of the phenomena; from the code side, the general qualification process, the capability to simulate the relevant phenomena identified, the qualification of the nodalization and of the code user have been independently assessed.

Several parameters of geometric or thermohydraulic nature can be used, in principle, to derive uncertainty from accuracy values; furthermore, the use of a unique parameter is preferable to minimize the possibility of counterfeiting information from the available data base. The selected parameter should constitute a link between the experimental data and the data foreseeable in the plant in the case of occurrence of the conditions of interest, it must be representative of the involved phenomena at a global scale (i.e. the equivalent diameter in the core simulators is representative of thermalhydraulic phenomena in the core but does not affect substantially pressure behaviour during a depressurization transient), it must take into account the present status of the technology (i.e. the height of the facilities or the initial pressure might not be suitable parameters because they are nearly the same in the different facilities and in the reference plant).

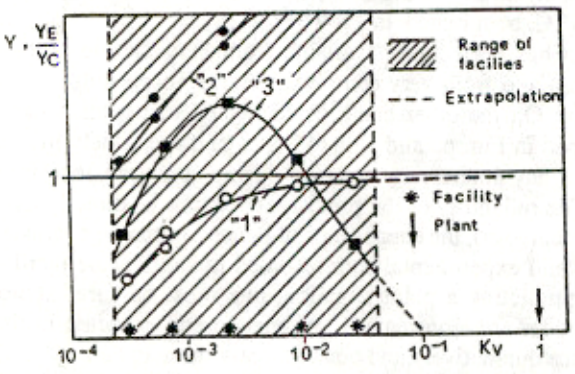


Figure 1. Possible trends resulting from scaling analyses: extrapolation of measured events/data and of code accuracy

Several parameters fulfill the above requirements, nevertheless the volume of the facility or, in dimensionless form, the ratio between primary system fluid volumes in the facilities and in the reference plant was selected as 'extrapolation' parameter.

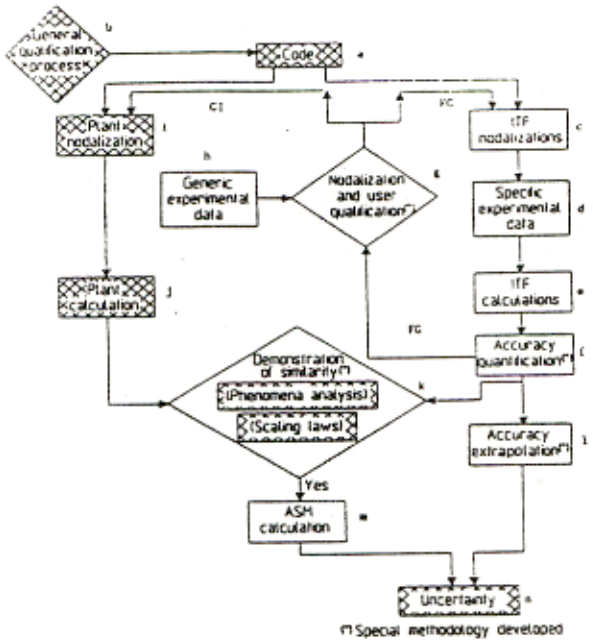
The situations depicted in Fig. 1 are expected from using such an approach[6]. The volume scaling ratio is reported on the horizontal axis; this quantity actually varies by four orders of magnitude from the smallest facility to the plant[5,12]. The shaded area represents the range of facilities, the smallest one and the largest one are characterized by a volume roughly 2000 times and 50 times, respectively, lower than that of a 1000 MWe plant. On the vertical axis the generic quantity Y and the ratio Y_E/Y_C (experimental over calculated value) are represented where Y is the value of any quantity that is relevant in a given transient.

3. OUTLINE OF THE UMAE

The use of calculated and measured data related to counterpart and similar tests, especially with the help of the code, directly led to the achievement of quantities connected with the uncertainty. "Dispersion bands" and "extrapolated" plant behaviour were previously defined and evaluated[5].

The UMAE procedure aims at calculating the uncertainty and, although making use of the same above-

mentioned data base, involves the rationalization of the various steps including the use of statistics in order to avoid or minimize the expert judgment at the various levels. Generic experiments in integral facilities and related calculations other than counterpart and similar tests, can be processed by the UMAE, provided the availability of data base related to a reasonable set of individual phenomena that envelope the key phenomena foreseeable in the selected plant scenario.



(*) Dashed blocks represent blocks that are common to UMANE and CSAU.

Figure 2. Simplified flowsheet of UMAE

A simplified flow-diagram of the UMAE is reported in Fig. 2. The way pursued to evaluate the data base and the conditions to extrapolate the accuracy are synthesized hereafter.

Evaluation of the Specific Data Base: the specific data base is constituted by the signals recorded during the considered experiments and by the results of the code calculations. Each test scenario (measured or calculated) should be divided into 'Phenomenological Windows' (Ph.W)[1]. In each Ph.W. 'Key Phenomena' (K.Ph) and 'Relevant Thermalhydraulic Aspects' (RTA) must be identified. K.Ph characterize the different classes (e.g. small break LOCA, large break LOCA, etc.) of transients and RTA are specific of the assigned one; K.Ph[4] are always applicable; an example of definition of RTA for small break LOCA in PWR can be found in ref. [5]. K.Ph and RTA qualitatively identify the assigned transient; in order to get quantitative information, each RTA must be characterized by 'Single Valued Parameters' (SVP, e.g. minimum level in the core), 'Non- Dimensional Parameters' (NDP, e.g. Froude number in hot leg at the beginning of reflux condensation), 'Time Sequence of Events' (TSE, e.g. time when dryout occurs) and 'Integral Parameters' (IPA, e.g. integral or average value of break flowrate during subcooled blowdown). Example of derivation of SVP, NDP, TSE and IPA can also be found in ref. [5].

Accuracy Extrapolation (block "1"): if the following conditions are fulfilled, accuracy in predicting SVP, NDP, IPA and TSE can be extrapolated[5]:

- the design scaling factors of the involved facilities are suitable;
- the test design scaling factors of the involved experiments are suitable;
- the experimental data base is qualified;
- the nodalizations and the related users are qualified;
- RTA are the same in the considered experiments if counterpart or similar tests are involved;otherwise, the same RTA can be identified in different experiments;
- RTA are well predicted by the code at a qualitative and a quantitative level;
- RTA are the same in the plant calculation 'facility K_V scaled' and in the experiments; parameters ranges (SVP, NDP, TSE and IPA), properly scaled, are also the same. This must be interpreted in different ways depending upon the availability of counterpart tests;
- in the plant calculation 'realistic conditions' Ph.W and K.Ph are the same as in the considered experiments; SVP, NDP, TSE and IPA may be different: reasons for this are understood.

The extrapolation of accuracy is achieved with reference to the above mentioned parameters through the use of the statistics[6]. The ratios of measured and calculated values of SVP, NDP, TSE and IPA are reported in diagrams like that shown in Fig. 1 assuming that they are randomly distributed around the unity value. This is also justified by the huge number of variables affecting the considered ratios. In this way 'mean accuracy' and '95th percentile accuracy' are derived that are applicable to the plant calculation. The measurement errors, the unavoidable scaling distortions and the dimensions of the facility are directly considered.

3.1 Statistical evaluation of the data base

A theory tailored to the available data base was set up.

The resulting value of the "average accuracy" is applicable to the results of plant calculations. Assuming that the distribution of the values of Y_E/Y_C is stochastic, the so-called "95th percentile accuracy" was defined. This assumption is justified by considering various experimental conditions and by the huge number of parameters which affect the above quantities (code models, code numeric, nodalizations, boundary conditions, user, etc.). The "average accuracy" was calculated as the average difference from the value of 1 of the Y_E/Y_C values. This and the standard deviation are given by:

$$\overline{A} = \frac{\sum_{i=1}^{4} \left| \left(\frac{Y_E}{Y_C} \right)_i - 1 \right|}{4} \qquad (1)$$

$$\sigma = \sqrt{\frac{\sum_{i=1}^{4} \left[\left| \left(\frac{Y_E}{Y_C} \right)_i - 1 \right| - \overline{A} \right]^2}{3}} \qquad (2)$$

Furthermore, assuming a Gaussian distribution for the deviation of Y_E/Y_C from unity, the "95th percentile accuracy" was calculated:

$$(A)_{95} = \overline{A} + 2\sigma \qquad (3)$$

The next step was to identify the uncertainty bands directly applicable to the results of the plant calculations representing the same single valued parameters. A reference value of the parameter representative of the plant scenario had to be defined to which "average accuracy" and the "95th percentile accuracy" can be applied. The average of the experimental values of the parameters, multiplied by the related scale parameter (if necessary) was selected:

$$Y_R = \frac{\sum_{i=1}^{4} Y_{E_i}}{4}. \qquad (4)$$

From this value the "average uncertainty" and the "95th percentile uncertainty" were calculated:

$$\overline{U} = \overline{A} \cdot Y_R \qquad (5)$$

$$(U)_{95} = (A)_{95} \cdot Y_R \qquad (6)$$

Weights which take into account of the intrinsic dispersion bands can be applied. The weight of each datum is proportional to the inverse of its dispersion band, so:

$$P_{D\,i} = \frac{1}{D_i} \qquad (7)$$

If a value is known without intrinsic dispersion (e.g. the peak cladding temperature in the data base considered) its weight should be infinite. To avoid this, a minimum dispersion derived from the unavoidable experimental signal error can be used.

An additional weight was introduced to take into account that the largest facilities are more suitable for simulating the plant behaviour. Combining these weights with those derived from Eq. (7), and normalizing so that the sum is 4:

$$P_i = 4 \frac{P_{D\,i} \cdot P_{K\,i}}{\sum_{i=1}^{4} P_{D\,i} \cdot P_{K\,i}} \qquad (8)$$

The average accuracy and the standard deviation are:

$$\overline{A} = \frac{\sum_{i=1}^{4} P_i \left| \left(\frac{Y_E}{Y_C} \right)_i - 1 \right|}{4} \qquad (9)$$

$$\sigma = \sqrt{\frac{\sum_{i=1}^{4} P_i \left[\left| \left(\frac{Y_E}{Y_C} \right)_i - 1 \right| - \overline{A} \right]^2}{3}} \qquad (10)$$

The results can be furtherly improved by assuming that the extrapolation toward larger and larger plants must involve an increase of the uncertainty. To account for this another uncertainty source has to be introduced. The following two conditions led to the definition of the related error:

- the minimum acceptable core assembly is 2 x 2, leading to a single channel. A scaling factor of 1/10000 roughly corresponds to this channel;
- the diameter of the downcomer in a facility scaled with K_V = 1/10000 is roughly 0.016 m, and this is too low. Similar considerations can be made in relation to the loop geometry.

The "extrapolation" error is:

$$E = \left| 0.3 - \frac{0.3}{\sqrt{K_V}} \right| (\%) \qquad (11)$$

The error calculated by Eq. (11) does not affect the calculation of accuracy but has to be taken into account in the calculation of uncertainty.

The reference value assumed for the plant, (Eq. 4), can be calculated by using weights which depend on the dispersion bands of the experimental parameters and on the weights of the facilities:

$$P_{R\,i} = 4 \frac{P_{E\,i} \cdot P_{K\,i}}{\sum_{i=1}^{4} P_{E\,i} \cdot P_{K\,i}} \qquad (12)$$

The weights P_E (related to Y_E) are calculated from the dispersion bands of the experimental values in the same way as the weights P_D (related to Y_E/Y_C). The reference value for the plant and the related standard deviation can be calculated as:

$$Y_R = \frac{\sum_{i=1}^{4} P_{R_i} \cdot Y_{E_i}}{4}. \qquad (13) \qquad \sigma_R = \sqrt{\frac{\sum_{i=1}^{4} P_{R_i} \cdot \left(Y_{E_i} - Y_R\right)^2}{3}} \qquad (14)$$

Finally, the uncertainty can be calculated as:

$$\overline{U} = Y_R \cdot \left(\overline{A} + E\right) \quad (15) \qquad \text{and} \qquad (U)_{95} = Y_R \cdot (\overline{A} + E) + 2 \cdot \sigma_R \cdot (\overline{A} + E) + 2 \cdot Y_R \cdot \sigma \quad (16)$$

4. APPLICATION OF UMAE

Parts or concepts of the UMAE have been applied to transient scenarios like small break LOCA in BWR[10], natural circulation in PWR[11], Loss of feedwater in PWR[12]; in these cases, quantities connected with uncertainty have been derived.

The only complete application, so far, has been carried out with reference to a small break LOCA in PWR[5], where Lobi, Spes, Bethsy and Lstf facilities are involved. Significant results from this analysis are summarized hereafter.

The transient is originated by a side oriented break in the cold leg having an area equivalent, roughly to 6% of the area of the cold leg itself. The sequence of interventions is typical of this kind of transient in a plant: after the break occurrence, scram and pumps trip are provided together with a signal for isolating steam generators. Accumulators intervention is foreseen when primary pressure falls below 4.2 MPa. Following accumulators emptying, break flowrate causes mass depletion in the primary system leading unavoidably to core dryout toward the end of the transient. In Lobi and Spes, Low Pressure Injection System actuation is foreseen and is effective in rewetting the rods. An idea of the transient scenario can be drawn from Figs. 3 and 4; the first dryout situation at about 100 s into the transient should be noted: this is quenched by loop seal clearing. The transient was subdivided into four Ph.W[5] and more than 40 RTA were identified. Some experimental values of TSE and SVP are given in Tab. 1.

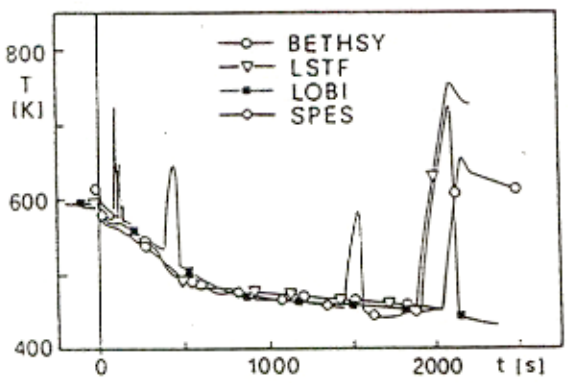


Figure 3. Small break LOCA counterpart tests: heater rod surface temperature

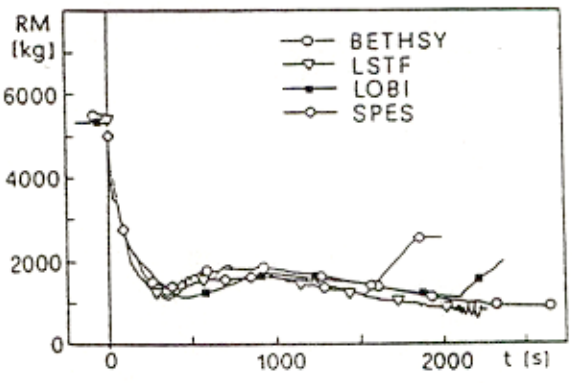


Figure 4. Small break LOCA counterpart tests: scaled primary side residual mass

TSE/SVP	unit	LOBI	SPES	BETHSY	LSTF
Duration of phase a)	s	0÷164	0÷138	0÷176	0÷165
time of pressurizer emptying	s	0-23	1-12	0-18	0-16
average specific break flowrate	kg/sm^2	39706	50257	47872	48169
first dry-out duration	s	135-178	112-132	134-159	94-129
direction of bypass flowrate	-	from UH to DC	from UH to DC	from UH to DC	from UH to DC
cold leg flowrate is less than 5% of the initial value	s	157	110	106	180
Duration of phase b)	s	164÷1705	138÷1322	176÷1730	165÷1572
time of primary-secondary pressure reversal	s	164	115-138	176	165
time of SGs U-tubes emptied	s	450	150	200	250
primary mass at time of accumulator intervention	%	21	26	21.4	19.8
accumulator intervention period	s	420-953	355-1058	345-976	346-688
time when minimum mass in primary side occurs	s	420	355	350	350
Duration of phase c)	s	1705÷2100	1322÷1522	1730÷2179	1572÷2113
third dry-out duration	s	1705-2150	1322-1500	1730-end	1572-end
Duration of phase d)	s	2100÷2400	1522÷2034	-	-
time of minimum mass in the primary side	s	2100	1522	2100	2100
value of minimum mass in primary side	%	21	26	21.4	19
saturation temperature decrease in SG-SS	K	548-546	549-552	554-553	557-556
average specific break flowrate	kg/sm^2	1764	2432	1006	1635
average rate of rod surface temperature increase	K/s	1.4	1.1	0.6	1.5

Table 1. Selected TSE and SVP values during the counterpart tests

The results shown in ref. [34] demonstrate that the Relap5/mod2 code is able to predict all of these.

The application of the statistical methodology, (sect. 3.1), dealing with step "l" in Fig. 2, led to the 'average' and '95th percentile' uncertainty values.

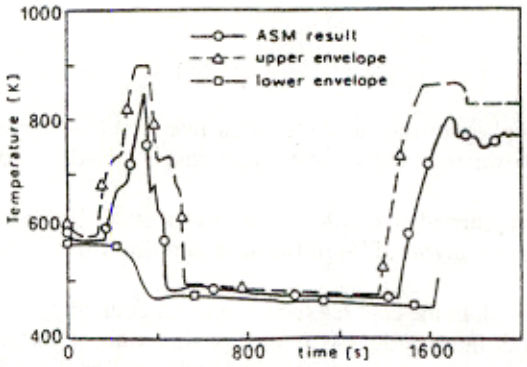


Figure 5. Uncertainty resulting from ASM calculation of a Small Break LOCA in the KRSKO Westinghouse plant.

The last step (block "n" in Fig. 2) consisted in deriving continuous values of 'timing', 'spatial' and 'mean integral' uncertainty, to be superimposed to the ASM calculation results carried out in 'realistic conditions'. The Westinghouse 630 Mwe two loops plant of Ksrko (Slovenia) was selected as reference reactor for the ASM calculation[5].

The results related to the rod surface temperature are shown in Figs. 5. For simplicity only the envelope of the curves obtained from the three above-mentioned types of uncertainty are shown. It can be noted that the positive error in predicting the peak cladding temperature is of the order of 100 K. The occurrence of the first dryout situation combines, in the 'realistic conditions' calculation with the second one occurring in the experiments.

5. CONCLUSIONS

The UMAE methodology has been presented that allows the calculation of uncertainty in the predictions of off-normal conditions in nuclear reactors by thermalhydraulic system codes. Essentially, the uncertainty is derived from the extrapolation of accuracy obtained by comparing measured and calculated variables trends that are relevant to the assigned accident scenario. The use of data from counterpart tests, was of large help in developing the concepts at the basis of the methodology.

One complete example of application of the UMAE to a small break LOCA in PWR has been given. In that case dryout is foreseen and peak cladding temperature, including the error of the order of 100 K, remains well below the licensing limits.

The main peculiarity of the UMAE is the direct exploitation of the huge experimental data base now available from integral test facilities: this is strictly necessary and is retained suitable to characterize any foreseeable accident scenario in Light Water Reactors. Moreover, all the aspects contributing to the uncertainty are taken into consideration: the user effect, the nodalization qualification, the errors in introducing boundary and initial conditions, the intrinsic capabilities of the code in predicting the phenomena of interest, are fully included in the final evaluation of the error bands.

The comparison with the CSAU methodology demonstrated that the expert judgment is avoided or minimized in the UMAE. Furthermore, the logic of UMAE prevents its use when phenomena expected in the

plant are not satisfactorily simulated by the code or when the code itself is based upon too simplified assumptions.

Few additional biases to be included in the final value of uncertainty that are not fully considered by the UMAE, have been identified. Among these, the potential occurrence of important multidimensional phenomena represents a critical issue if only codes based on one-dimensional models are available: experimental data from specific facilities should be used to accertain the codes capabilities in this connection.

Finally, it can be mentioned that the UMAE development required an effort equivalent, roughly to 10 man-years.

REFERENCES

/1/ CSNI Group of Experts. "Thermohydraulic of Emergency Core Cooling in Light Water Reactors", Report No. 161, Committee on the Safety of Nuclear Installations (Sep. 1989)

/2/ US-NRC. "Compendium of ECCS Research for Realistic LOCA Analysis", NUREG-1230, U.S. Nuclear Regulatory Commission (Dec. 1989)

/3/ Boyack B.E., Catton I., Duffey R.B., Griffith P., Katsma K.R., Lellouche G.S., Levy S., Rohatgi U.S., Wilson G.E., Wulff W., Zuber N. "An overview of the code scaling, applicability, and uncertainty evaluation methodology", J. Nuclear Engineering and Design Vol. 119, 1990

/4/ Boyack B.E., Catton I., Duffey R.B., Griffith P., Katsma K.R., Lellouche G.S., Levy S., Rohatgi U.S., Wilson G.E., Wulff W., Zuber N. "Characterization of important contributors to uncertainty", J. Nuclear Engineering and Design Vol. 119, 1990

/5/ D'Auria F., Debrecin N., Galassi G.M. "Outline of the Uncertainty Methodology based on Accuracy Extrapolation (UMAE)", Submitted at J. Nuclear Technology.

/6/ Bovalini R., D'Auria F. "Scaling of the accuracy of Relap5/mod2 Code", J. Nuclear Engineering and Design, vol 139 Nr. 1, 1993

/7/ Bovalini R., D'Auria F., Galassi G.M. "Scaling of complex phenomena in System Thermalhydraulics", J. Nuclear Science and Engineering, Oct. 1993

/8/ D'Auria F. "Experimental Facilities and System Codes in Nuclear Reactor Safety", Int. Seminar State of the Art on Safety Analyses and Licensing of Nuclear Power Plants, Varna (BG), Nov. 2-6 1987

/9/ Belsito S., D'Auria F., Galassi G. M. "Application of a Statistical model to the evaluation of Counterpart Test data base", ANS Winter Meeting, San Francisco (US), Nov. 10-13 1993

/10/ Bovalini R., D'Auria F., De Varti A., Maugeri P., Mazzini M. "Analysis of Counterpart Tests performed in BWR Experimental Simulators", J. Nuclear Technology, Vol. 97 Nr. 1, 1992

/11/ D'Auria F., Galassi G.M., Vigni P., Calastri A. "Scaling of Natural Circulation in PWR Systems", J. Nuclear Engineering and Design, Vol 132 Nr. 2, 1992

/12/ D'Auria F., Debrecin N., Galassi G.M., Galeazzi S. "Application of RELAP5/MOD3 to the Evaluation of Loss of Feedwater in test Facilities and in Nuclear Plants", J. Nuclear Engineering and Design. Vol. 141, Nr. 3, 1993

TWO METHODS FOR ESTIMATING THE PROBABILITY OF FUEL/COOLANT INTERACTIONS - APPLICATIONS TO ALUMINUM/WATER

J. A. Close, R. L. Moore, and L. G. Blackwood

Idaho National Engineering Laboratory
EG&G Idaho, Inc.,
P. O. Box 1625
Idaho Falls, ID 83415

INTRODUCTION

One of the important phenomena that may be involved in severe accidents of nuclear reactors is known as fuel/coolant interaction (FCI). A FCI results from the interaction of very hot fuel with the coolant and can be quite complex for certain metal/water systems. This is the case for research, test and production reactors, which utilize uranium-aluminum fuels to minimize non-productive neutron absorption. In the uranium-aluminum/water system, when molten fuel is poured into water (referred to as pour mode), the phenomenon can range from relatively benign rapid boiling, to a vapor explosion, to a vapor explosion accompanied by ignition, a self-sustaining exothermic chemical reaction producing hydrogen. The exothermic reaction releases considerably more energy than the vapor explosion alone. Uranium-aluminum/water FCIs, with low atomic percent uranium, are believed to behave like aluminum/water FCIs, and since there are so few data for the uranium-aluminum/water system, the data on which this study is based are limited to those from aluminum/water FCIs.

The motivation for the present study was twofold. First, an estimate of the probability of vapor explosions from pouring uranium-aluminum melt into water is essential for estimating the risk from this phenomenon. Second, an estimate of the probability of ignition was needed. Some theoretically based arguments have been advanced for such an estimate, but they are only weakly linked to experimental data. To obtain these estimates, data from 6 studies [1-6], comprising 82 experiments, were analyzed using two statistically based methods, the pLOGIC proprietary software and logistic regression analysis.

DATA

Results from pour mode aluminum/water FCI experiments and theoretical studies show that many parameters may affect the progression of aluminum/water FCIs. A screening was performed to select the following parameters, which were considered most important: the mass, temperature, entry velocity (represented by drop height), and pour diameter (represented by crucible hole diameter) of the melt; and water depth and subcooling. Wettability of the bottom surface of the tank is also important, but only data from experiments employing mild or stainless steel tank bottoms were used; therefore, no change was assumed for this parameter. External trigger occurrence and strength are other important parameters, but were not of interest in this study. Pertinent data, extracted from the

aluminum/water vapor explosion literature cited above, are presented in Table 1. These were the base values used in the pLOGIC and logistic regression analyses.

Table 1. Aluminum-water vapor explosion database used for pLOGIC and logistic regression analysis.

Reference	Mass (kg)	Hole Diameter (cm)	Drop Height (cm)	Water Depth (cm)	Aluminum Temp (K)	Water Temp (K)	Subcooling (K)	Vapor Explosion Prediction	Vapor Explosion Probability	Ignition Prediction
Long	22.00	1.91	30.48	15.24	943[1]	292.5	80.5	No	0.3125	No
[1]	22.00	3.81	30.48	15.24	943[1]	292.5	80.5	No	0.3125	No
	22.00	6.35	30.48	15.24	943[1]	292.5	80.5	No	0.4375	No
	22.00	6.99	30.48	15.24	943[1]	292.5	80.5	Yes	0.6364	No
	22.00	8.25	30.48	15.24	943[1]	292.5	80.5	Yes	0.6364	No
	22.00	10.16	30.48	15.24	943[1]	292.5	80.5	Yes	0.8333	No
	4.40	6.99	30.48	15.24	1023	292.5	80.5	Yes	0.6667	No
	22.00	8.25	76.20	15.24	943[1]	292.5	80.5	Yes	0.6364	No
	22.00	8.25	106.68	15.24	943[1]	292.5	80.5	Yes	0.7273	No
	22.00	8.25	289.56	15.24	943[1]	292.5	80.5	No	0.1667	No
	22.00	8.25	30.48	7.62	943	292.5	80.5	Yes	0.6667	No
	22.00	8.25	30.48	25.40	943	292.5	80.5	No	0.4545	No
	22.00	8.25	30.48	25.40	1023	292.5	80.5	Yes	0.6364	No
	22.00	8.25	30.48	50.80	1023	292.5	80.5	No	0.3125	No
	22.00	8.25	30.48	76.20	1173	292.5	80.5	No	0.0625	No
	22.00	8.25	30.48	5.08	943	292.5	80.5	No	0.4375	No
	22.00	8.25	30.48	5.08	1023	292.5	80.5	No	0.4375	No
	22.00	8.25	30.48	5.08	1173	292.5	80.5	No	0.4375	No
	22.00	8.25	30.48	15.24	1023	273	100	Yes	0.6364	No
	22.00	8.25	30.48	15.24	1023	323	50	Yes[2]	0.6667	No
	22.00	8.25	20.32	25.40	1023	273	100	Yes	0.8333	No
	22.00	8.25	20.32	25.40	1023	323	50	Yes[2]	0.5455	No
	22.00	8.25	30.48	15.24	1023	333	40	No	0.4545	No
	22.00	8.25	30.48	15.24	1023	373	0	No	0.1818	No
	22.00	8.25	20.32	25.40	1023	333	40	No	0.2727	No
	22.00	8.25	20.32	25.40	1023	373	0	No	0.3125	No
Lemmon	12.32	8.25	35.56	15.24	1000	292	81	Yes	0.7273	No
[2]	12.32	8.25	35.56	15.24	1183	292	81	Yes	0.5455	No
	12.32	8.25	35.56	15.24	1183	292	81	Yes[2,3]	0.5455	No
	12.32	8.25	35.56	15.24	1183	292	81	Yes	0.5455	No
	12.32	8.25	35.56	15.24	1189	292	81	No	0.4545	No
	17.60	8.25	35.56	15.24	1189	292	81	No	0.4545	No
	12.32	8.25	35.56	15.24	1322	292	81	Yes	0.7273	Yes
	12.32	8.25	35.56	15.24	1244	292	81	Yes	0.6364	Yes
	12.32	8.25	35.56	15.24	1283	292	81	Yes[2,3]	0.7273	No
	12.32	8.25	35.56	15.24	1283	292	81	Yes[2,3]	0.7273	No
	12.32	8.25	35.56	15.24	1311	292	81	Yes[2,3]	0.7273	No
	12.32	8.25	35.56	15.24	1300	292	81	Yes	0.7273	Yes
	12.32	8.25	35.56	15.24	1305	292	81	Yes	0.7273	Yes
	12.32	8.25	35.56	15.24	1289	292	81	Yes	0.7273	No
	12.32	8.25	35.56	15.24	1316	292	81	Yes	0.7273	No
	12.32	8.25	35.56	15.24	1283	292	81	Yes	0.7273	Yes
	12.32	8.25	35.56	15.24	1327	292	81	Yes	0.7273	Yes
	4.40	8.25	35.56	15.24	1310	292	81	Yes	0.7273	Yes
Greene et al	1.79	0.32	19.00	50.00	976	296.7	76.3	No	0.001	No
[3]	0.98	0.32	19.00	50.00	963	315.5	57.5	No	0.001	No
	1.72	0.32	19.00	50.00	1008	313.2	59.8	No	0.001	No
	1.39	0.32	19.00	50.00	1009	332	41	No	0.001	No
	1.98	0.32	19.00	50.00	1001	323.8	49.2	No	0.001	No
	1.90	0.64	19.00	50.00	991	295.9	77.1	No	0.001	No
	1.98	0.64	19.00	50.00	983	304	69	No	0.001	No
	2.06	0.64	19.00	50.00	988	315	58	No	0.001	No
	2.00	0.64	19.00	50.00	992	322.7	50.3	No	0.001	No
	2.02	0.64	19.00	50.00	993	333.5	39.5	No	0.001	No
	2.00	0.64	19.00	50.00	993	343.7	29.3	No	0.001	No
	1.94	0.64	43.00	25.00	993	344.9	28.1	No	0.4375	No

Table 1. (Continued)

Reference	Mass (kg)	Hole Diameter (cm)	Drop Height (cm)	Water Depth (cm)	Aluminum Temp (K)	Water Temp (K)	Subcooling (K)	Vapor Explosion Prediction	Vapor Explosion Probability	Ignition Prediction
	1.69	0.32	43.00	25.00	1015	344	29	No	0.4375	No
	2.50	1.27	21.00	50.00	939	326.6	46.4	No	0.001	No
	2.81	1.27	29.50	50.00	952	314.2	58.8	No	0.001	No
	2.57	1.27	40.00	30.00	953	313	60	No	0.4375	No
	2.77	1.27	35.00	30.00	952	313.7	59.3	No	0.4375	No
	2.70	1.27	40.00	50.00	957	313	60	No	0.001	No
Briggs	2.00	8.25	110.00	20.00	1020	282	91	No	0.500	No
[4]	7.50	8.25	97.00	15.00	1030	297	76	Yes	0.6364	No
	10.50	8.25	100.00	8.00	1082	291	82	No	0.4375	No
	19.90	8.25	100.00	20.00	1073	292	81	Yes[2,3]	0.8333	No
	20.00	8.25	50.00	20.00	1076	281	92	Yes	1.000	No
	20.00	8.25	50.00	15.00	1073	278	95	Yes[2,3]	0.9091	No
	20.00	8.25	50.00	20.00	1073	276	97	Yes	0.9091	Yes
	20.00	8.25	50.00	20.00	1077	280	93	Yes	0.9091	No
	20.00	8.25	50.00	20.00	1072	294	79	Yes	0.8889	No
	20.00	8.25	50.00	20.00	1075	283	90	Yes	1.000	No
	20.00	8.25	50.00	20.00	1076	280	93	Yes	0.9091	Yes
	10.00	8.25	100.00	20.00	1079	281	92	Yes	0.7273	No
Hess and	22.00	8.25	43.18	12.70	983	282	91	Yes	0.9091	No
Brondyke	22.00	8.25	43.18	12.70	983	301	72	Yes	0.8182	No
[5]	22.00	8.25	43.18	12.70	1094	282	91	Yes	0.7778	No
	22.00	8.25	43.18	12.70	1094	301	72	Yes	0.9091	No
Hess et al	22.00	8.25	29.84	15.24	977.8	276.67	96.33	Yes	0.7273	No
[6]	22.00	8.25	29.84	15.24	977.8	304	69	Yes	0.7778	No
	22.00	8.25	29.84	15.24	1116	276.67	96.33	Yes	0.9091	No
	22.00	8.25	29.84	15.24	1116	304	69	Yes	0.500	No

[1] Melt temperature changed from 943 to 1023 K.
[2] Potentially bad data point identified by pLOGIC.
[3] Incorrect prediction by pLOGIC.

ANALYSIS WITH pLOGIC

The extracted data were used in conjunction with pLOGIC [7], an advanced statistical pattern recognition computer code. The function of pLOGIC is to recognize patterns in data, i.e., the program analyzes the interactions among all the variables one identifies as being important to the problem so as to learn their underlying relationships. To use pLOGIC one has to supply it with a database corresponding to the problem to be solved. pLOGIC takes the historical database and develops from it a number of trained rules (decision rules) based on the input database. Then based on the decision rules, pLOGIC takes new data and classifies it. In this study pLOGIC classifies the new data as to whether a vapor explosion will occur or not occur. Once the code has trained itself on the data, it produces a model that can predict with high statistical reliability when such patterns will occur again. pLOGIC uses a form of the k-nearest neighbor statistical method. The present study utilized pLOGIC to reduce the number of potentially bad data points associated with the experiment data, and to predict the probability of vapor explosion and ignition.

One of the features of pLOGIC is the ability to indicate data that are inconsistent, and hence suspect. The literature was sometimes ambiguous about experimental conditions, or occasionally did not include parameter values because of instrumentation failures. Alternative runs with pLOGIC allow one to adjust the suspect parameter values and search for a more consistent set of experimental parameters. Using this procedure together with insights gained from the literature, 6 variations on the original database were developed, using "improved" values for questionable parameters. With this technique, a new database was found that reduced the number of incorrect predictions from 18 to 6 and the number of potentially bad data points from 19 to 6. The pLOGIC predictions (yes or no) and probabilities for vapor explosion for each experiment shown in Table 1 are derived from the new database. pLOGIC predicts yes for an explosion if the probability is greater than or equal to 0.5. Footnotes in Table 1 indicate a) melt temperatures that were changed to improve the pLOGIC model, b) experiments with additional potentially bad data points, and c) pLOGIC predictions

that are incorrect. It is interesting to note that, in all incorrect cases, pLOGIC predicted explosions would occur.

Upon replacing the questionable values in the original database with the preferred consistent values, the pLOGIC model determined that pour diameter, water depth, and subcooling are important parameters with respect to vapor explosion.

There was a particular need to estimate the probability of vapor explosion for conditions in the following range:

- Melt mass 5 - 7 kg
- Melt temperature 925 - 1150 K
- Drop height 10 cm
- Hole diameter 2 - 5 cm
- Water depth 70 -100 cm
- Water subcooling 0 - 80 K

The pLOGIC model with the most consistent database estimates the probability to be less than or equal to 0.001 for these conditions.

The same type of analysis was performed to determine if ignition would occur during a vapor explosion. For this analysis, the important parameters are: the temperature of the melt, the mass of the melt, and whether or not a vapor explosion occurs prior to an ignition event. Drawing from the vapor explosion experiments that have been conducted over the last three decades, it is known an ignition event will not occur if not preceded by a vapor explosion. At this time there is no way to convey to pLOGIC that there is a bias toward the explosion variable (yes or no) when the variable is entered as no. Thus, there, is a chance that pLOGIC could give a yes - ignition will occur - even if a vapor explosion was predicted not to occur. However, the likelihood of this happening is small. pLOGIC analysis estimated the probability of ignition to be less than 0.001 for the conditions listed previously. The version of pLOGIC used does not provide probabilities less.than 0.001.

To assess the credibility for using pLOGIC to estimate the probability of ignition events occurring, some aluminum FCI data recently generated from experiments at Sandia National Laboratories [8] were investigated. Two of the six Sandia tests were reported to have no external trigger. One of these resulted in a vapor explosion involving ignition. pLOGIC correctly predicted the experiment outcome with a probability of 0.588. The relatively low probability is attributed to the paucity of experiments performed with melt temperatures above 1300 K. Aluminum temperature for the Sandia experiment was 1540 K.

LOGISTIC REGRESSION ANALYSIS

A logistic regression analysis was performed to reanalyze the data used in the pLOGIC analyses to provide results that can be compared to those produced by pLOGIC.

Prediction of outcomes based on specific input variable values is often obtained using standard linear regression analysis methods. However, when the outcome is a binary response (in this case explosion or no explosion) and the interest is in predicting probabilities of outcomes, standard regression methods do not work well. Logistic regression is a method of analysis for investigating the relationship between binary response variables and explanatory variables that avoids the shortcomings of standard regression methods. Rather than modeling binary outcomes or probabilities directly, logistic regression models the logit or logarithm of the odds of a binary event as a linear function of the input variables. The logistic regression analysis in this study was performed using the procedure LOGISTIC in the SAS statistical software package [9].

An important part of the modeling procedure is to establish which of the seven variables aluminum mass, drop height, hole diameter, water depth, aluminum temperature, water temperature, and subcooling should be included in the model. The "preferred" model for the data is one which, according to a specific set of criteria, contains all variables with significant effects and none with non-significant effects. Using the SAS software, a preferred logistic model was selected, maximum likelihood estimates were obtained for the slope and intercept parameters in the model, and an equation and uncertainties for predicted explosion probabilities for specific sets of values of explanatory variables were developed.

Figure 1 is a scatterplot of water subcooling by hole diameter with a contour plot of predicted vapor explosion probabilities. Hole diameter and subcooling were the only two parameters found to influence the probability in the logistic regression analysis. An

indication of what confidence can be placed in the prediction of vapor explosion probability is also shown for representative experiments. The innermost error bars are the lower and upper confidence interval bounds, given the data are reasonably correct. However, as mentioned earlier, some of the data in the literature were ambiguous. To the extent that the data values used were incorrect, bias has been introduced into the parameter estimates and thus the predicted probabilities of explosion. Thus the true uncertainty in the predicted values is greater than that indicated by the confidence intervals alone. An estimate of total uncertainty is depicted with the outermost error bars, which include the bias error . Arrows indicate error bars extending beyond the edge of the graph.

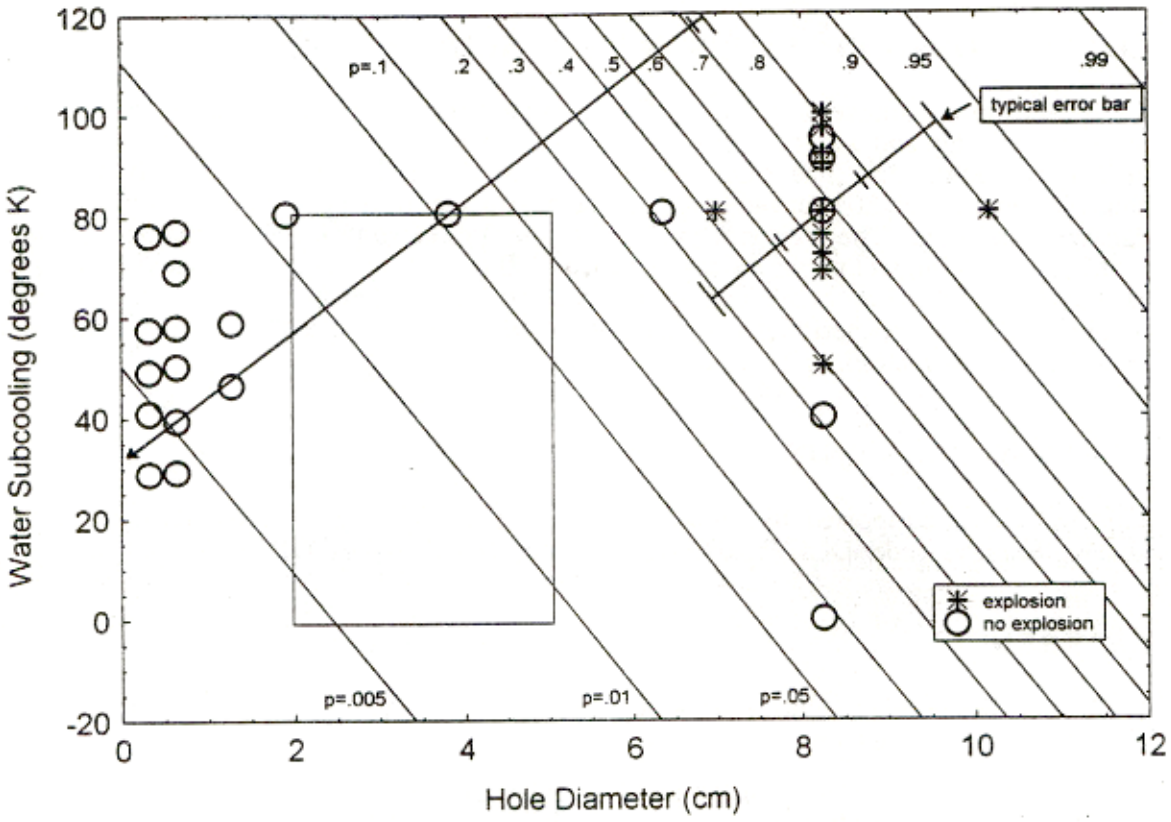


Figure 1. Scatterplot of water subcooling by hole diameter with a contour plot of predicted vapor explosion probabilities. The rectangle delineates the region of interest.

The estimate of the extent of bias uncertainty induced by the estimated data values, was obtained by substituting alternate values for some of the questionable data. No changes were made in the hole diameter data because it was quite well reported in the studies reviewed. In two studies, subcooling was not well reported so some changes were made in that variable. Of the variables not in the model, aluminum temperature showed the greatest potential for uncertainty, so changes were made there as well to see if the model building process was affected. Some data were so poorly summarized that all variable values, including the occurrence of explosions are suspect. Those cases were completely eliminated from the bias analysis.

Four sets of changes were made to the original data. By taking all combinations of the four sets, 36 alternate data sets were created. The logistic regression analysis was repeated for each of the 36 alternate data sets and the resulting models and parameter estimates compared to that obtained using the original data values. All data sets except two produced the same variables in the preferred model as those selected in the analysis of the original data (i.e. hole diameter and subcooling). In the two exceptions only hole diameter entered the model. The bias for a predicted logit was calculated using the bias error propagation formula of Coleman and Steele [10].

An expression for the total uncertainty in the predicted logit can be obtained by combining the confidence interval uncertainty with the bias uncertainty. The formulas for

obtaining total uncertainty are based on the methods described in Coleman and Steele. The total uncertainty limits are a combination of 95% confidence limits and bias limits of unknown coverage. If the bias limits can be assumed to be a reasonable approximation of 95% limits on bias, then the total uncertainty limits are 95% limits. Otherwise they are a hybrid of limits.

The uncertainty intervals are quite wide in all cases, indicating that the predicted probabilities of explosions can only be taken as rough indicators of the true probabilities. The bias error has little effect on the relative uncertainty for some data points but a quite large effect for others. The length of the total uncertainty intervals compared to the precision error uncertainty intervals varied from less than 5% larger to more than twice as large.

CONCLUSIONS - COMPARISON OF RESULTS

Based on the sparse data, pLOGIC determined that three parameters: hole diameter, water subcooling, and water depth are important; whereas logistic regression analysis found only hole diameter and subcooling to be significant. This difference is probably due to the paucity of experimental data, and to the particular structure of the experiments from which the data were collected. The logistic regression analysis predicted probability of vapor explosion in the region of interest to vary from less than 0.005 to 0.1. The total estimated uncertainty associated with these probabilities is quite large and spans the probability of 0.001 predicted by pLOGIC. Three experiments are planned in the region of interest to improve confidence in probability estimates in that space.

ACKNOWLEDGMENTS

This work was supported by the U.S. Department of Energy, Assistant Secretary for Nuclear Energy, Under DOE Field Office Contract DE-AC07-76ID01570.

REFERENCES

1. G. Long, Explosion of Molten Aluminum in Water - Cause and Prevention, *Metal Progress*, 71, 5, (1957) pp. 107-1 12 .

2 A. W. Lemmon, Explosions of Molten Aluminum and Water, *Light Metals 1980 Conference Proceedings*, The Metallurgical Society of AIME (1980), pp. 817-835.

3. G. A Greene, C. C. Finfrock, C. E. Schwarz, and M. L. Hyder, "Breakup of Molten Aluminum Jets Injected Into Water", BNL 52327, January 1992.

4 A. J. Briggs, Experimental Studies of Thermal Interactions at AEE Winfrith, *Proceedings of the Third Specialist Meeting on Sodium/Fuel Interaction in Fast Reactors*, Tokyo Japan, March 22-26, 1976.

5. P. D. Hess and K. J. Brondyke, Causes of Molten Aluminum-Water Explosions and Their Prevention, *Metal Progress*, 95, 4, (1979), pp. 93-100.

6. P. D. Hess, R. E. Miller, W. E. Wahnsiedler, C. N. Cochran, Molten Aluminum/Water Explosions, *Proc. of Tech. Sessions Sponsored by TMS Light Metals Committee at 190th AIME Annual Mtg.*, C. McMinn Ed., (1980).

7. Knowledge Systems, Inc., pLOGIC. Version 1.0, (1990).

8. M. J. Rightley, D. F. Beck, and M. Berman, "NPR/FCI EXO-FITS Experiment Series Report," SAND91-1544, January 1993.

9. SAS Institute Inc., "SAS Technical Report P-200, SAS/STAT Software: CALIS and LOGISTIC Procedures, Release 6.04," Cary, NC, (1990).

10. Coleman, H. W., and Steele, W. G. Jr., "Experimentation and Uncertainty Analysis for Engineers," John Wiley and Sons, New York (1989).

UNCERTAINTIES IN THE CHARACTERIZATION OF THE THERMAL ENVIRONMENT OF A SOLID ROCKET PROPELLANT FIRE*

Julio C. Diaz

Lawrence Livermore National Laboratory
P.O. Box 808, L-85
Livermore, CA 94551

INTRODUCTION

There has been an interest in developing models capable of predicting the response of systems to Minuteman (MM) III third-stage solid propellant fires. Input parameters for such an effort include the boundary conditions that describe the fire temperature, heat flux, emissivity, and propellant burn rate. In this study scanning spectroscopy and pyrometry were used to infer plume temperatures. Each diagnostic system possessed strengths and weaknesses. The intention was to use various supportive methods to infer plume temperature and emissivity, because no one diagnostic had proven capabilities for determining temperature under these conditions. Furthermore, these diagnostics were being used near the limit of their applicability. All these points created some uncertainty in the data collected.

Temperature Measurements

We used two spectrometric methods of temperature measurement to determine the temperature profile. These methods operate on the principle that perfectly radiating bodies (blackbodies) at a given temperature will emit energy within a range of wavelengths and at an intensity that is predicted by Planck's Equation. Most real surfaces are not perfect blackbodies but radiate energy at some fraction of a blackbody: these are referred to as graybodies and the fraction is referred to as emissivity (ε). Assuming that the plume was a freely radiating graybody, the spectral radiance could be modeled from Planck's equation as

$$L(\lambda, T) = \frac{\varepsilon C_1}{\lambda^5 (\exp(C_2 / \lambda T) - 1)} \qquad (1)$$

* Work performed by Lawrence Livermore National Laboratory under the auspices of the U.S. Department of Energy under contract number W-7405-ENG-48s.

where

$L(\lambda,T)$ = spectral radiance from the plume (mW/cm^2 nm)
T = source temperature (K)
ε = emissivity of the plume
λ = wavelength (mm)
C_1 = 37418 E3 mW mm^5/cm^2 nm
C_2 = 14388 mm K.

Pyrometry and spectrometric methods were used to determine plume temperatures. W. Eckl and N. Eisenreich[1] were able to successfully estimate plume temperatures by analyzing the continuous emission spectra of burning solid propellant. We wanted to determine if our propellant, being similar in composition to the one they used, behaved as a graybody radiator in the visible to near-IR field (400 to 900 nm). Knowing the degree to which the plume spectrum resembled a graybody would allow us to apply pyrometry to take continuous temperature measurements.

Pyrometry. Two pyrometric methods were used to extract temperature and emissivity data for the plume. A two-color commercial pyrometer with narrow bandwidths located between wavelengths of 780 and 1000 nm was used to infer the temperature. This system determines temperature based on the ratio of the intensities at each of two wavelengths and is generally appropriate for use on a graybody or blackbody source. However, the instrument we used was adjustable and could determine temperatures for non-graybodies as long as the body produces a continuous spectrum between 780 nm and 1000 nm.

A second, single-color commercial pyrometer with a narrow bandwidth at 950 nm was used to provide a method of determining ε. A color temperature was inferred by the single-color pyrometer based on the assumption that the plume was a blackbody (ε=1). To estimate emissivity we coupled the measurements of the two-color pyrometer with that of a single-color pyrometer by focusing our pyrometers on the same volume-space of the plume. This (ratio spectrometry) is an accepted method and its validity has been tested by R. B. Johnson and C. Feng.[2] Assuming that the plume acts as a graybody, then

$$L_1(\lambda,T) = \frac{C_1}{\lambda^5(\exp(C_2/\lambda T_1)-1)} = L_2(\lambda,T) = \frac{\varepsilon C_1}{\lambda^5(\exp(C_2/\lambda T_2)-1)} \qquad (2)$$

where

subscript 1 refers to measurements by the two-color pyrometer,
subscript 2 refers to measurements by the single-color pyrometer,
and λ = wavelength of single-color pyrometer (950 nm).

To solve for ε we rearrange the equations above to

$$\varepsilon = \frac{\exp(C_2/\lambda T_2)-1}{\exp(C_2/\lambda T_1)-1} \qquad (3)$$

Scanning spectroscopy. We applied scanning spectrometry to measure the emission spectra of the plume between wavelengths (λ) of 400 nm and 900 nm. This was to determine how well the plume could be represented as a graybody radiator and to substantiate pyrometry measurements for temperature and emissivity.

The spectral radiance detected by our apparatus would be predicted by

$$L(\lambda, T) = \frac{\varepsilon C_1}{\lambda^5 r^2 (\exp(C_2 / \lambda T) - 1)} \tag{4}$$

where

r = distance from source to sensor (cm).

Using this equation we superimposed a best estimate of the spectral radiance vs. the spectral data to estimate temperature and emissivity. An analogous method that is used to estimate temperature is based on a log function of spectral radiance. The resulting linear equation can be written as

$$\ln(f(L)) = \frac{C_2}{T}\left(\frac{1}{\lambda}\right) \tag{5}$$

where

$$f(L) = \left(\frac{\varepsilon C_1}{L\lambda^5 r^2}\right) + 1 \tag{6}$$

The slope of the line represented by this equation is a function of temperature (T), while the intercept is a function of ε. In our analyses we estimated temperature by matching the slope of that line using a least squares fit.

EXPERIMENTAL

Test Design

Typical layouts of experiments are depicted in Fig. 1. In these tests a 2.5-cm-thick graphite plate was used as a base for the propellant. A chimney was placed over the

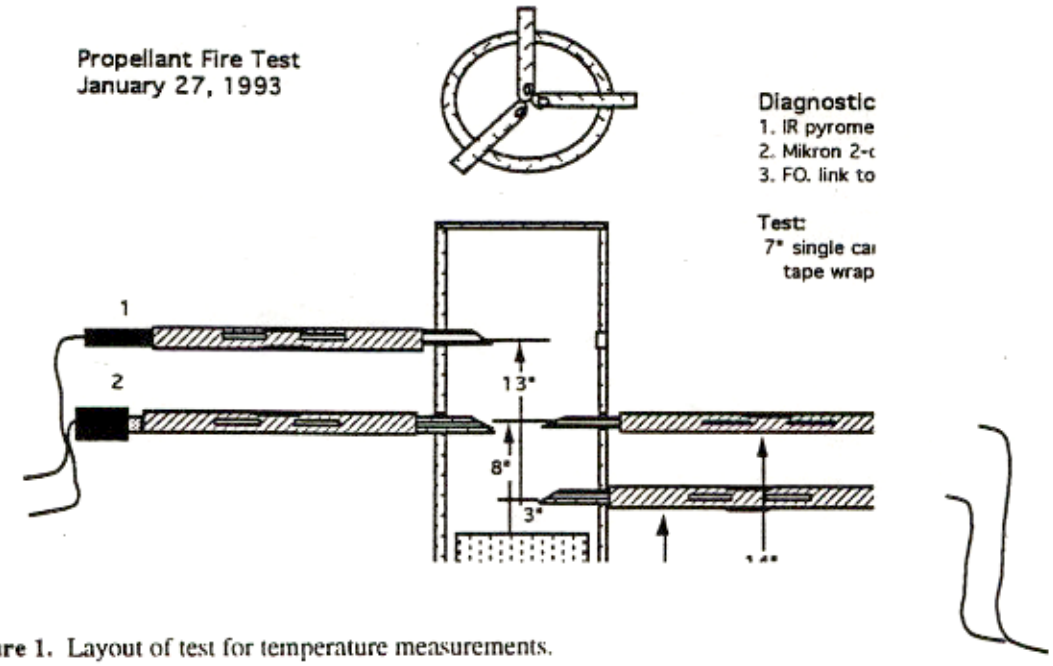


Figure 1. Layout of test for temperature measurements.

propellant and diagnostics were inserted through selected holes along the height of the chimney wall. Figure 1 shows a test layout designed to measure the temperature distribution and collect spectrometry data to compare with two-color pyrometry data.

Temperatures along the center line of the plume were observed by using graphite sight tubes. These were hollow tubes with one end cut at an angle. The sight tube was inserted into the plume with the slant cut facing upward (in the direction of flow of the plume). This device allowed detectors to view a small internal volume of plume. Spectrometric measurements were made through this means. These devices were coupled to the sensors by the use of alignment tubes. Figure 1 shows how sight tubes were used.

Temperature measurements

Tests were performed using combinations of diagnostics that would provide correlation and validation of each other's measurements. This was especially important because the measured variable (spectral radiance) is a function of both temperature and emissivity. To calibrate our spectrometry data, the spectrograph was deployed at our test site and aligned onto a portable blackbody source: the source was set at 1150°C (1423 K). Data was collected as in a test and was processed to determine an estimate of temperature and emissivity. The results matched the calibrated source temperature and estimated ε at 0.98.

Tests were conducted with instrumentation at standoffs ranging from 8 cm (3 in) to 135 cm (59 in). Pyrometry data was collected along with the spectrometry data in most tests. Spectral data was collected at many times during a burn. Very often the instrumentation was set at the same standoff as the pyrometers (see Fig. 1). We processed the spectrographic data using equation 5 and from the resulting line estimated temperature and emissivity. We then determined the validity of the estimate by calculating a graybody spectrum using the values just determined and plotting it with the measured radiance.

Several spectra were recorded during any one test. Figure 2 shows three spectra collected at a standoff of 8 cm in a 35 cm chimney. There is a temperature and emissivity value next to each spectrum that indicates the best estimate values for the corresponding spectrum. The temperature and emissivity written in bold refer to the values used to generate the "predicted" spectrum. Note for this figure that the analysis method used on the

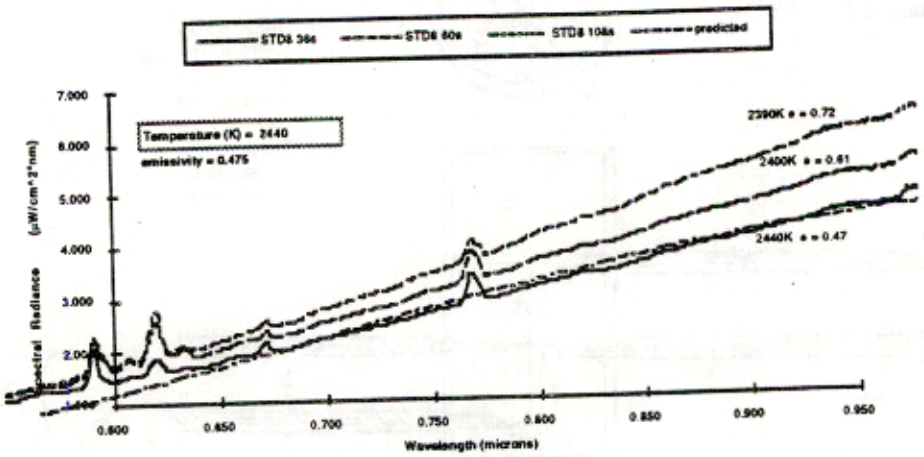


Figure 2. Spectra observed during a burn in a 35 cm chimney.

data was able to discriminate temperature variations of 50K. It was also clear that the analytical process provided a means of estimating temperature with relatively good resolution. Because the spectra were approximated rather well by the graybody radiation predicted by equation 4, we also had a high level of confidence in the results.

To validate results obtained through this process and to validate two-color pyrometry data, temperatures calculated as in Figure 2 were superimposed on temperature histories of the corresponding tests. This was done when the two-color pyrometer and the spectrograph were focused on the same volume-space in the plume. Figure 3 shows the results for one test in an 18 cm chimney. Clearly, there is room for improvement in the accuracy of the predictions, but the error is less than 60°C (approximately 3%). The level of uncertainty associated with the temperature data collected using a two-color pyrometer was reduced. In fact, this analysis allowed us to develop a high level of confidence on the pyrometry data.

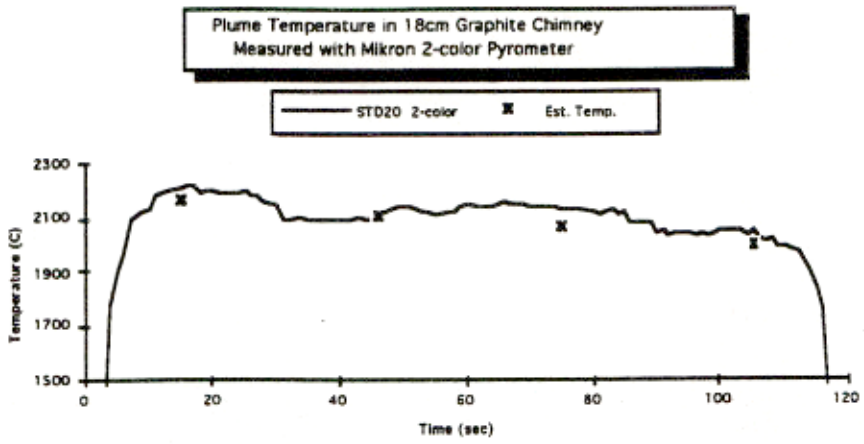


Figure 3. Temperatures estimated via spectrometry superimposed on pyrometry data.

Emissivity measurements

Early results of tests performed to determine plume emissivities had shown reasonable values near the propellant surface and extremely low values at high standoffs. It is known[3] that emissivity is a function of particulate size and concentration in the plume, and at a temperature above the melting point of alumina the emissivity of the plume is much higher than it is below the melting point. As the alumina condenses and solidifies into a "dry" powder, the emissivity of the plume would be expected to drop below 0.1. Such low emissivities pose a problem to pyrometers because of the low quantity of light that is received by the instrument.

We used two different approaches to determine an emissivity profile: (1) estimating emissivity from spectrographic data using equations 4 and 5; (2) ratio spectrometry. Figure 2 contains spectra that were collected in the 35 cm chimney and shows the resulting emissivity estimates. Ratio spectrometry data were collected by focusing the two-color pyrometer and the single-color pyrometer on the same volume-space of the plume.

Processing single and two-color pyrometry data using equation 3 led to results such as the emissivity data on Fig. 4. Figure 4 shows single and two-color pyrometry data collected at a 20 cm standoff and has superimposed the calculated emissivity as a function of time. In that test, the emissivity varied from approximately 0.03 to 0.05. These results verified the values of emissivity that were calculated from the spectrographic data. Test results of this

nature further strengthened our level of confidence in our results even for low values of emissivity.

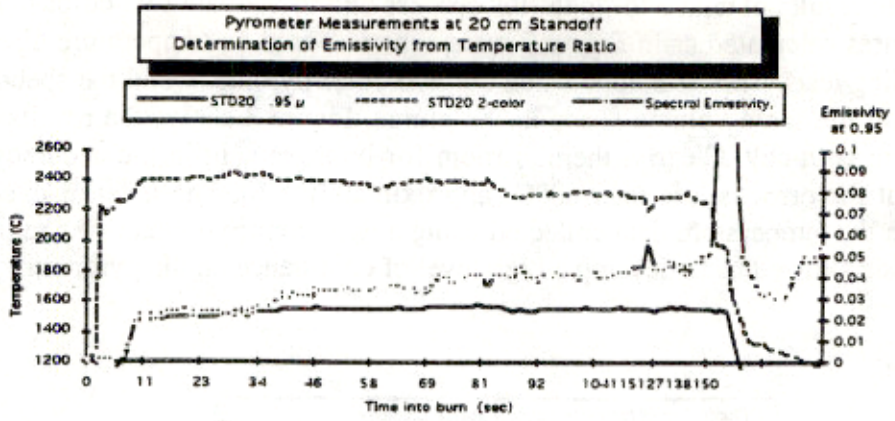


Figure 4. Time history for emissivity of propellant fire plume.

ACKNOWLEDGMENTS

The author would like to acknowledge the scientific contributions of Charles Honodel, Frank Helm, and Russ Sanborn. Among the many test site personnel who contributed to this study were Douglas Bakker, Frederick Sator, John Rubke, David White, John Elliott, and Vince Gase.

REFERENCES

1. W. Eckl and N. Eisenreich, *Determination of the Temperature in a Solid Propellant Flame by Analysis of Emission Spectra*, Propellants, Explosives, Pyrotechnics 17, 202-206 (1992).
2. R. B. Johnson, C. Feng, and J. Fehribach, *On the Validity and Techniques of Temperature Measurement and Emissivity Measurements*. SPIE, Thermosense X, Vol. 934, 202-206 (1988).
3. V. Calia, M. Celentino, et al., *Measurements of UV/VIS/LWIR Optical Properties of Al_2O_3 Particles*. Proceedings, 18th JANNAF Exhaust Plume Technology Meeting (1989).

PROBABILISTIC ESTIMATES OF HANFORD WASTE TANK FAILURE DUE TO HYDROGEN BURNS

R. Kenneth Deremer[1] and Donald R. MacFarlane[2]

[1]PLG, Inc.
4590 MacArthur Boulevard, Suite 400
Newport Beach, CA 92660-2027

[2]Los Alamos National Laboratory
Engineering and Safety Analysis Group, N6
P.O. Box 990, MS K557
Los Alamos, NM 87545

This paper discusses a probabilistic model for estimating the frequency of tank failure due to burns associated with the episodic release of combustible gases into the dome space of the Hanford waste tank designated 241-SY-101. This high-level waste tank is one of 177 such tanks, located in the 200W and 200E areas of the U.S. Department of Energy Hanford site, that contain high-level waste which has accumulated over 50 years of weapons material production. Given the potential for radiological exposure (both onsite and offsite) to the radiological contents of this tank as a result of such burns, it is important to estimate the frequency of various releases from the tank.

The frequency of tank failure resulting from hydrogen burns is determined by a probabilistic model that combines the frequency and magnitude of episodic hydrogen releases from the waste to the vapor space of the tank, the likelihood of ignition of this hydrogen, the overpressure resulting from ignition, and the ability of the tank to withstand this overpressure.

Tank 241-SY-101 is composed of three concentric structures: (1) an outer, reinforced concrete tank designed to sustain induced loads for soil, seismicity, and thermal gradients between the radioactive wastes and the outside soil; (2) a secondary carbon steel tank that lines the concrete tank and is designed to serve as a leak barrier; and (3) a freestanding carbon steel primary tank resting on an insulating concrete pad within the secondary tank. The tank contains a number of vertical risers extending from the tank dome to either a process pit or to a level above grade. The tank dome space and the annulus between the primary and secondary steel shells are actively ventilated through dedicated process pits. Inlet air to the dome space and annulus region comes from filtered intakes and leakage at the various penetrations. A probability characterization (based on limit state analyses) of

the pressure capacities of tank 241-SY-101 waste storage tank for various failure modes was performed by EQE Engineering Consultants.

Approximately every 100 days, Tank 241-SY-101 experiences a release of flammable (hydrogen) and oxidizer (nitrous oxide) gases from the waste into the dome space of the tank, producing concentrations approaching the lower flammability limit. A review of the releases indicates an overall trend in which the magnitude of such releases is increasing with time, although consecutive releases are cyclic in nature.

Recognizing the potential for future high concentrations of hydrogen in the tank dome space and ventilation system, and the availability of ignition sources, a probabilistic model was developed to estimate potential pressure loads within these systems, to compare these loads with the pressure capacities of the tank, and to determine the likelihood of tank failure. Except for static electricity and the potential for sparks caused by metal-to-metal contact, there are no other ignition sources in the vapor space or waste of Tank 241-SY-101. The more likely source of ignition of the episodic hydrogen releases is from instrumentation installed to monitor these releases and from sources associated with the ventilation system. Ignition sources in the ventilation ducting and burn propagation from the ducting back to the dome space were addressed. A probabilistic characterization of the likelihood of ignition of the hydrogen-laden mixture of gases released into the vapor space of the tank is extremely difficult. Mixtures of hydrogen are easily ignited, requiring only minimal sources of energy. The probability that an ignition occurring in the ventilation system can propagate back into the tank depends on the ventilation flow velocity relative to the burning velocity associated with the reacting gases.

Based on observed trends, the magnitude and frequency of gas releases to the dome space were estimated for the next 3 years.* The measured and predicted drops in waste level, which are correlated with the volume of gas released, are shown in Figure 1. With these projections and the actuarial database (since 1989) of release data, the probability distribution shown in Figure 2 was generated for the magnitude (volume) of the gas release. Probability distributions were also generated for the amount of hydrogen contained in these releases (based on Figure 3) and for the pressure loads for various quantities of hydrogen burned (based on Figure 4). Best estimate and conservative hydrogen concentrations and pressure load predictions were calculated with the HMS and TRAC computer programs.

The quantification of the frequency of tank failure due to combustion events was accomplished with the STADIC program, which uses Monte Carlo sampling techniques to combine input probability distributions of various types to generate output distributions according to a prescribed algorithm. A flow chart for this algorithm is shown in Figure 5. As indicated, the first step in the algorithm is to sample the cumulative probability distribution for the volume of gas released. The next step in the algorithm is to assess the probability of ignition. Assuming that the gas mixture ignites for the sampled volume, the pressure rise distribution corresponding to this volume is sampled, (based on interpolation). The probability distribution for tank strength is then sampled and the peak tank pressure is compared to the sampled strength. If the pressure load exceeds the tank strength, the trial is assumed to result in tank failure. If the sampled strength exceeds the sampled load, the trial does not result in tank failure. This process is repeated thousands of times to provide statistically meaningful results for the conditional frequency of a tank failure, given an episodic release of gas from the waste.

---

*The projected releases do not include the effect of a recirculation pump that has been recently installed in the tank. It is believed that operation of this mixing pump will tend to release gas from the waste continuously rather than periodically.

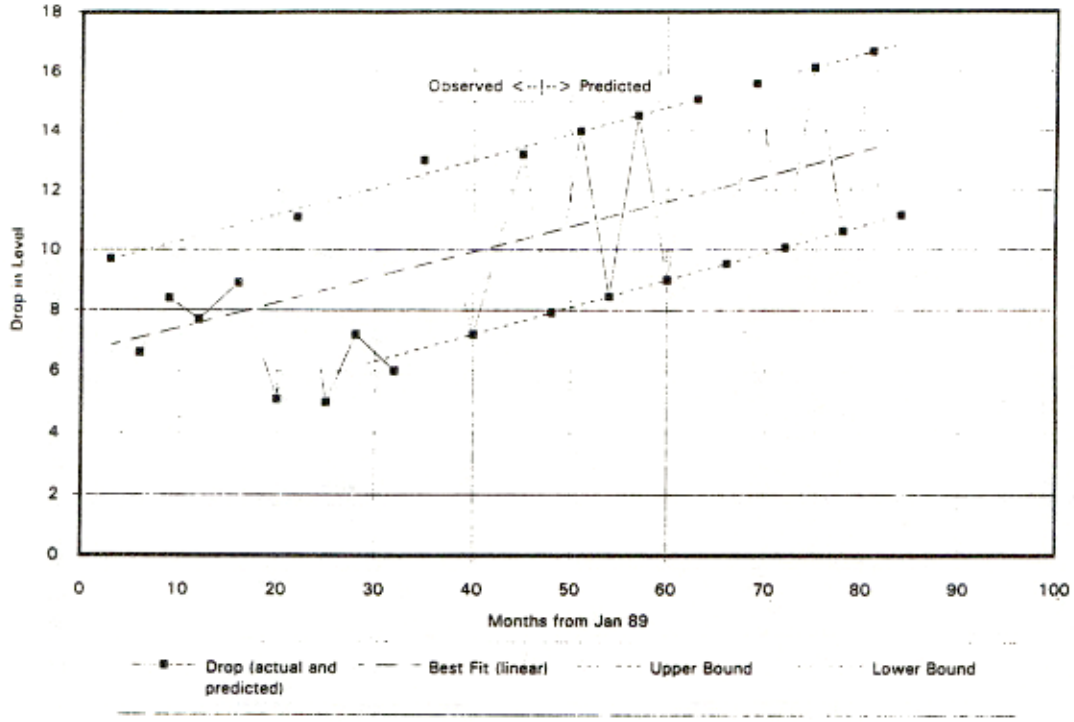


Figure 1. Observed and predicted drops in waste level.

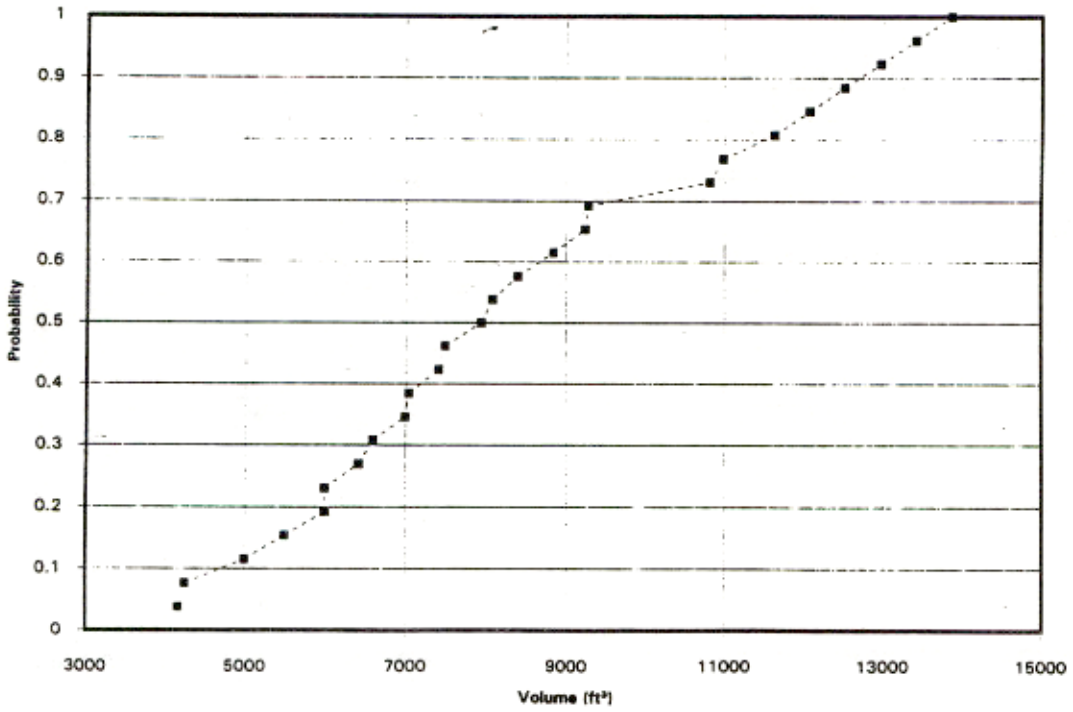


Figure 2. Cumulative probability distribution for volume of gas released (based on observed drops since March 1989 and extrapolated for the next 3 years).

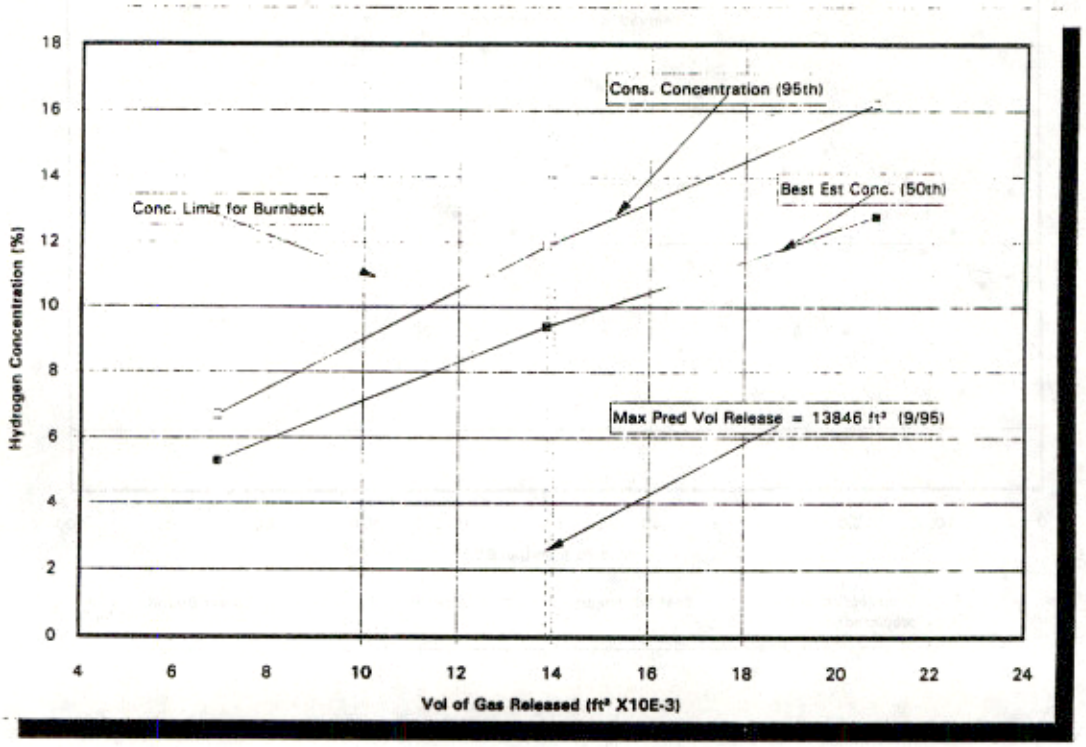


Figure 3. Hydrogen concentration versus volume of gas released.

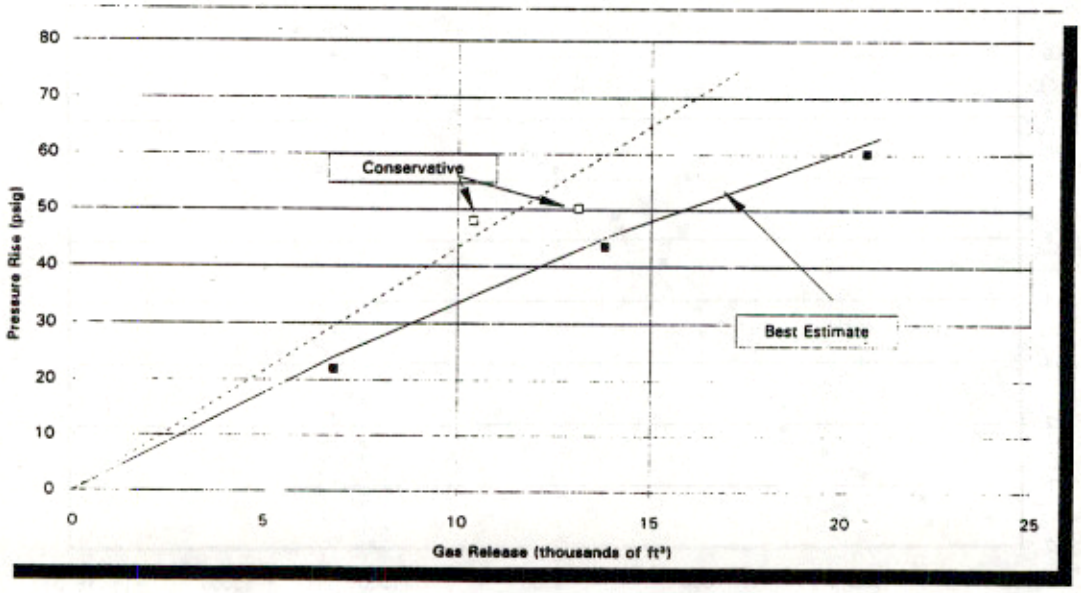


Figure 4. Pressure rise due to hydrogen burn.

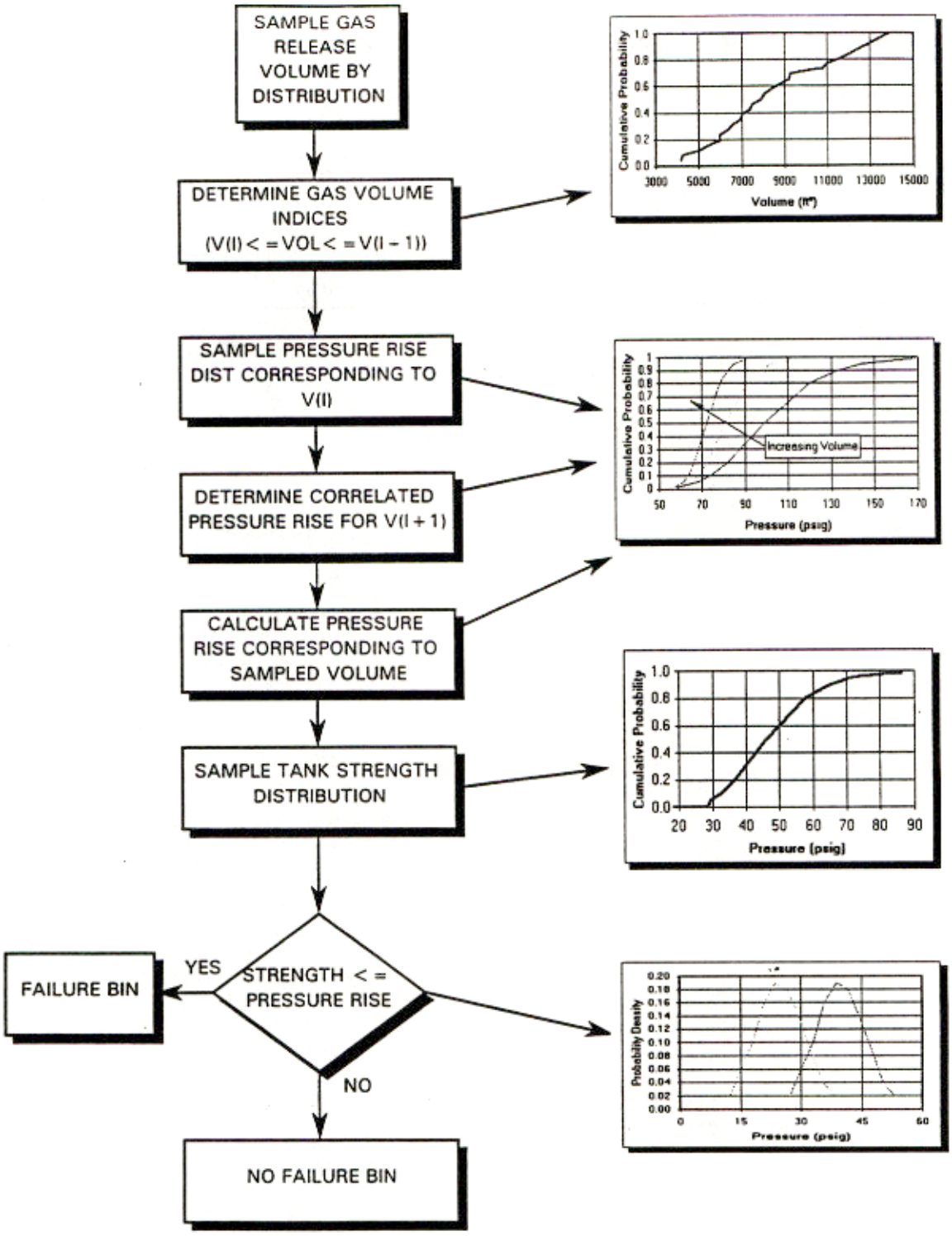


Figure 5. Stadic algorithm for tank 101-SY failure.

The following three cases were analyzed with the model described above:

1. Actuarial data for all significant waste level drops/gas releases that have been observed since January 1984.
2. Actuarial data since March 1989 and estimated level drops/gas releases for the next 3 years.
3. Gas release of 13,100 ft^3 ["maximum allowable burp" (MAB)].

The STADIC evaluation of these three cases is summarized in Table 1. Case 2 is of particular interest and indicates that for any burn, the conditional probability of tank failure is 0.12. If only actuarial data (Case 1) are used in this evaluation, the conditional probability of tank failure is reduced by than order of magnitude to 0.014.

Table 1. Results of STADIC analyses for tank failure frequency.

Case	Conditional Frequency of Tank Failure
1	0.014
2	0.12
3	0.37

007 Quantitative Risk Assessment and Process Industry Decision Making

Chair: I.A. Papazoglou, Inst. Nucl. Technol. & Radiat. Protec.

The Use of Quantitative Risk Assessment as a Decision Making Tool
G.N. Pettitt, B. Harvey, D.R.E Worthington (DNV Technica)

THE USE OF QUANTITATIVE RISK ASSESSMENT AS A DECISION MAKING TOOL

Dr G.N. Pettitt

DNV Technica, Ltd,
Palace House, 3 Cathedral Street,
London SE1 9DE

Mr B. Harvey
Dr D.R.E. Worthington

DNV Technica Inc,
40925 County Center Drive,
Temecula, CA 92591

ABSTRACT

Quantitative risk assessment (QRA) is a tool that was used initially in countries to assist land-use planning and to determine whether a process or industrial complex meets certain risk criteria. However, it has developed into a more powerful tool for making decisions on different process or mitigation options for equipment items, processes or whole complexes. QRA will show the options that are economically justified and those which are not. QRAs will be used increasingly in a cost-benefit mode to evaluate these different options.

INTRODUCTION

What is the use in performing a Quantitative Risk Assessment (QRA)? This question is often asked in the chemical, petrochemical and petroleum industries in the United States and around the world. In many countries the obvious answer was because it is a requirement set by the Government. Companies must be within certain risk criteria and a QRA will establish whether these criteria are met. However, even this role is changing dramatically as national criteria switch from a pass/fail mode to an ALARP mode (A Low As Reasonably Practicable). QRAs are thus used to select between different mitigation alternatives where the test is 'gross disproportion' in cost vs. the benefits.

In the United States risk criteria are not legislated, while the application of consequence modeling is. Consequence modeling gives hazard zones. Different events could give equivalent zones. QRA provides a tool by which the significance of the hazard zones can be put in perspective. QRA tells you which events are dominant and, thus, it can be used as a decision-making tool and often save financial resources.

A QRA may show that a capital expenditure on extensive risk-mitigating projects is not justified and that a smaller investment in another less expensive, but possibly more effective measure is more appropriate. This decision is obviously cheaper and more effective. A tougher decision would have to be made if the alternative was cheaper and less effective. A proportionally small investment in undertaking a QRA may prove to have a substantial return if it shows that a capital mitigation project would be a disproportionately large investment.

Many QRA studies have provided management with a tangible basis for making both planning and engineering decisions. Otherwise, some of these economically significant decisions may only have been made on a 'gut feeling' basis.

WHAT IS QRA ?

The underlying basis of risk analysis is simple in concept. It offers methods to answer the following four questions:

- What can go wrong?
- What are the causes?
- What are the consequences and impacts?
- How likely is it?

The combination of the answers to these four questions defines the risk and the potential for risk reduction based on preventive and mitigative measures.

Figure 1 is a simple flow diagram that illustrates one version of the procedures for conducting a QRA. After defining the goals of the QRA and the system to be studied, the next step is the identification of potential failures that could result in the release of a hazardous material from its normal containment state. This may be achieved using several techniques, such as 'generic' failures, HAZOP studies, What-If studies, previous experience, etc. After identification of a particular failure case, the various factors that affect risk are introduced in a logical fashion. Factors which directly affect risk are:

- the likelihood of a particular failure occurring;
- the release conditions (source terms);
- the behavior of the material upon release (consequences);
- the probability of the meteorological conditions causing the release to drift in a particular direction;
- in the case of a flammable material, the probability of a release being ignited;
- in the case of a toxic material, the toxicity;
- the proximity of the local population; and
- the extent of protection provided by in-place sheltering.

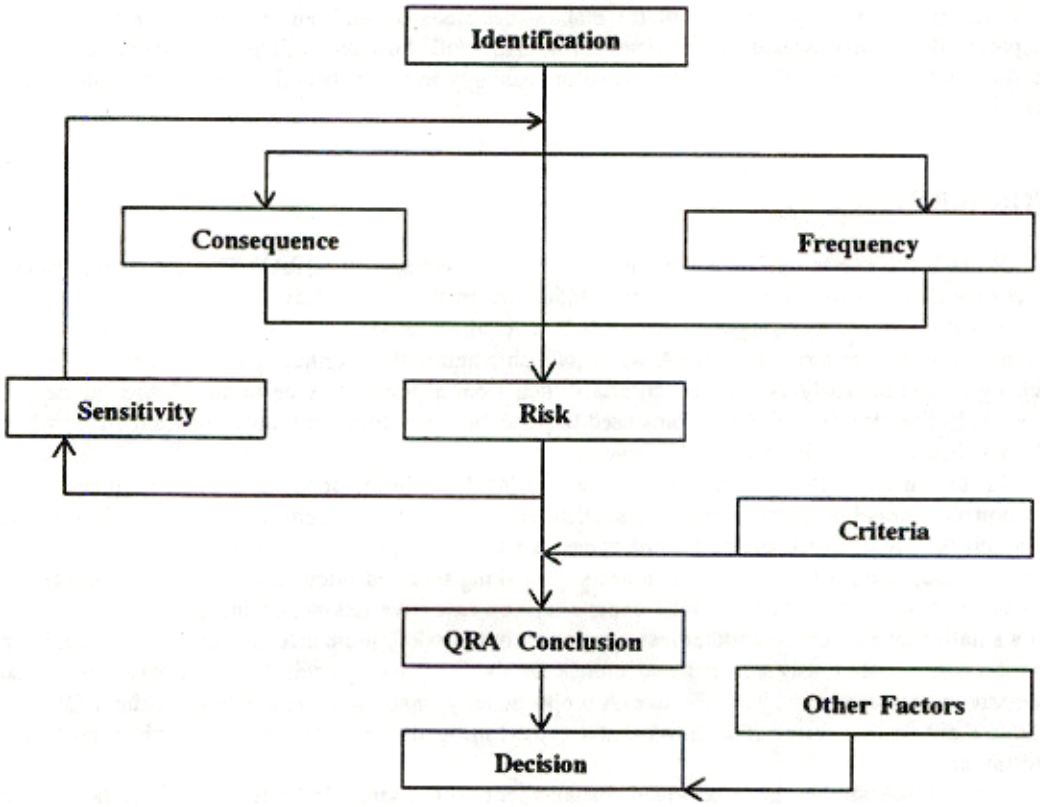


Figure 1 - QRA Framework

Typically, QRA studies will assess the impact of major accidents on people, with results expressed as risks to on-site and off-site individuals (individual risk), or to population groups or society as a whole (societal risk). The risk considered may be the risk of fatalities, major injuries, minor injuries, or all of these. The UK Institution of Chemical Engineers[1] defines individual risk as *"The frequency at which an individual may be*

expected to sustain a given level of harm from the realization of specified hazards". They define societal risk as "*The relationship between frequency and the number of people suffering from a specified level of harm in a given population from the realization of specified hazards*"

Individual and societal risk may be supplemented by risks of financial losses arising from accidents (financial risk). Financial risk may include material damage to plant or off-site property, indirect production losses due to shutdown periods for repairs, losses resulting from damage to a company's image and the financial consequences of legal proceedings.

QUALITY AND QRA

Over time QRA is becoming better established as a proper engineering procedure. Uncertainties are better understood, models are more accurate and data is more freely available. The application of quality management procedures is making the technique more consistent and dependable. ISO 9000 and Total Quality Management are both applied to studies. In the US, the CCPS has issued guidelines for risk analysis. In the UK there is a draft British Standard.

In DNV Technica, a major program, reflecting an investment of $750,000, has produced: a Consultancy Policy, Guidelines and Technical Notes and a Procedure for Deviations. The largest part, the creation of Guidelines and Technical Notes, has produced twenty-one such documents. While flexibility is retained to meet clients needs, a greater degree of consistency and quality should result. Unwanted variability should be eliminated and agreed deviations will be documented properly.

RISK CRITERIA

Many countries have developed their own risk criteria. Some have set standards for individual risk, societal risk or both. Hence, companies within the UK, the Netherlands, Hong Kong and Australia, among others, must meet these criteria and, therefore, are subject to performing a QRA. In the United States (and other countries such as Canada, Germany and France), no criteria has been set for acute risk and so a QRA is not mandated. In the United States, the main criteria now is for a Process Hazards Analysis (PHA) to be performed as outlined in OSHA 29 CFR 1910.119. However, some companies have developed their own internal risk criteria that have encompassed both individual and societal risk, and they perform QRAs to meet these criteria.

Many companies are under the misconception that QRA is only useful if they have to adhere to certain criteria. However, QRAs can save man-hours and often large investments if utilized to determine the effectiveness of proposed mitigation measures that may or may not reduce the risk from a facility.

From an accident prevention standpoint, most accidents are preventable given perfect hindsight. QRA helps turn this hindsight into foresight. Once management knows what could happen and how likely it is, they are in a better position to develop the optimum safety approach (better procedures, engineering and supervision). Given foresight, they can prevent accidents from happening.

QUANTIFYING RISK REDUCTION USING QRA

A QRA will determine the risk from a facility now. This is often known as the base case. For this task, a full set of potential incidents is defined and the risk from these is determined by counting their frequency of occurrence and their potential consequences. By summing the risks of each incident, the overall risk may be determined. This is the so-called absolute risk result. Given the potential error in data and models, this has a relatively large uncertainty band. A more robust use of the QRA result is the so-called relative mode based on risk comparisons. It is often useful to rank the incident cases. This will show where the majority of risk is originating. This will also help indicate which pieces of equipment should be considered for risk reduction measures.

After determining which equipment items are high contributors to the overall risk, the methods by which the risks can be mitigated most effectively can be investigated. Some mitigation options will be investigated to reduce the probability of a release, while others will reduce the release consequences or possibly both. Often, there are many different mitigation options available, some of which will appear to have a similar effect in reducing risk when investigated qualitatively. For each mitigation measure considered, it is determined how each particular release case defined will be mitigated and the appropriate changes are made to the release case

inputs. The risk is then recalculated and the actual risk reduction can be quantified. The risk reduction may be quantified in terms of the reduction in statistical fatalities, the reduction in serious injuries, or whatever measure is desired.

If the cost of each mitigation measure is applied, the effectiveness of each measure may then be determined. This may be simply achieved by a ratio of the total cost of the measure (capital and operating costs) over the reduction in risk. This is often known as a cost-benefit analysis (CBA). Another more complex method of analyzing the effectiveness of a mitigation option is by use of the following equation[2]:

$$\textit{cost per statistical fatality or injury averted} = \frac{\textit{cost of option - reduction in expected economic loss}}{\textit{statistical fatalities or injuries averted}} \quad (1)$$

The calculation is performed on the basis of a specified period, usually one year. Therefore, an amortization period for the cost of an option must be used, i.e., if a mitigation measure is assumed to be in place for ten years, then the cost of the measure must be divided by ten to determine the yearly cost.

The reduction in expected economic losses is determined by first calculating the yearly financial loss for the base case and then subtracting the yearly financial loss for the mitigated case. If the calculated reduction in expected economic losses is greater than the cost of the option, then the mitigation measure is deemed cost-beneficial, whatever the calculated statistical fatalities or injuries averted. For cases where the cost of the option is greater than the reduction in expected economic losses, a cost per statistical fatality or injury averted will be obtained. At the outset of a project, a decision should be made on a value above which a mitigation option will be deemed grossly disproportional.

In some countries a cost-benefit analysis is a requirement. For these countries, if it is determined that the risks are below an intolerable level, but above a negligible level (the levels set by the governing body), a cost-benefit analysis must be performed to determine which risk reducing measures are reasonable and cost-effective. This will demonstrate that they have been reduced to As Low As Reasonably Practicable (ALARP). For countries that do not have specified risk criteria, the cost-benefit analysis technique using QRA is still appropriate and is a very useful, but under-used, tool for decision making.

One important aspect that may need to be taken into consideration when investigating risk reduction from different options is the portrayal of the company's image in the local community and beyond. It may be decided in the course of a study that particular mitigation measures are not cost-beneficial. In most circumstances, such measures would not be installed. However, if certain mitigation options have received much attention from public bodies (such as water sprays for HF mitigation), then it may be deemed a good public-relations exercise to have these options installed. The benefits may be realized in other ways, in that the public image of the company is improved and that the company is associated with public safety. Conversely, if a company develops a bad public image, this may have a significant adverse effect, particularly if there is a boycott of the company's products.

EXAMPLE 1, HF ALKYLATION

DNV Technica has worked with several multi-national petroleum and chemical companies in helping them to determine how to reduce the risk from a unit most effectively with respect to cost. Much of this work has been in the area of HF alkylation. Recently, much emphasis has been put on the risks associated with an accidental release of HF acid into the atmosphere. The emphasis had in some part been engendered by the so-called 'Goldfish' trials[3], in which hydrogen fluoride release experiments were performed at the Nevada Desert test site, and the release of such articles entitled 'American Bhopals'[4] and 'The Most Dangerous Chemical In Town'[5]. Many companies who employ HF acid as a catalyst in their alkylation units have expressed some concern. For these companies, the risk from the HF alkylation unit was quantified and the major risk contributors established. A list of potential mitigation measures was then drawn up and the risk reduction from each measure quantified. (Many of these mitigation options were suggested in API RP 751[6]).

Some of the results were surprising. In some cases, the measures that were most effective in reducing risk were more simple changes that would not require a large capital expense, e.g., isolation. Conversely, it was found that some measures that would require an extensive capital project were not particularly effective in reducing the risk, e.g., dump tank, water sprays. Hence, savings that totaled millions of dollars were made in some cases where previously budgeted mitigation designs were not implemented (and more cost effective alternatives utilized) as a result of the QRA study.

One interesting aspect of conducting parallel studies of different HF alkylation units is that the same

mitigation option may be deemed cost-beneficial for one unit, but not cost-beneficial for another. The results are site-specific and dependent on, for example, the capacity of the unit, local meteorological data, proximity of the population, standard of housing, etc. The results may be different depending upon what population groups are considered in the study, i.e., off-site population, on-site workers, or both. This would suggest that overly simplistic studies which do not consider the totality of the problem may give misleading results.

EXAMPLE 2, HYPOTHETICAL CHLORINE UTILITY

Suppose we are interested in reducing the risk from a Chlorine storage and transfer utility. 40,000 kg of Chlorine is stored pressurized at ambient temperature, and is transported via a liquid line. For simplicity, five base case incidents were modeled:

1. A catastrophic rupture of the Tank ($1x10^{-6}$ per year)
2. A liquid release from a 25mm hole at the bottom of the tank, representing the range of possible liquid release scenarios ($1x10^{-5}$ per year)
3. A vapor release from a 25mm hole on top of the tank, representing the range of possible vapor release scenarios ($1x10^{-5}$ per year)
4. A vapor release due to operation of the relief valve on top of the tank ($1x10^{-4}$ per year)
5. A 12mm leak from the liquid transfer line, representing the range of possible release scenarios from the transfer line ($1x10^{-3}$ per year)

Figure 2 shows risk contours predicted by DNV Technica's SAFETI*Micro* program. Even with a simple system, possible mitigation measures can be investigated. Since the liquid transfer line is seen to be the major contributor to risk, it was decided to use a vacuum vapor transfer line. The risk results for this case show a remarkable decrease in overall risk from the utility. Figure 3 shows the F-N curve for the two cases and Figure 4 illustrates the dramatic overall reduction in risk. This is clearly a mitigation measure to be considered. Not all studies have such clear-cut conclusions, but this example serves to highlight the power of the technique.

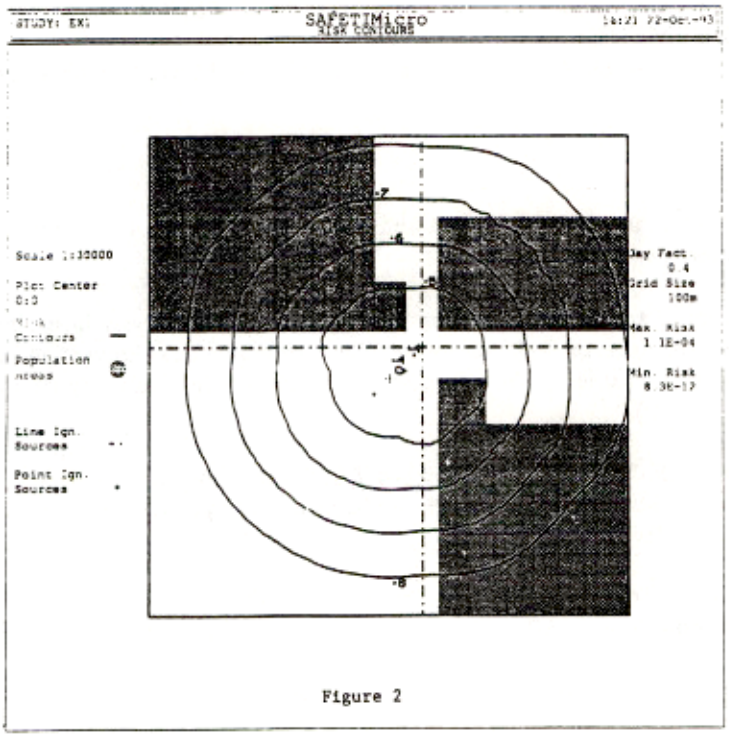


Figure 2

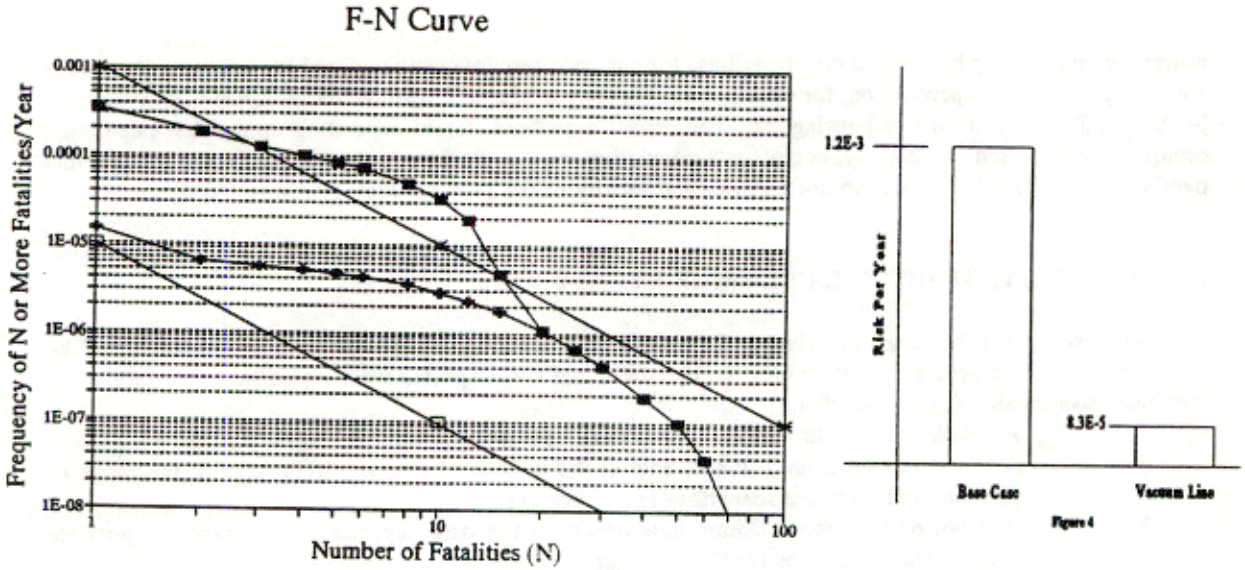


Figure 3

Figure 4

CONCLUSION

It can be seen that QRA can be a very useful tool in decision making. Companies who are considering capital projects for mitigation should consider using QRA before making any decision. The QRA will help to show which mitigation measures are most effective with regards to reducing the level of overall risk and hence show where the money is best spent. The QRA may show that it is unnecessary and unjustified to put a large amount of effort into a capital project that may not be particularly effective in reducing the risk.

This technique is applicable from small to large scales. It can apply to certain pieces of equipment alone, where the analysis may be performed by hand calculations or simple computer models. On a larger scale, it can be applied to parts of or a complete process or unit. On a very large scale, this technique may be applied to a complete chemical or petroleum facility. For the larger scale projects, use of comprehensive computer models is recommended, such as DNV Technica's SAFETI[7] program (Software for the Assessment of Flammable, Explosive and Toxic Impacts).

ACKNOWLEDGEMENT

The contribution of Dr Robin Pitblado and Mr Philip M. Myers towards this paper is acknowledged by the authors.

REFERENCES

1. IChemE, "Nomenclature for Hazard and Risk Assessment in the Process Industries", 2nd Edition, D. Jones, ed., Rugby (1992).

2. A.B. Fleishman and M.S. Hogh, The use of cost benefit analysis in evaluating the acceptability of industrial risks, *in*: "6th International Symposium on Loss Prevention and Safety Promotion in the Process Industries", The European Federation of Chemical Engineering, Moberg & Helli A/S, Oslo (1989).

3. D.N. Blewitt, J.F. John, R.P. Koopman and T.C. Brown, Conduct of Anhydrous Hydrofluoric Acid Spill Experiments, *in*: "International Conference on Vapor Cloud Modelling", J.L. Woodward, ed., AIChE, New York (1987).

4. N. Livingstone, "American Bhopals, The Threat of Catastrophic Refinery Accidents and Sabotage to Hydrofluoric Acid Alkylation Units", The Energy Safety Council, Lincolnshire, Illinois (1991).

5. B. Selcraig, The Most Dangerous Chemical in Town, *in*: "Audubon", Nov-Dec (1992).

6. API RP 751, "Safe Operation of Hydrofluoric Acid Alkylation Units" API, Washington D.C. (1992).

7. Software for Assessment of Flammable, Explosive and Toxic Impact (SAFETI), Technica Ltd, London, UK

008 Choosing Among Alternative Programs or Strategies

Chair: H.F. Martz, LANL

Integrated Regional Risk Assessment and Safety Management: The Experience of Switzerland

A.V. Gheorghe (ETH, Switzerland)

WESVA: A Decision Aid for Comparing Warhead Advanced Surety R&D Options

R.V. Homsy, A. Sicherman, D.R. Stephens (LLNL)

INTEGRATED REGIONAL RISK ASSESSMENT AND SAFETY MANAGEMENT: THE EXPERIENCE OF SWITZERLAND

Adrian V. Gheorghe

Swiss Federal Technological Institute - ETH
Polyproject "Risk and Safety Technological Systems"
ETH-Zentrum, 8092- Zurich
Switzerland

PPR & S : A SWISS INTERDISCIPLINARY PROJECT ON " RISK AND SAFETY OF TECHNOLOGICAL SYSTEMS "

The main goal of the ETH - Polyproject on "Risk and Safety of Technological Systems" (PPS&S) is the discursive description of knowledge in addition to the development of interdisciplinary and practical methods for the application of risk analysis, risk evaluation and risk management of a large variety of technological systems (e.g. transportation of dangerous goods, chemical engineering, landfills, nuclear power plants, biotechnologies, railroads, etc.). The scope of these applications is intended to be an integrated regional risk assesssment and safety management guideline manual and specialized computer software, databases and a novel methodological framework with due regard to the existing conditions of Switzerland. Associated with this main goal, there are the following secondary goals of the PPR&S, namely (see /4/ , /6/):

i) encouraging and promoting multidisciplinary work among the different departments and institutes at the ETH - Swiss Federal Institute of Technology;
ii) furthering the technical competence of the ETH in the field of risk and safety of technological systems including their relationship with natural disasters;
iii) furthering the scientific and academic contacts to other polytechnic institutes, universities, government departments, political institutes and industrial companies within Switzerland as well as internationally;
iv) supporting the teaching aims in the interdisciplinary field of risk analysis at ETH in Zurich.

ETH-Zurich has plans that, together with ETH-Lausanne, to develop a comprehensive post-graduate study program in the field of "Risk and Safety". For the most part the PPR&S has developed from a local / national interest in disasters prevention and emergency planning preparation. The work it concentrates mainly on the followings:

i) Technical Risks : not all types of technical risks can be handled in detail within the present frame of the Polyproject (see Figure 1). Whereas representative, technical systems (such as chemical or biotechnological industrial facilities) would be investigated in some detail although much of the effort in the project is given toward developing methodological tools, analytical models, databases that are, in principle, applicable to investigating all kind of risks (e.g. environemntal, health, economic, social). It is considered that these "tools" are

fundamental to understanding technical risks which, in turn, are part of integrated regional risk assessment and safety management / planning, but are not, in of themselves, the subject of research in this project. The same is true for risk from natural events. Regional risk managemeent / planning must be capable of handling properly both- technical and natural-risks (hazards). towards this goal, the PPR&S works together with EAWAG (Swiss Federal Department of Water Economy), whose official mandate is to co-ordinate the integration of natural hazards into the space planning; the Polyproject has additional contacts to other federal projects which work in the area of natural risks.

ii) Accidental Risks : "creeping risks" are more important than technical risks; they are not the research subject in the Polyproject. However, when dealing with regional safety management / planning, such risks must be considered, at least as pre-existing risk burdens.

iii) Regional Safety Management / Planning : the focus on a regional risk assessment and safety analysis and management is the main concern and one of the definitory characteristic of the PPR&S. It is recognized here that until now, the scope of questions of technological systems safety were mostly limited to single facilities (e.g. a storage or a chemical plant, a nuclear power plant, etc.), single risk sources (e.g. natural hazards such as avalanches, land slides, etc.), or, at most, whole technologies.

According to the recent experience in the PPR&S, the integrated regional risk assessment and management requires a fundamentally new different treatment of concepts of risk and safety:

i) it must portray and analyze the complete risk situation from normal operation, industrial hazards as well as natural disasters which might occur in a region. Different types of risks must be made comparable and mutual, reciprocal actions must be considered;

ii) risk evaluation must take into consideration the entire regional complexities, including the institutional framework, legislation, public acceptance and participation in solving practical problems related to risk management (e.g. selection for a new landfill site in the area study);

iii) risk assessment and safety management on a regional level must, not only include operational measures at the plant level, but also enable emergency planning to be agreed by different organizations and further implemented in case of hazardous situations occured. A regional risk-safety management approach must set up priorities at the level of the area study (e.g. cantons, towns, communes, industrial sites), and consider further how to optimize the resources, action plans, etc. for minimizing health and environmental impacts (risks) due to hazardous events as well as from continuous emissions in a given region.

The PPR&S is focusing on developing of a proper "model" for integrated regional risk assessement and safety management, with due regard to Swiss conditions. Parallel to this theoretical work, a real area study / region has been selected for investigation and analysis. The region consists of the eastern part on Canton Aargau and the western part of Canton Zurich. The model study is intended to validate the practical implementation of the research results. This work is being undertaken by the Swiss Federal Institute of Technology and other relevant research bodies (e.g. PSI-Paul Scherrer Institute), in close co-operation with cantonal officials and industry representatives.

INTEGRATED REGIONAL RISK ASSESSMENT AND SAFETY MANAGEMENT

Managing the hazards of modern technological systems has become a key activity in highly industrialized countries. Decision makers are often confrunted with complex issues concerning economic and social development, industrialization and associated infrastructure needs, and population and land use planning. Such issues have to be addressed in such a way that ensures that public health will not be endagered by continuous or accidental emissions and that ecological systems will not be disrupted or substantially degraded.

While hazard managers and risk assessors have been succcessful at identifying hazards and reducing overall risk exposure, economic growth and technological development have led to a new risk situation characterized by:

- an increasing number and variety of hazards;
- hazards giving rise to a broad range of spacial and temporal risks;
- public dissatisfaction with hazard managers and hazard "owners".

Due to increasing complexity of technological systems, the higher geographical density of hazard sources, a new mix and greater density of hazards are posing a new challange for hazard managers (see /8/). Risks from these new complex technological systems are inherently different from those addressed by the hazard managers of the 1960's and 70's. Recent worldwide dissatisfaction and outrage among the public by at large (including individual citizens, special interest groups), has produced difficult problems for hazard managers. On the one hand, it is increasingly difficult to site new facilities which are persived as risky or undesirable. On the other hand, the loss of trust is so problematic that at times, hazards managers are not considered reliable sources for risk protection information. In short, it is no longer clear what the public wants managers to do. It is needed a supplement to existing hazard management techniques that is integrative at a regional level.

The new key concepts which characterize the practice of integrated regional risk assessment and safety management are: inclusive, synergetic, and co-operative.

Remark 1 : Integrated regional risk assessment and safety / hazard management (IRRASM) represents a co-ordinated strategy for risk reduction and safety / hazard management in a spatially-defined region across a broad range of hazard sources (normal operation and accidental situations) that includes synergistic effects.

Remark 2 : IRRASM is a multi-disciplinary process; engineers and computer scientists play central roles in the risk assessment stage. Social scientists can contribute practice advice on how the embeddedness of the hazard sources in the organization, local economic conditions, political reality; they can make important contributions toward understanding how the practice of regional hazard management can meet the needs and expectations of society / community. It integrates more easily other kinds of regional planning functions (e.g. waste disposal, infrastructure, zoning, emergency preparedness, etc.).

The present Guideline Manual developed by PPR&S is addressed to systems engineers and decision makers working for risk problems at regional level and are intended to help regional risk assesment and safety management specialists (see /7/):

- identify existing hazards of technological systems within an area study;
- identify some of the criteria needed to evaluate the risks from these hazards;
- assess and evaluate the risks posed by these hazards;
- co-ordinate hazard management activities with land use planning;
- suggest regulatory mechanisms to reduce risks and eliminate hazards;
- design accident prevention schemes and emergency response plans.

A hazard may pose several different kinds of risk to different risk targets : people (threats to their health), things people value, which includes tangible and non-tangible items; environment (animals, plants, ecological systems). Economic resources can also be at risk. Shared or collective valuations have to be reached in a responsible and legal way. Hazards associated with the technological systems in a given region are divided as:

i) those which realize harm or damage through accidents (attributed to technological failure, human errors, natural interventions, etc.);
ii) those which realize damage or harm through continuous emissions to air, water, and land.

The scope of analysis is limited to the risks that explicitely do *not* include: routine occupational risk, consumer risk (through product consumption); voluntary risk; risk from natural hazards (except when they trigger or confound a hazard event of a technological system).

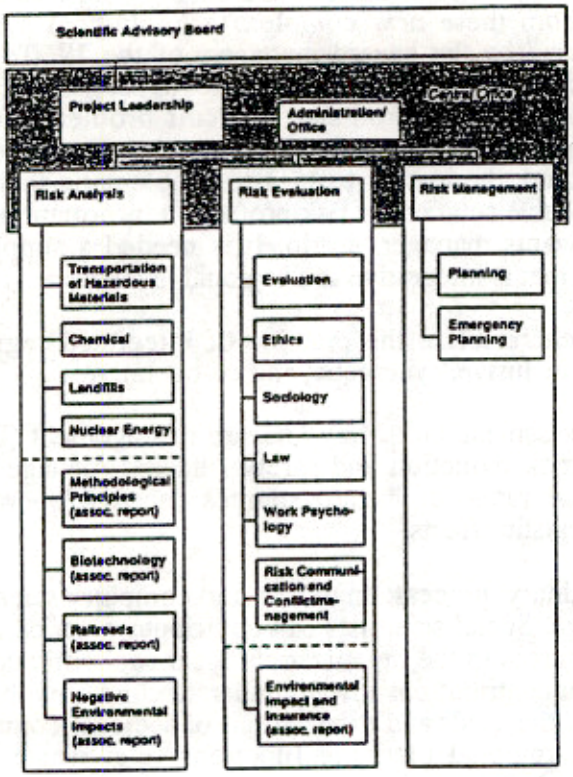


Figure 1. Organizational diagram

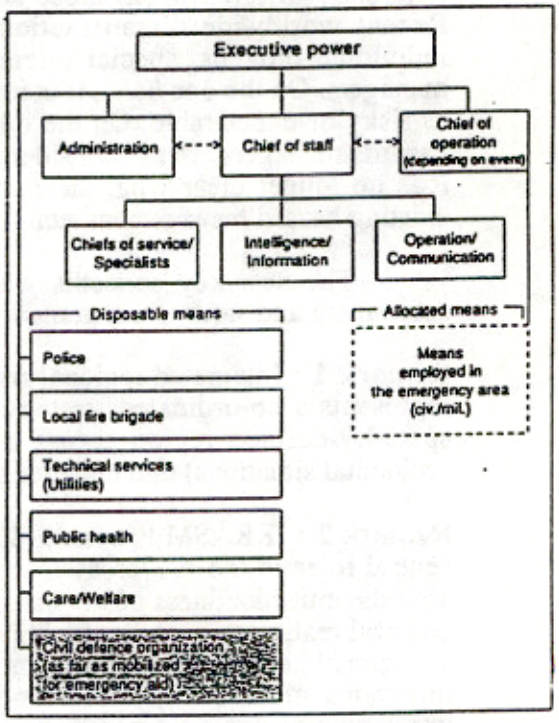


Figure 3. Community management

DISASTER	RESPONSABILITY		INSTITUTIONAL FRAMEWORK (PREPAREDNESS) AT THE FEDERAL LEVEL
	PRIMARY	SECONDARY	
AVALANCHES GLACIER BREAKDOWN	MUNICIPAL	CANTONAL	SWISS FEDERAL INSTITUTE FOR FOREST, SNOW AND LANDSCAPE RESEARCH
DROUGHT	MUNICIPAL	CANTONAL	NATIONAL HYDROLOGICAL AND GEOLOGICAL SURVEY
EARTHQUAKES	MUNICIPAL	CANTONAL	SWISS SEISMOLOGICAL SERVICE
EPIDEMICS/EPIZOOTY	CANTONAL	FEDERAL	PUBLIC HEALTH FEDERAL OFFICE FEDERAL VETERINARY OFFICE
FLOODS, STORMS HAILSTORMS	MUNICIPAL	CANTONAL	FEDERAL OFFICE FOR WATER MANAGMENT NATIONAL HYDROLOGICAL AND GEOLOGICAL SURVEY
FORESTFIRES	MUNICIPAL	CANTONAL	
LANDSLIDES	MUNICIPAL	CANTONAL	NATIONAL HYDROLOGICAL AND GEOLOGICAL SURVEY
	TECHNOLOGICAL DISASTER		
CHEMICALS ACCIDENT	MUNICIPAL ENTERPRISE	CANTONAL	NATIONAL ALARM CENTER
RADIOACTIVITY	FEDERAL	CANTONAL	DIRECTING COMMITTEE FOR RADIOACTIVITY
DAM RUPTURE	OWNER / CANTONAL	FEDERAL	FEDERAL OFFICE FOR WATER MANAGMENT

Figure 2. Institutional responsability

NATURAL DISASTERS AND RISK PREVENTION FOR TECHNOLOGICAL SYSTEMS: SPECIFICITY OF SWITZERLAND

Switzerland is a federal country where 26 cantons are sovereign in principle: the central authority only has jurisdiction in those areas determined by the federal Constitution and all other state powers automatically belong to the cantons or to the communes. Many of the regional government functions are delegated to the communes. Disaster prevention and management follow the same rules. Radioactivity and epidemics are the only disasters under the direct responsability of the Swiss Government. All other events are under the authority of the cantons or the communes. The Civil Defence provides assistance in co-operation with assigned operational services in natural and man-made disasters and in other types of disasters. A federal commission (COMCAT) has been recently created i) to co-ordinate the preparedness in case of disasters in Switzerland, ii) to exchange technical information and iii) to harmonize the rescue's methods with others countries.

Monitoring of the environement is an essential part of a disaster pervention and preparedness plan. Switzerland has a dense hydrometric federal network providing measurements of waterlevel and runoff (450 stations), and automatic meteorological measurements (780 stations), precipitations values (348 stations), stormwarning network (29 stations), and 2 radar equiped stations. The natural hazards are highly monitored. A forest monitoring activity / program is done yearly. The radioactivity control (a network of 51 stations) is designed as warning system network. Seismological service has 22 stations with automatic teletransmitters (a network of strong motion instruments with 33 stations is implemented in Switzerland).

In Switzerland, hazard mapping and zonation is done for hazard and risk assessment of various natural disasters (e. g. avalanches, landslides, floods); GIS (Geographical Information Systems) are now in different stages of implementation . Building codes for engineering construction are used as a technical instrument to mitigate the effects of earthquakes. Other measures provided through legislation are: land use planning, forestry and protection against floods, protection of human life and property from damage caused by flooding, erosion and deposit of debris. Swiss research programmes which are now active in the field descriebed in this section are: i) "Climate Change and Natural Disasters", ii) "Priority Program Environement ", iii) Forest Monitoring Program". In Figure 2 is given a list of natural disasters as well as technological disasters and the appropiate institutional responsability (primary and secondary) in Switzerland (preparedness at the federal level). A chart of a "possible" crisis committee at the communal level is presented in Figure 3 (see /9/).

RISK CRITERIA AND A PROPOSED ACCIDENT EVENT SCALE FOR RISK COMMUNICATION MANAGEMENT

A tool for **accident event scale** risk communication has not yet been agreed. The federal authorities (e.g. BUWAL) published, in view of beeing exercised on a trail base, a multi- indicators event scale (see /2/) based on the following type of impact (risk) indicators: n_1-number of death or number of persons with high degree of invalidity, n_2-number of injuries, n_3-number of persons evacuated from the affected , n_4- alarm factor, n_5-animal population loss, n_6-ecosystem damage, n_7-contaminated ground, n_8-contaminated groundwater, n_9-discounted expenditures (see Figure 4).

A **risk criteria** F-N diagram in practice in Switzerland is using mainly linguistic variables (e.g. incident, accident, catastrophy, for consequence description and rare, very rare, improbable, extremely rare for the likelihood description etc.) next to a probabilistic scale of values and consequence assessment (see /2/). No definitive criterias were agreed at the national, regional or at the industrial / technological type levels (see Figure 5).

Such risk communication instruments are meant to assist decision makers and risk engineeres making comparative assessment of various technological risk scenarious (see /2/).

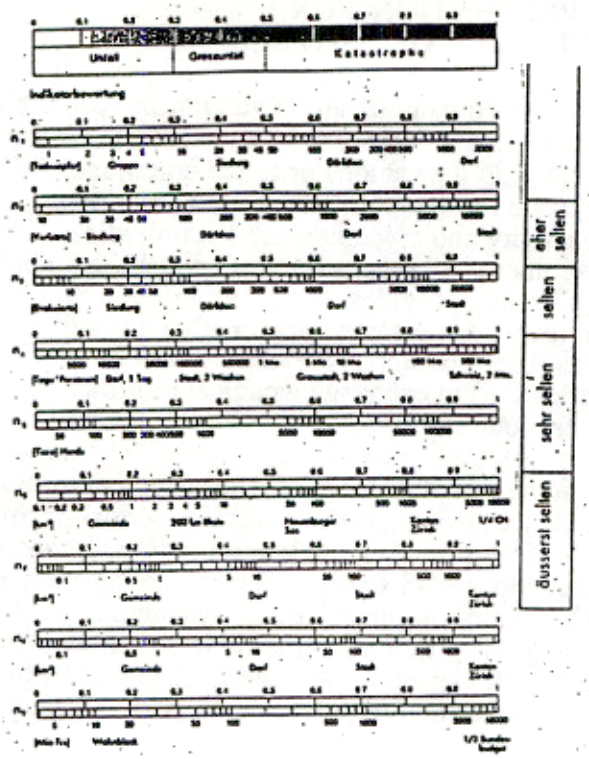


Figure 4. Accident event scale

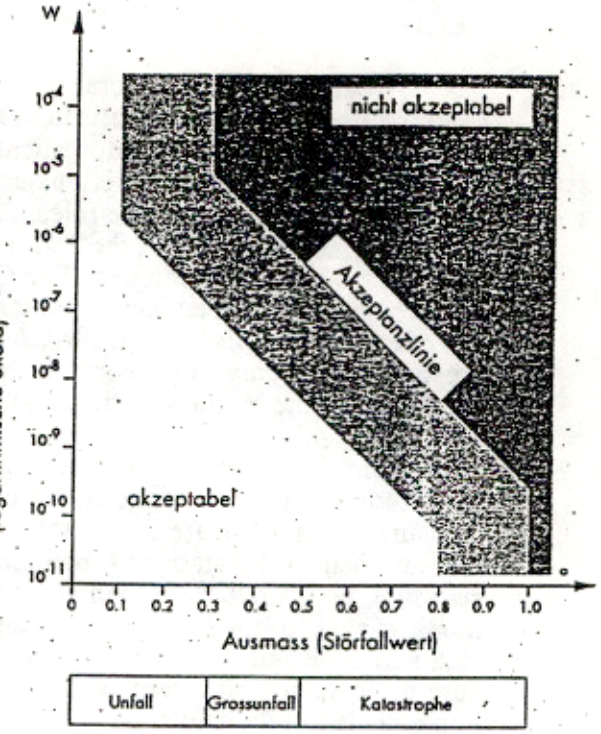


Figure 5. Risk criteria diagram

SWISS LEGISLATION FOR RISK PREVENTION AND SAFETY MANAGEMENT: PROCESS INDUSTRIES, TRANSPORTATION OF DANGEROUS GOODS, MICROORGANISMS AND BIOTECHNOLOGIES

Legislative acts regulate risks from industrial and other types of activities (see /5/). The most recent / important legislative act is known as "Die Storfallverordnung (StFV)" entered into effect in April 1991; it is reffering to preventing hazarduous situations when (heavy) consequences on population and environment could occur; all these are due to (industrial) accidents (see /1/). The StFV approach is dealing with various chemical installations and plants, instalations dealing with microorganisms, as well as with the systems of transportation of dangerous goods either by rail, road or on the river Rhein . Additional literature references present a number of methodological considerations and guidelines for implementing different risk assessment procedural issues which are relevant to the existing Swiss legislation on industrial risk assessment and safety management (e.g. StFV), (see /2/, /3/).

REFERENCES

1. *** "Die Storfallverordnung (StFV): Verordnung uber den Schutz vor Storfallen", BUWAL, Bern, Switzerland, 27 February 1991.
2. *** "Handbuch I zur Stoerfallverordnung StFV, Richtlinien fuer Betribe mit Stoffen, Erzeugnissen oder Sonderabfaellen", Eidg. Drucksachen und Materialzentrale, Bern, Switzerland, 1991.
3. *** "Handbuch II zur Stoerfallverordnung StFV, Richtlinien fuer Betribe mit Mikroorganismen", Eidg. Drucksachen und Materialzentrale, Bern, Switzerland, 1992.
4. J. Schneider (ed.) - "Risiko und Sicherheit technischer Systeme", Birkhauser Verlag, Basel, 1991.
5. H. Seiler - " Risiko und Sicherheit technischer Systeme: Rechtsgrundlagen", PPR&S-Bericht 03/93, May 1993.
6. W. Kroger , H. Wasmer - Vorlesungsskript "Risiko und Sicherheit", Sommersemester 1991, ETH, Zurich.
7. A. V. Gheorghe (ed.) - " Integrated Regional Risk Assessment and Safety Management. A Guideline Manual for Systems Enginers and Decision Makers" (in Draft), ETH, Zurich, November 1993.
8. G.E.G. Beroggi et. al.- " Operationelle Routenwahl im Gefahrenguttransport", PPR&S Dokumente, No. 1, ETH, Zurich, 1993.
9. *** " The Swiss IDNDR Committee", in the Internatioanl Civil Defence Journal, volume 6, September 1993.

WESVA: A DECISION AID FOR COMPARING WARHEAD ADVANCED SURETY R&D OPTIONS*

Robert V. Homsy, Alan Sicherman, Douglas R. Stephens

Lawrence Livermore National Laboratory
P. O. Box 808, L-85
Livermore, CA 94551

INTRODUCTION

Newly designed warheads that incorporate advanced surety concepts can reduce the risks of accidental radiological material dispersal, nuclear detonation, and unauthorized use. But these potential surety benefits entail cost and performance penalties. Present constraints on R&D budgets, time, and allowable nuclear tests also create significant uncertainties as to whether new concepts can be successfully developed and implemented. These factors complicate the decisions involved in selecting surety concepts for more extensive R&D.

To help decision makers compare R&D options, we developed a decision aid called Weapon Safety Value Assessment (WESVA). This paper describes WESVA and suggests how a WESVA-like approach can be of interest in other decision-making contexts.

WESVA OVERVIEW

WESVA helped to analyze the alternative concepts by modeling complex facets of the problem individually, and then combining these submodels to compute an expected surety payoff for each alternative (Figure 1). The submodels were developed pragmatically in six weeks and incorporated in an Excel spreadsheet, where key parameter inputs for each concept and submodel could be easily varied by the decision maker. By interacting with WESVA, the

Figure 1. Schematic of the WESVA decision-aid model for comparing advanced surety options.

* Work performed under the auspices of the U.S. Department of Energy by the Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

Weapons Surety program leader was able to identify concepts that remained top ranked over a credible range of key parameter variations. More specifically, submodels were developed to address the issues described below.

Probability of Technical Success

We defined probability of technical success as the likelihood of achieving the concept's design goals — surety and military performance — given the constraints of time, number of permitted tests, and expected budgets. With enough time, testing, and funding, the likelihood of reaching design goals would be high, but given the situation in November 1992, technical success was not deemed certain for most concepts.

We used subjective probability assessment techniques[1] to elicit the probability of technical success from an expert panel of physicists, materials scientists, and design engineers. Estimates of the probabilities of physics success, materials success, and engineering success were obtained first, and then the probability of technical success was calculated as the product of these three probabilities. Then for each concept the panel assessed an overall probability of technical success that was consistent with the product of the individual probabilities.

Probability of Acceptance

While each concept (if technically successful) offers varying degrees of risk reduction, each has an associated penalty of cost and reduced military performance. DOE incurs R&D and testing costs, and DOD may incur the cost of flight testing and modifications to the delivery system. Military performance penalties could accrue from reduced warhead yield or reliability. The more penalties there are, the less likely it is that a new concept would be preferred over existing alternatives that have fewer surety improvements, but also fewer penalties. We developed a marketing submodel that computes the probability of government acceptance for each concept. This submodel incorporates judgments about the relative severity of individual penalties.

Probability of Producibility

The probability of being able to produce the concept was estimated by a process similar to the one used to determine technical success. An expert panel considered the present DOE nuclear weapon production complex and plans for future production. Issues and uncertainties included the likelihood and timing of infrastructures required for production of each concept: whether production would be possible with relatively simple modifications to current facilities (present production facilities possibly augmented by national laboratory facilities), or whether an entirely new complex would be necessary. Given the uncertain status of Complex-21, the planned DOE nuclear weapon production complex, higher probabilities of producibility were assigned to systems involving warhead pit reuse than to those requiring new pits.

Probability of Implementation

The product of the probabilities for technical success, government acceptance, and producibility yields the overall probability of implementation of a concept.

Surety Improvements

A submodel was developed to compute the surety enhancements for each concept. This submodel incorporated judgments about a concept's reduced risk relative to the current warhead for different accident scenarios and assumptions about weapon operational configurations. For each concept, enhancements were quantified for each of the three surety concerns: radiological dispersal, nuclear detonation, and use control*.

---

* Use control features minimize or prevent unauthorized enablement.

Preferences and Expected Payoff

A preference submodel (multi-attribute utility function) was developed and calibrated using formal assessments of a decision maker's (a) willingness to gamble for more impressive surety achievements and (b) view of the relative importance of surety risk-reduction aspects (dispersal, detonation, and use control). For each alternative warhead concept, input to the preference model consists of individual payoffs on the three surety scales and the probability of implementation. The model then computes a single expected payoff for each concept, consistent with the decision-maker's preferences. The alternative R&D concepts are then rank ordered according to their expected payoff.

DETAILS OF THREE SUBMODELS

Surety Enhancement Risk Assessments Submodel

The major goals of the enhanced surety program are to reduce the risks of special nuclear materials (SNM) dispersal, nuclear detonation, and the unauthorized use of SNM for nuclear weapons. We needed to perform a very quick risk assessment for nuclear weapons in the submarine-launched ballistic missile (SLBM) system. Although there were no published risk assessments for this application, we were able to use the limited information available from a number of other weapons studies.

We decided to carry out a relative risk assessment, i.e., risks relative to the existing W88 warhead carried in the Mk5 re-entry body (RB). We evaluated four accidental dispersal modes: fuel fire, propellant fire, propellant detonation, and HE detonation. The radiological materials included both plutonium and enriched uranium (oralloy). Health consequences are different for the various dispersal modes and radiological materials. We therefore explicitly took into account the fraction of respirable material and relative health effects of the various materials.

We used the risk assessment carried out for the ICBM Replacement Warhead Phase I Study for the Minuteman III W78 warhead to evaluate risks in some of the weapon states, and thus needed to assess risks of the W88 relative to the W78. Fortunately, both weapons contain similar conventional high explosives, so the assessment was not too difficult.

Our assessment considered three operational configurations for warhead-missile operations (Figure 2):

- In the 'no mated missile moves' configuration a missile is transported to the explosive handling wharf and loaded into a submarine before the RB, which contains warheads, is attached to the missile. Risks of SNM dispersal resulting from either propellant fire or detonation are minimized.
- In the 'mated missile moves' configuration the RBs are installed on a missile prior to transportation to the explosive handling wharf, and thus accidents leading to either propellant fire or detonation could potentially cause SNM dispersal.
- In the 'no stage III detonable propellant' configuration a mated missile is moved, but either it has no third stage or its third stage propellant is non-detonable.

We evaluated four RB life-cycle states (Figure 2). The DOE Pilot Safety Study showed that the risks for both assembly and disassembly at Pantex are very low, so they were not considered further. Risks for transport by Safe-Secure Trailers (SST) were included in the study, as was RB storage. Results from the ICBM Replacement Warhead Phase I Study were modified for these weapon-state risks for the SLBM case. Finally, a quick assessment was carried out at an SLBM base for the three operational configurations described above.

The SNM dispersal frequencies were estimated for each of the warhead candidates with respect to the existing warhead for each of the three weapon system states of transportation, storage, and SLBM operational configurations, and for the potential dispersal modes. These were then corrected for relative consequences by relative health effects and mass of SNM to arrive at relative dispersal risk-reduction estimates for each candidate.

The presence or lack of multipoint detonation safety and relative improvements in use control were obtained from expert panels. These three factors — SNM dispersal risk reduction, multipoint safety, and use control improvement — constituted the surety improvement input to WESVA.

Figure 2. Four RB life cycles (indicated by shadows) were evaluated.

Probability of Acceptance Submodel

The surety improvements for any concept are not obtained without incurring penalties. In this submodel we first estimated penalties involving increased cost and decreased military performance. We then estimated the effect of these penalties on the probability of acceptance.

Costs. Costs that would be incurred by implementing an enhanced surety concept into the stockpile include both DOE and DOD expenditures. DOE costs include the research, development, testing and engineering necessary to prove out the concept, followed by the costs to produce it. DOD costs could range from relatively minor changes in software and in RB baseplate design, to major costs if the RB or third stage configuration is significantly altered or additional flight testing is required. These costs were estimated from previous studies.

Military Performance. None of the proposed enhanced surety concepts would improve the military performance of the Mk5 system, where military performance comprises the warhead's nuclear yield and reliability, and the Mk5's range and accuracy. One of the design constraints was that the weight of the warhead must not exceed that of the current W88. Thus the range and accuracy of the system was not expected to change.

We examined the effects of yield from plots of the probability of target kill. A problem with such an approach is the uncertainty as to what a target set should be, given the recent —and still changing — fundamental changes worldwide. We chose two target sets that should reasonably bound the ranges of uncertainty in target sets: the 400 hardest targets in the Bush-Yeltsin database (i.e., given the Bush-Yeltsin agreement) and the 100 hardest targets in the START I database.

Reliabilities for each concept were estimated by a team of design experts in the same way the probability of technical success was estimated. These results — effects of decreased yield and reliability — were considered in the probability of acceptance.

Probability of Acceptance Estimation Algorithm. Given the possible penalties associated with a concept, the surety enhancement concern was the effect that such penalties would have on the probability of acceptance. To estimate this effect, WESVA provided a four-step algorithm to compute a probability of acceptance for each alternative.

In step 1, each different kind of penalty was *converted* into an equivalent penalty expressed in the form of equivalent DOD dollars. For DOD cost penalties, such a conversion was direct; e.g., any RB modification costs associated with a concept represented direct DOD dollar costs. For DOE costs, the issue was how extra DOE dollars would influence acceptance rela-

tive to extra DOD dollars. WESVA modeled this issue by assessing the ratio of DOE to DOD dollar equivalent penalty analogous to monetary currency conversion.

For specific yield (and reliability) decrements, equivalent DOD dollar penalties were assessed by posing this question to the decision maker: Which would be a more difficult situation to 'market': warhead A with a penalty of yield level Y, or warhead B with a penalty of DOD dollar costs $P (with all other issues otherwise identical for A and B)? By adjusting the level of $P, we assessed that dollar level where the marketing of hypothetical alternatives A or B was deemed *equally* difficult. This represented the equivalent DOD dollar cost for that penalty.

In step 2, all the equivalent costs for an alternative were summed into a grand total penalty.

In step 3, a 'breakeven' total cost was assessed as follows. If a concept were to offer a particular surety improvement with negligible penalty ($0), the probability of acceptance would be 1. If, however, a concept offered the surety improvement at ultimately too steep a penalty (a 'no-sale' cost), there would be negligible chance of successful marketing, implying a probability of acceptance of 0. Midway between $0 and $no-sale, we found a breakeven point where it was assessed to be just as likely as not (50/50 chance) to successfully market the alternative (i.e., convince DOD to accept) given its penalty.

Figure 3. A probability of acceptance model.

In step 4, the information from steps 1-3 was combined to calibrate a probability of acceptance model such as the one illustrated in Figure 3, which reflects a simple analytic marketing model based on a 'logit' function of the form:

$$\text{prob. of acceptance} = 1/[1+\exp(a*(\text{total penalty} - \text{breakeven penalty}))]$$

where parameter a controls the reverse S-shape of the curve. The shape of the curve reflects the judgment that penalty changes relatively near either extreme on the abscissa will hardly affect marketing success, but that changes near the breakeven point have a more dramatic effect. The 'logit' function commonly appears in marketing acceptance modeling literature.

Preferences and Expected Payoff Submodel

If there were an alternative option that had equal or better 'ratings' on each surety concern and probability of implementation than any other option, choosing this alternative as the best would be easy. But there is a *dilemma* when some options have lower implementation probabilities but better surety improvements than others or when an alternative is better on one aspect of surety but not as good on another aspect.

Preference models based on multi-attribute utility theory[2] have been developed to help decision makers logically and systematically address precisely this kind of dilemma. These models adopt a set of reasonable preference assumptions that can be used to simplify the comparison problem. With these assumptions, a decision maker indicates preferences and willingness to gamble for relatively simple decision situations to calibrate a preference model. The model is then used to establish how more complicated comparisons should be made to be consistent with the simpler comparisons and the preference assumptions.

A few basic questions are asked of a decision maker (or study team) in calibrating a preference model. They involve comparing simple hypothetical alternatives labeled A and B. The questioning proceeds by varying one of the alternatives until the decision maker is indifferent

(prefers neither A nor B). A set of model equations is then solved to compute model parameters that will reflect the decision maker's preferences expressed by the comparisons of A and B.

An example of such a question is: Which would you prefer if you had to choose between *only* these two options: (1) hypothetical warhead A with (dispersal = 100, use control = 1000) or (2) hypothetical warhead B with (dispersal = 1000, use control = 1)? In this comparison, all other concerns are assumed identical for options A and B. If the decision maker prefers neither A nor B, this indicates a willingness to go from a dispersal achievement of 1000 down to 100 in order to gain use control improvement from 1 to 1000. Tradeoff questions such as these capture the relative importance of levels of achievement for the different surety concerns.

A surety improvement multi-attribute utility function, u_{si}, is calibrated using such value-judgment assessments, so that the *expected value* of u_{si} is the appropriate index to use in rank ordering the alternatives. The main results of multi-attribute utility theory cover *conditions* for which u_{si} can be expressed in a simple mathematical form and meaningfully and consistently calibrated using preference information like that illustrated above.

Conditions justifying the use of the following additive form were found to be reasonable for our problem. Let $\underline{a}$ denote the surety 3-tuple for an alternative A having surety estimates (dispersal=a_1, multipoint safety (multipt)=a_2, use control=a_3). Then

$$u_{si}(\underline{a}) = k_{\text{dispersal}}{}^{*}u_{\text{dispersal}}(a_1) + k_{\text{multipt}}{}^{*}u_{\text{multipt}}(a_2) + k_{\text{use control}}{}^{*}u_{\text{use control}}(a_3)$$

In the formula above, the u_i embody the decision maker's willingness to gamble, and the k_i embody the tradeoffs. An expected payoff for each actual alternative is calculated as follows:

$$\text{Expected payoff} = p_{\text{implementation}}{}^{*}u_{si}(\text{alternative}) + (1\text{-}p_{\text{implementation}})^{*}u_{si}(\text{default})$$

The default represents the surety outcome if a recommended alternative fails to be implemented.

CONCLUSIONS

WESVA provided a framework for systematically analyzing and discussing the pros and cons of complex, competing alternatives. By interacting with the WESVA spreadsheet, the decision maker was able to identify alternatives that remained top ranked over a wide range of key input parameter and assumption variations. The model was exercised hundreds of times to investigate the sensitivity of results to such things as changes in surety estimate assumptions, acceptability and producibility assumptions, and preferences and value judgments.

The submodels quantitatively address in a tractable manner basic questions related to comparing alternatives including: How is a concept an improvement over presently available technology? Can technical feasibility be established within time and resource constraints? Will the 'customer' accept the product, and if so, can the DOE deliver?

The WESVA approach incorporates a generic decision analysis philosophy that stresses the following issues: (1) Assumptions should be well-defined. Decision analysis is formally derived from a set of well-defined assumptions (axioms) that underlie rational decision-making. (2) Preferences should be explicitly stated. Decision analysis clearly identifies the tradeoffs involved in a decision. (3) Uncertainties should be explicitly addressed. Key uncertainties associated with a given alternative can be quantified using probabilities. The mathematical foundations of multi-attribute utility theory allow these probabilities to be combined with preference information to arrive at an overall decision. A WESVA-like approach to decision-making forces explicit assumptions,formally documents the analysis inputs, and provides feedback to designers on how to modify alternatives to improve expected payoff.

REFERENCES

1. M. W. Merkhofer, "Quantifying judgmental uncertainty: methodology, experiences, and insights," *IEEE Trans. Systems, Man, Cybernetics*, SMC-17(5) (1987).
2. R. L. Keeney and H. Raiffa, "Decisions with Multiple Objectives," Wiley, New York (1976).

009 Uncertainty in Offsite Consequence Models for Reactor Accidents

Chair: J.C. Helton, Arizona St. U

Modular Analysis of Radiological Consequence Uncertainties and Sensitivities (MARCUS)

L.F. Restrepo (SNL), F.E. Haskin (U. New Mexico)

Summary of Uncertainty Analysis of Dispersion and Deposition Modules of the MACCS and COSYMA Consequence Codes - A Joint USNRC/CEC Study

F.T. Harper, L.A. Miller, M.L. Young (SNL); L.H.J. Goossens, R.M. Cooke (Delft U. Technol.); S.C. Hora (U. Hawaii); J. Pasler-Sauer (KfK, Germany); C. Lui (USNRC), N. Kelly (CEC, Belgium)

A Procedure for Assessing Uncertainty in Models.

M.D. McKay, R.J. Beckman (LANL)

Uncertainty and Sensitivity Analysis of Early Exposure Results with the MACCS Reactor Accident Consequence Model

J.C. Helton (Arizona St. U), J.D. Johnson (GRAM); M.D. McKay (LANL); A.W. Shiver, J.L. Sprung (SNL)

MODULAR ANALYSIS of RADIOLOGICAL CONSEQUENCE UNCERTAINTIES and SENSITIVITIES (MARCUS)

Louis F. Restrepo[1], F. Eric Haskin[2]

[1]Sandia National Laboratories (SNL), Albuquerque, NM
[2]University of New Mexico (UNM), Albuquerque, NM

INTRODUCTION

Models to support dispersion, transport, and radiological consequences with significantly improved capabilities have evolved over the last two decades. Unfortunately, most available computer codes have not been able to incorporate some of these capabilities, mainly because they can not be easily adapted into the framework of older codes (e.g., MACCS[1]). To fully support uncertainty and sensitivity (U&S) analyses, computer codes which are much faster running than the current ones are needed along with those that automatically have built into their structure U&S capabilities, including the ability to propagate throughout the models the distribution of possible input variables and to consider alternative analytical models.

With those computer codes that have been able to incorporate some improved modeling capabilities, however, have come increased levels of complexity and increased computer run times. As a result, the current U.S computer codes are only partially able to model some of the important needs required for safety analysis and probabilistic safety assessments (PSAs) of power plants or DOE nuclear facilities. Within the last decade, the European Community has been developing state-of-the-art probabilistic accident-consequence assessment codes such as COSYMA and UFOMOD.[2,3] Even though these codes do incorporate some of the latest models and have great flexibility (i.e., allow the selection of alternative models), the greater flexibility of the European codes has been achieved at the cost of greatly increased run-time; therefore, they are unable to support full U&S analyses adequately.

A new generation of radiological consequence computer code called the Modular Analysis of Radiological Consequence Uncertainties and Sensitivities (MARCUS) is being developed by SNL and UNM to follow modern software engineering practices.[4,5] This paper presents (1) a brief description of its major modules with emphasis on new approaches or models being implemented and (2) discusses the software requirements for the code, including the techniques being used to optimize the run-time, and the U&S analysis capabilities of the code.

STRUCTURE AND DESCRIPTION OF THE MARCUS PROGRAM SYSTEM

MARCUS is being developed using modern software quality engineering practices[4,5] to allow convenient maintenance and upgrades. Preprocessors are being used to generate site-specific and time-dependent calculational factors to minimize run-time.

MARCUS is being designed to model both short-term (up to one week) and long-term (up to 50 years) consequences within a 50-mile radius; as such, the structure of the code is divided

into two sub-systems: early and chronic. Population densities, land cover, and receptor locations are defined in a polar-coordinate system, similar to the one being used by MACCS.[1]

Each subsystem of MARCUS has an almost identical modular structure, the only difference being the time frame modeled. Each subsystem consists of several program modules designed to sequentially assess the radiological consequences.

Each of the modules is designed to be called directly from the MAIN program, the function of which is to coordinate the execution of the subsystems and the processing of input and output. Intermediate results can be obtained from various modules if requested by the user. The following is a brief description of the major modules within MARCUS.

Input Module (INPUT)

This module reads all the data required to define the accident consequences to be modeled. Point estimates or distribution functions (i.e., uncertainty of input) can be defined. Furthermore, the user will be able to select from several predefined models (e.g., dispersion and coefficient models) for which U&S analyses can be performed. Output options are also controlled by this module.

Input Sampling Module (SAMPLE)

This module prepares the input matrices for input to MARCUS when distribution functions are assigned to input variables. Presently, only the Latin Hypercube Sampling (LHS)[6] model will be implemented due to its calculational efficiency. The input for the code is supplied via ASCII text files which are in "free format" and "self documenting," as is done with MACCS.[1]

Dispersion and Transport Module (DISPER)

This module calculates (depending on model selection, from analytical solutions) space- and time- dependent integrated air concentrations per unit release (χ) for instantaneous, transient, or long- term releases. A puff model is used to simulate instantaneous releases, whereas a Gaussian plume model is used to model continuous or long-term releases. These models or their analytical solutions are commonly used and are implemented in various codes (e.g., MACCS[1] and SMART[7]). Transient or short-term releases are simulated by a combination of a puff and Gaussian plume model. Analytical solutions for transient releases are based on the assumption that the dispersion and advection of a pollutant in the downwind direction could be uncoupled from the dispersion in the crosswind and vertical directions.[8,9] As such, the concentration distribution per unit release (χ), or dispersion factor can be expressed as the product of the variation in the x-direction due to advection and dispersion, $\chi_{puff}(x,t)$, and the variation in the cross-wind and vertical directions, $\chi_{yz}(x,y,z)$; i.e.,

$$\chi(x,y,z,t) = \chi_{puff}(x,t) \cdot \chi_{yz}(x,y,z) \quad (1)$$

where

$$\chi_{yz}(x,y,z) = 1/(2\,\pi\,u\,\sigma_{yo}\,\sigma_{zo}) \cdot \exp\{-[(y^2/2\sigma_{yo}^2) + (z^2/2\sigma_{zo}^2)]\} \quad (2)$$

$\chi_{yz}(x,y,z)$ is the conventional Gaussian plume concentration per unit release or dispersion factor equation. $\chi_{puff}(x,t)$ represents the 1-D puff model; it will be assumed that the advection and dispersion of the puffs has a constant value of the downwind dispersion coefficient, σ_{xo} (calculated at the receptor location). This model provides results which are very similar to those obtained assuming the puff grows in all directions - 3D.[8] The 1-D concentration distribution for a puff of unit strength, $\chi_{puff}(x,t)$, is:

$$\chi_{puff}(x,t') = 1/[(2\pi)^{1/2}\,\sigma_{xo}] \cdot \exp\{-([x-u(t-t')]^2/2\sigma_{xo})\} \quad (3)$$

Where u is the average wind speed, and σ_{xo}, σ_{yo}, and σ_{zo} are calculated at the midpoint of the spatial interval. Integration times are based on either the travel time of the puff, the duration of the passing cloud over the receptor location (range), or the duration of the evacuation. All dispersion calculations are calculated at the midpoint of the interval.

The concentration due to a transient release is found by integrating the product of the source function [i.e., $q(t') = q_o \exp(k_o t')$, where, k_o is the first order decay constant for the source strength] and the concentration distribution from the beginning of the release, or impact time (to receptor) to the present time. For the 1-D puff approach, the integrated concentration is given by:

$$\chi(x,y,z,t) = {}_o\int^t q(t')\, \chi_{puff}(x,t') \cdot \chi_{yz}(x,y,z)\, dt' \qquad (4)$$

The dispersion factor distribution integral represented by Equation 4 is a convoluted integral, whose analytical solution can be obtained by appropriate use of Laplace transforms. The dispersion factor distribution based on puffs of constant size is approximately given, after some simplifications (e.g., $k_o = 0$, constant source strength), by:

$$\chi(x,y,z,t) \sim 1/u \{1+\mathrm{erf}[(ut/2^{1/2}\sigma_{xo})+ (x/2^{1/2}\sigma_{xo})]\} \cdot \chi_{yz}(x,y,z) \qquad (5)$$

By providing analytical solutions to equations like 4, the running time of the code will be minimized and similar analytical solutions will be implemented into MARCUS to deal with exposure during evacuation and nonconstant source strengths (i.e., $K_o \neq 0$).

Concentration Module (CONCENT)

This module calculates the space- and time-dependent integrated air and ground concentrations by chemical group (e.g., noble gases, halogens, etc.). This module then proceeds to calculate the concentration for each individual radionuclide postulated to be released. The first set of calculations minimizes the number of operations or calculations that needs to be performed by assigning deposition velocity and washout coefficients to each chemical group instead of to each radionuclide. The second set of calculations includes the actual radionuclide-inventory release and calculates the ingrowth and decay of each radionuclide during transport. Ingrowth and decay calculations are performed by a submodule which is called by CONCENT and by the dose consequence calculational module.

Dose Module (DOSES)

This module calculates individual organ doses for both short- and long-term exposures. An implementation of the new ICRP 60[10] organ-weighting factors (W_t) and "effective dose" will be used instead of the ICRP 26[11] organ-weighting risk factors for effective dose equivalent (EDE). Contributions by radionuclide and exposure pathway can be obtained.

In the early- or short-term subsystem, exposures from inhalation and immersion are calculated, along with the exposure from groundshine up to the time of evacuation (maximum of 7 days). In the chronic or long-term subsystem, additional doses are calculated from ingestion and resuspension inhalation of material deposited on the ground. Precalculated dose-to-source conversion factors for ingestion based on Regulatory Guide 1.145[12] are available. Time-dependent dose-conversion factors (DCFs) are generated by another preprocessor (IDCF)[13] and are also available for this module.

This module also calculates dose-dependent actions (i.e., relocation) of evacuees by using analytical solutions (e.g., convoluted integrals/Laplace transforms, and approximations).

Early Health Risk Module (EHRISK)

This module calculates individual risk (nonstochastic) health effects, from both low and high linear energy transfer (LET) radiation. Presently, no computer codes in the U.S. including MACCS[1] have been able to incorporate the modeling of health effects from both low- and high-LET radiation, mainly because their model structures are unable to handle dose-rate calculations required for full implementation of these models. MARCUS will include the means to incorporate dose-rate- dependent models within its structure.

The risks of early (nonstochastic) and continuing health effects from low- and high-LET radiation are modeled using hazard functions. The relationship between health risk and

hazard functions is given by equation 6.[14,15]

$$\text{Risk} = 1 - \exp(-H) \tag{6}$$

Where Risk is the probability that a person will exhibit a health effect of interest (usually death) and H is the lethality or morbidity hazard (i.e., cumulative hazard function). This cumulative hazard function represents for independent exposures the sum of radiation-specific hazard functions H_a, H_b, H_g, and H^*, for alpha, beta, gamma, and short high dose-rate exposure to external gamma radiation, respectively. The first three hazard functions (i.e., H_a, H_b, and H_g) correspond to protracted exposures, H_p, while H^* represents that from an acute exposure. That is, the hazard function for exposure scenarios in which all or some of the above radiation types are present, is given by:[14,15]

$$H = 0.693(D_s/\theta_{50\,s} + \Sigma_i\, DR_{p,i}/\theta_{50\,p,i})^v \quad \text{for } D_{s \text{ or } p} > T \tag{7}$$

Where

- D_s is the short-term exposure to high dose rates of gamma radiation, Gy
- $\theta_{50\,s}$ is the dose from high dose rates (short exposures) at which 50% for the population exposed will die (i.e., $LD_{50,s}$), Gy
- $DR_{p,i}$ is the low dose rate delivered in time period i (protracted dose) from alpha, beta, or gamma radiation, Gy
- $\theta_{50\,p,i}$ is the dose from low dose rates delivered in time period i for alpha, beta, or gamma radiation at which 50% of the population exposed will die (i.e., $LD_{50,p}$), Gy
- v is the combined exposure shape parameter of the radiation.
- T threshold dose for a given lethal effect, Gy

The second term in Equation 7 corrects for those doses which are received from low dose rates at longer periods of time. (A cut-off of 0.05 Gy/hr is used to distinguished between high and low dose rates.) Competing modes of death (e.g.. pulmonary, hematopoietic, and gastrointestinal death) are modeled by summing the respective lethality or hazard functions for each mode of death to obtain the overall lethality or hazard function. Upper and lower bounds for model parameters are provided to facilitate the evaluation of uncertainties.

Chronic Health Risk Module (CHRISK)

This module calculates both fatal and nonfatal individual stochastic somatic health effects using absolute and relative risk models along with cancer morbidities.[14] The recommendation of ICRP 60[10] is also incorporated.

Collective Health Effects Module (COLEFFEC)

This module calculates collective or population dose and health effects calculated in DOSES and EHRISK. COLEFFEC reads databases containing the population density as a function of radial distance and sector (same as input to MACCS[1]).

SOFTWARE REQUIREMENTS FOR MARCUS

MARCUS will be written in FORTRAN 77 with some FORTRAN 90 capabilities, using the LAHEY® Fortran compiler. MARCUS will run on any IBM-compatible 386/486 computer system with a minimum of 8 MB RAM. Besides designing the code in a modular form to allow easy maintenance and modifications, the following are the most important software requirements placed on MARCUS: (1) minimize running time of the code, (2) allow for uncertainties in important input variables and models. (3) implement new and accepted conventional models for important phenomena, and (4) provide output which is designed to support safety analysis and PSA activities.

Minimize Running Time

One of the main goals in the development of MARCUS is the ability to support full U&S analyses, that is, to develop a computer code that is faster by at least a factor of ten than the most commonly used codes with similar features. Such a goal will be accomplished by the implementation of the following features: (1) use of analytical solutions for dispersion models, e.g., Equation 5, (2) analytical solutions of evacuation models, (3) use of representative chemical groups to determine the dispersion factor or concentrations, (4) the development of efficient ways to sample meteorological data in order to represent the entire meteorological data in the most efficient and rapid manner. (5) use of preprocessors to develop a site- and time-dependent dose-conversion-factor database when needed, (6) use of a fast and efficient submodule to support ingrowth/decay calculations, and (7) the use of RAM instead of disk files to store intermediate results.

Uncertainty in Important Input Variables and Models

MARCUS will use stratified sampling based on Latin Hypercube Sampling (LHS)[6] to support the U&S analyses. LHS allows the handling of input variables with different distribution functions and reduces the number of samples required to represent each of the input variable distributions. Because of the modular structure of the code, the flexibility of using various predefined important models for U&S purposes will be supported.

Important variables will be selected based on previous sensitivity analyses performed for other offsite consequence modeling codes.[16,17] MARCUS will concentrate on the uncertainty of the dispersion and transport input parameters and models, on the exposure durations, and on other parameters affecting the consequence calculations; uncertainty in source term input variables will not be handled by the code during the early development.

The user will have the flexibility to use either single-point estimates or frequency distributions for the set of input variables preselected to support U&S analyses. To accomplish this, MARCUS will use the LHS code[18] to sample from distributions when these have been assigned to various input variables and to create input matrices for the code. Correlations among input variables will also be modeled.

Implementation of New and Conventional Models for Important Phenomena

MARCUS will incorporate some of the new state-of-the-art models developed in the last two decades, along with some conventional acceptable models that are widely implemented in other codes like MACCS.[1] More specifically, it will incorporate better models to determine the dispersion coefficients using similarity theory or distance/surface-dependent models, plume-height models, resuspension modeling, particle size distribution modeling, and new health-effects models, among others.

Output Designed to Support Safety Analysis and PSAs

The last goal of MARCUS is to be able to support the needs of safety-analysis activities and probabilistic safety assessments (PSAs), especially for DOE facilities. This includes calculating concentrations per unit release or dispersion factor distributions, dose rankings per radionuclide or exposure pathway, health effects, and risk distributions (consequence vs. frequency distributions).

CONCLUSION

The first phase will consist of the development of the code to support early consequences, including those during evacuations. The following tasks will be included in this phase: (1) a thorough literature review of models developed in the last two decades to support consequence calculations (e.g., dispersion, transport, dosimetric, health effects, and uncertainty/sensitivity modeling); (2) the development of the software quality-engineering

documentation for the code; (3) the development of the basic modular structure or software logic of the code; (4) the code documentation (source listing), which will include the default models to support early consequences (e.g., Latin Hypercube Sampling, modeling of instantaneous, short- and long-term releases, early health effects models for low- and high-LET radiation, and use of semi-dynamic food models).

The second phase will consist of further development of the code to incorporate models to support chronic or late consequences. It will also begin the incorporation of the alternative models to be used by the code (e.g., use of various dispersion-coefficient models, including the use of similarity theory, plume rise, and building wake effects).

The third phase will consist of a refinement of all the models incorporated into the code so far and full software testing, including validation and benchmarking against other codes, e.g., MACCS, and development of user-friendly interfaces like windows or menu-screen-driven input capabilities.

REFERENCES

1. H-N Jow, et. al., MELCOR Accident Consequence Code System (MACCS), NUREG/CR-4691, U.S. Nuclear Regulatory Commission (1990).
2. J. Ehrhardt and J. A. Jones, An Outline of COSYMA, A New Program Package for Accident Consequence Assessments, Nuclear Technology, Vol. 94 (1991).
3. J. Ehrhardt, et. al., Structure, Important Features, and Illustrative Results of the New UFOMOD Program System for Assessing the Radiological Consequences of Nuclear Accidents, Vol. 94 (1991).
4. Draft - DOE Software Quality Assurance Requirements Procedures and Guidance, Department of Energy (1993).
5. Software Engineering Handbook by General Electric Corp.. McGraw-Hill Book Co. (1986)
6. R. L. Iman and W. J. Conover, Sensitivity Analysis Techniques: Self-Teaching Curriculum, NUREG/CR-2350, U.S. Nuclear Regulatory Commission (1982).
7. I. K. Madni, et. al., A Simplified Model for Calculating Early Offsite Consequences from Nuclear Reactor Accidents, NUREG/CR-5164, U.S. NRC (1988).
8. D. J. Wilson, Along-Wind Diffusion of Source Transients, Atmospheric Environment, Vol.15 (1981).
9. E. Pallazi, et. al., Diffusion from a Steady Source of Short Duration, Atmospheric Environment, Vol. 16 (1982).
10. 1990 Recommendations of the International Commission on Radiological Protection, ICRP Publication 60 (1991).
11. Recommendations of the International Commission on Radiological Protection, ICRP Publication 26 (1977).
12. L. F. Restrepo, Dosimetric Modeling in the Terrain Responsive Atmospheric Code (TRAC), Health Physics Journal, Vol. 56, No. 3, MPM-A6 (1989).
13. J. Foster, IDCFMAX - A Preprocessor for MACCS2 Dose Conversion Factors, Sandia National Laboratories (1993).
14. J. S. Evans, Health Effects Model for Nuclear Power Plant Accident Consequence Analysis, NUREG/CR-4214, Rev.1, Part I, U.S. NRC (1990).
15. S. Abrahamson, et. al., Health Effects Model for Nuclear Power Plant Accident Consequence Analysis, NUREG/CR-4214, Rev.1, Part II, U.S. NRC (1992).
16. J. Helton, et. al., MELCOR Accident Consequence Code System (MACCS) Sensitivity Analysis, Sandia National Laboratories, Albuquerque, NM (1990).
17. L. F. Restrepo and R. L. Iman, Draft Report of the Terrain Responsive Atmospheric Code (TRAC) Sensitivity Analysis (TRAC), Rocky Flats Plant, CO (1987).
18. R. L. Iman and M. J. Shortencarier, A FORTRAN-77 Program and User's Guide for Generation of Latin Hypercube and Random Samples for Use with Computer Models, NUREG/CR-3624, U.S., Nuclear Regulatory Commission (1984).

SUMMARY OF UNCERTAINTY ANALYSIS OF DISPERSION AND DEPOSITION MODULES OF THE MACCS AND COSYMA CONSEQUENCE CODES – A JOINT USNRC/CEC STUDY*

F. T. Harper,[1] L. H. J. Goossens,[2] R. M. Cooke,[2] S. C. Hora,[3]
L. A. Miller,[1] M. L. Young,[1] J. Pasler-Sauer,[4] C. Lui,[5] N. Kelly[6]

[1]Sandia National Laboratories
Albuquerque, NM
[2]Delft University of Technology
Delft, the Netherlands
[3]University of Hawaii at Hilo
Hilo, HI
[4]Kernforschungszentrum
Karlsruhe, Germany
[5]US Nuclear Regulatory Commission
Washington, DC
[6]Commission of European Communities
Brussels, Belgium

INTRODUCTION

This paper briefly describes an ongoing project designed to assess the uncertainty in offsite radiological consequence calculations of hypothetical accidents in commercial nuclear power plants. This project is supported jointly by the Commission of European Communities (CEC) and the US Nuclear Regulatory Commission (USNRC). Both commissions have expressed an interest in assessing the uncertainty in consequence calculations used for risk assessments and regulatory purposes.

Previously, uncertainty analyses have been performed for the Level 1 (core damage frequency evaluation) and Level 2 (evaluation of radionuclide transport from the melt to the environment) portions of risk assessments (for example in NUREG-1150[1]). However, uncertainty studies in the consequence area have been typified by the more conventional parametric sensitivity studies in which uncertainty distributions of input variables are sampled, and the impact of the different input parameter values on the output parameters are observed. In these sensitivity studies, the uncertainty distributions were developed by the code developers and not by experts in the many different scientific disciplines that constitute a consequence code. No consequence uncertainty study has been performed in which the contribution of the uncertainty from alternative modeling approaches and

*This work is supported by the U.S. Nuclear Regulatory Commission and the Commission of European Communities. Sandia National Laboratories is operated for the U.S. Department of Energy under Contract Number DE-AC04-94AL85000.

modeling weaknesses has been included for either the USNRC or the CEC. Both commissions have realized that uncertainty plays a key role in regulatory decisions involving prioritization of activities and research. Therefore, the commissions decided to pool their resources and fund this joint study.

The stated objective of the project is to formulate the methodology and obtain much of the information necessary to perform offsite radiological consequence uncertainty studies for accidental releases from commercial nuclear power plants in the US and Europe. The MACCS consequence code (US)[2] and the COSYMA consequence code (CEC)[3] will be used to perform these uncertainty studies.

With respect to this objective, a methodology for performing uncertainty studies acceptable to both the USNRC and the CEC has been developed that incorporates the developments from previous work in the field of uncertainty (methods developed in the NUREG-1150 study, the CEC pilot study on atmospheric dispersion and deposition using formal expert judgment techniques,[4] and other studies).

In addition, a library of distributions that are general in nature is being developed using formal expert judgment elicitation and evaluation techniques. The distributions will be general in nature so that they can be of use to many uncertainty studies. In order to do this, the uncertainty distributions will be quantified so that, when fitted, the models in the consequence codes emulate the uncertainty distribution information given by the experts as well as extrapolate to areas not addressed by the experts. This approach was developed because it has the potential to address the uncertainty due to the fundamental flaws in model physics, data uncertainties, and random or stochastic uncertainties in observational data. A tentative list of phenomenological areas in the consequence calculation that require distributions that will be developed jointly is presented in Table 1:

Table 1. Phenomenological Areas in the Consequence Calculation that Require Uncertainty Distributions

Phenomenological Area	Input Variable Requiring Uncertainty
Dispersion	Plume spread parameters*
Deposition	Dry Deposition velocity* Wet deposition parameters*
Behavior of deposited material and calculation of related doses	Decontamination Resuspension parameters Weathering parameters Shielding factors Penetration factors
Plume rise	Amount of plume rise Critical windspeed for liftoff
Internal dosimetry	Breathing rate Dose conversion factors
Early health effects	LD_{50} Thresholds
Late health effects	Dose rate effectiveness factors Risk coefficients (cancer)
Food chain	All food chain parameters

* -- See Description of Issues section.

Other areas are also required for consequence calculations (emergency response, land interdiction, food interdiction, etc.). Distributions for the parameters in these areas were felt to be specific to Europe and the US and are not being developed jointly (methods developed in the joint

project will be applied when performing these analyses).

It was decided to develop distributions for the dispersion and deposition models in order to demonstrate the efficacy and feasibility of the joint effort before expending the resources in the other areas relevant to consequence calculations. The reasons for choosing these two areas for assessment by the first two expert panels are (1) the dispersion and deposition parameters score high on a list of parameters prioritized by importance to different consequence measures, (2) the dispersion and deposition module comes before other modules in both MACCS and COSYMA, and (3) methods were developed to process the dispersion and deposition variables in the CEC pilot study.

For reasons related to the objective, all distributions requested in this joint exercise are general in nature. It is easy to see how distributions from the field of health effects can be used in many different consequence uncertainty studies (the somatic response to radiation is not site specific, time specific, or accident scenario specific). The problems posed for the dispersion and deposition areas are not general and were customized to be applicable to as many situations as possible; the terrain was defined as flat or gently rolling hills in order to provide information for the majority of the nuclear power plants. Surveys performed in the US and Europe indicate that about 70% of the reactors are located at sites that can be classified as having uncomplicated terrain and uncomplicated meteorology.

SUMMARY OF METHODS

The methodology formulated for this project is a combination of methods from previous US and CEC studies (in particular, the NUREG-1150 study and the CEC pilot study) as well as methods developed specifically for the joint effort. Table 2 summarizes some of the major contributions to the joint methodology from previous US studies and previous CEC studies.

Table 2. Some Contributions to the Joint Methodology from US and CEC Studies

Contributions from previous US studies	Contributions from previous CEC studies
Philosophy of choosing high quality experts and paying them	Ready made processing methodology and software for dispersion and deposition
Formal elicitation protocol developed for NUREG-1150	Concept of elicitation on variables that can be conceived as being experimentally observable
Probabilistic training and coaching during elicitation session for experts	Aggregation techniques using performance based weighting techniques[5]
Aggregation techniques using equal weighting for experts	

Formal expert judgment techniques were selected to develop these distributions for several reasons: (1) in the areas of interest, the experimental data base cannot provide the necessary information, (2) the analytical models that would provide information not observed experimentally are not indisputably correct, and (3) the uncertainty distributions provided by the experts will include the uncertainty due to alternative modeling approaches and general model weaknesses. The joint methodology for this project is summarized below.

1. **Definition of issues**: It is the responsibility of the probability assessment team to construct elicitation questions in such a way that only physically measurable quantities are addressed. Sometimes the parameters themselves are not directly measurable so that some translation is necessary to conform to this principle.

Sensitivity analyses were performed at Sandia National Laboratories (SNL) using techniques developed at Los Alamos National Laboratory (LANL) and SNL to select the code input variables

that will be assessed in the study. The list of important code input variables that was developed in the US was combined with a similar European list that was also generated from sensitivity studies.

In the case of dispersion, the important code input parameters are those that define the spread of the plume in the Gaussian model. The Gaussian model predicts airborne concentrations downwind of a release as a function of release rate, windspeed, and the plume concentration standard deviations in the horizontal (σ_y) and vertical (σ_z) directions. These dispersion parameters are modeled using the power law:

$$\sigma_y = a_y x^{b_y};\ \sigma_z = a_z x b^{b_z} \quad (1)$$

where a_y, b_y, a_z, b_z are constants and are the parameters that need to be developed.

The important deposition parameters are the dry deposition velocity v_d (v_d is defined as the ratio of the rate of deposition of radioactivity to the ground to the air concentration at ground level) and the removal coefficient for wet deposition. The removal coefficient may be written as:

$$\Lambda = aI^b \quad (2)$$

where I is the rain intensity. Distributions were needed for v_d , a and b in the area of deposition.

From the combined list of code input variables, elicitation variables were defined. Elicitation variables are the variables presented to the experts for assessment and are physical variables (potentially observable in experiments). The requirement that elicitation variables are physical (as opposed to a fitted exponent having no interpretation in terms of the physics of the problem) is imposed so that there will be no ambiguity when presenting the definition of the elicitation variables. If the experts assess poorly defined variables, the potential for incompatible assessments is high. Also, their assessments are not dependent on the model so model uncertainties can be assessed. The deposition and dispersion variables that were elicited are presented below:

Deposition:

A) Distributions on the dry deposition velocity v_d for four surface types, six particle sizes, iodine, and methyl iodide.

B) Uncertainty distributions for the fraction of material removed by wet deposition for aerosols (four particle sizes), elemental iodine, and methyl iodide.

Dispersion (for several centerline locations and for several synoptic weather conditions):

A) The normalized concentration measured at a collector located at the centerline (χ_c/Q).

B) The concentration relative to the centerline concentration at a specified crosswind location y (χ_y/χ_c).

C) The concentration relative to the centerline concentration at a vertical distance, z and at the centerline, y=0 (χ_y/χ_c).

D) The standard deviation associated with the cross wind concentration (s_y) as would be measured by a line of collectors at specified distance from the source.

E) The total area [km^2] covered by 90% of the time integrated concentration in that distance region between r_1 and r_2 (r_1 and r_2 are in the far field).

Questions in which experimental answers were known were asked as part of the probabilistic training exercise and also during the elicitation session to form the basis to apply performance based weighting techniques.

The decision was made to elicit s_y and χ/Q to enable the use of the CEC processing method (already developed and mature) and to elicit on χ_y/χ_c and χ_z/χ_c in order to also enable the use of a newer method that would address additional uncertainty (developed for the project).

2. **Selection of experts**: The project staff sought to engage the best experts available in the fields of atmospheric dispersion and deposition. Experience in the NUREG-1150 study and elsewhere has shown that the selection of experts can be subjected to much scrutiny. Thus, it is necessary to construct a selection procedure that is defensible: (1) a large list of experts was compiled from the literature and by requesting nominations from organizations familiar with the areas; (2) the experts were contacted and Curriculum Vitae (CV) were requested; and (3) an objective selection board studied the CVs and selected eight experts in dispersion and eight experts

in deposition according to selection criteria agreed upon before the process. The result was two panels of internationally recognized scientists, half of whom were provided by the US and half of whom were provided by the CEC.

3. **Preparation of experts for elicitation**: The experts were introduced to the purposes of the study including how their judgments will be used. They were also introduced to background material on consequence codes and the science of probability elicitation. This required the distribution of materials explaining the consequence area, the relation of the questions posed to the parameters in the model, and the specific initial conditions and assumptions to be used in answering the elicitation questions. Training was conducted to introduce the experts to the psychological biases in judgment formation and to give them feedback on their performance in assessing probability distributions. This was accomplished using questions similar to the elicitation questions that had known answers.

The preparation for elicitation occurred in a meeting with the experts held a month prior to the probability elicitation. Following the first meeting, the experts spent one to two weeks preparing responses to the elicitation questions and preparing a statement explaining their information sources and rationale.

4. **Elicitation**: On the first day of the elicitation meeting, the experts all delivered presentations explaining how they addressed the issues. The elicitation of each expert took place privately with a specialist in probability assessment and project specialist in the consequence codes forming the elicitation team. The elicitation interviews allowed for significant interaction between the assessment team and the expert in the encoding of probabilities.

5. **Processing of judgments**: The philosophy of the project is to allow the experts to use whatever modeling technique or experimental results that they may feel appropriate to assess the problems; the only constraints placed on the experts by the project are (1) the initial conditions had to be defined at the same level of detail as the code input (uncertainty due to lack of detail in the initial conditions has to be included in the uncertainty distributions provided); (2) the results have to be usable by the project; and (3) the rationale behind the distributions must be thoroughly documented. The project is constrained in that the MACCS and COSYMA codes will not be changed to simplify the uncertainty study. The philosophy of the project combined with this constraint have led to some complicated mathematical processing issues.

This situation was faced in the dispersion area by the CEC pilot study and a method for processing the elicited results was developed. The CEC method assessed uncertainty on the spread of the plume (a major advance over the treatment of dispersion in previous consequence uncertainty/sensitivity studies). The CEC method is briefly described below:

> In the area of dispersion, distributions on the normalized concentration (χ/Q) and the empirical standard deviation of the crosswind concentration distribution (s_y) were obtained for selected down wind distances $x_1 \ldots x_5$ from expert elicitation (s_y was assumed to approximate σ_y in the Gaussian equation). The distributions on χ/Q and s_y were combined. An optimal distribution over the parameters A,B in the equation
>
> $$lnY = lnA + Blnx_i \qquad (2)$$
>
> given quantiles for Y at $X_1, \ldots X_5$ and given an initial search grid for (A,B) is determined using the code PARFUM[6]. In the context of the Gaussian dispersion models used in both COSYMA and MACCS (assuming the power law model for growth of the plume) there is one such equation for both $Y = \sigma_y$ and $Y = \sigma_z$. On the Gaussian model, the centerline concentration sufficiently far from the source is proportional to $C = \sigma_y\sigma_z$, and hence also follows a power law. Therefore, if a joint distribution is known for A_y, B_y, A_c, B_c; the distribution for σ_z is also fixed.

In the dispersion area, the joint study proposed to include more uncertainty than that on the growth of the plume. Originally, the intent was to elicit concentration values which would sever most constraints placed on the exercise by the use of the Gaussian model in the two consequence codes. This approach would include the uncertainty from asymmetric plume behavior not captured by Gaussian models. This approach became mathematically unfeasible under realistic project constraints. A processing method in which the ratio of the concentration at specified distances from

the centerline (in both the y and z directions) over the centerline was developed. This method is briefly described below:

> The solution is based on the ideas embodied in the CEC method code. In this proposed solution, the elicited variables are χ/Q, χ_y/χ_c, and χ_z/χ_c. This solution differs from the PARFUM solution in that three distributions are used for input (the distributions for χ/Q, χ_y/χ_c, and χ_z/χ_c). The use of three distributions allows the determination of a minimally informative joint distribution. The solution is flexible (it could be used with many models) and has the advantage that expert information in the z direction is used directly.

In contrast to the processing necessary for the dispersion distributions, the processing of the deposition distributions is relatively easy. The dry deposition code input variables are elicited directly. For enhanced value of the information the dry deposition variables were elicited at a greater level of detail than that used by the codes (for example, the dry deposition velocity was elicited for several surface types (meadow, forest), whereas consequence codes typically do not allow direct inclusion of this surface dependance). The wet deposition distributions can be easily processed using PARFUM through the following equation:

$$\ln\left(\frac{\ln(f)}{-t}\right)=\ln(a)+b(\ln(I)) \qquad (4)$$

where f is the fraction removed, I is the rain intensity, t is the duration of the rain, and a and b are the code input variables mentioned above.

CONCLUSIONS

The elicitation methods developed for the joint CEC/USNRC Consequence Uncertainty Program have been successfully tested on the dispersion and deposition panel. Initial feedback from the experts is extremely positive. The distribution information obtained from the experts has been processed and dry deposition uncertainty distributions, wet deposition uncertainty distributions, and dispersion distributions that include uncertainty in the growth of the plume can be provided to those interested shortly (including those in a regulatory environment). The project will investigate the robustness of different weighting schemes (equal weighting, performance based weighting) and plans to use the joint methods on the other phenomenological areas necessary for consequence calculations.

REFERENCES

1. U. S. Nuclear Regulatory Commission, NUREG-1150, "Severe Accident Risks: An Assessment For Five U. S. Nuclear Power Plants," final summary report, Washington (1990).
2. H. N. Jow, et. al, "MELCOR Accident Consequence Code System (MACCS)," NUREG/CR-4691, SAND86-1562, Sandia National Laboratories, Albuquerque (1990).
3. Kernforschungszentrum Karlsruhe GmbH (FRG) and National Radiological Protection Board (UK), "COSYMA, A New Program Package for Accident Consequence Assessment," Luxembourg (1990).
4. R. M. Cooke, "Expert Judgment Study on Atmospheric Dispersion and Deposition - Main Report and Annexes," Report of the Faculty of Technical Mathematics and Informatics, no 91-81, Delft (1991).
5. Cooke, R. M., "Experts in Uncertainty," Oxford University Press, New York (1991).
6. S. French, R. Cooke, F. Vogt, "The Use of Expert Judgment in the Context of a Postulated Mathematical Model," Bayesian Statistics 4, 617-624, J. M. Bernardo, J. O. Berger, A. P. Dawid and A. F. M. Smith (editors), Oxford University Press (1992).

A PROCEDURE FOR ASSESSING UNCERTAINTY IN MODELS

Michael D. McKay and Richard J. Beckman

Statistics Group, MS F600
Los Alamos National Laboratory
Los Alamos, NM 87545

INTRODUCTION

This paper discusses uncertainty in the output calculation of a model due to uncertainty in inputs values. Uncertainty in input values, characterized by suitable probability distributions, propagates through the model to a probability distribution of an output. Our objective in studying uncertainty is to identify a subset of inputs as being important in the sense that fixing them greatly reduces the uncertainty, or variability, in the output.

The procedures we propose are demonstrated with an application of the model called MELCOR Accident Consequence Code System (MACCS), described in Helton *et al.* (1992). The purpose of MACCS is to simulate the impact of severe accidents at nuclear power plants on the surrounding environment. In any particular application of MACCS there are likely to be many possible inputs and outputs of interest. In this paper, attention focuses on a single output and 36 inputs. Our objective is to determine a subset of the 36 model inputs that can be said to be dominant, or important, in the sense that they are the principal contributors to uncertainty in the output.

OUTPUT, INPUTS AND PROBABILITY DISTRIBUTIONS

MACCS is used to calculate consequences of a reactor accident at a nuclear power station whose characteristics and those of the surrounding environment are defined by inputs. The output selected for examination is Early Fatalities, meaning the number of fatalities within one year of the accident. MACCS is composed of submodels for source term, plume rise, atmospheric transport, dry deposition, wet deposition, evacuation, food chain transport, and dosimetry and health effects. For each of the inputs, analysts determined plausible ranges of uncertainty for the inputs from the literature, experimental results and submodel considerations. Because of the preliminary nature of this particular analysis, uniform and loguniform probability distributions defined on input ranges were used. For subsets of inputs that could not be treated reasonably as stochastically independent, joint

probability distributions or correlation coefficients were determined. For many more details on this part of the analysis process see Helton *et al.* (1992).

In a discussion, it is easy to gloss over the initial step of deciding upon probability distributions for inputs. Nevertheless, this step constitutes the basis for all inference regarding uncertainty. The probability distribution of the output and the identification of important input subsets depend directly on the probability distribution (form and range) of inputs. A very reasonable last stage of uncertainty analysis would be investigation of sensitivity of results to assumed distributions for inputs.

SOME DETAILS

The output of interest is Early Fatalities. In more precise terms, the quantity that MACCS computes is the complementary cumulative distribution function (CCDF) of Early Fatalities induced by treating weather conditions at the time of the accident as a random phenomenon. Tables of weather parameters (one year of hourly readings of wind speed, wind direction, atmospheric stability, and precipitation) are sampled repeatedly during the MACCS run to produce, in effect, a Monte Carlo estimate of the CCDF as a function of time. We denote this output CCDF by $Y(t)$. Then, we have

$$\begin{aligned} X &= \text{Input vector of length 36,} \\ Z &= \text{Weather conditions,} \\ Y(t) &= \text{Output CCDF of Early Fatalities } (EF), \\ &= Pr\{EF > t\} \text{ for } t \in T = \text{ a range for } EF, \\ &= M(X, Z), \text{ the model MACCS,} \\ f_x(x) &= \text{probability distribution of } X, \\ f_y(y) &= \text{probability distribution of } Y(t) \text{ at} \\ &\quad \text{a specific but arbitrary value of } t. \end{aligned} \tag{1}$$

Strictly speaking, for each set $\{t_1, t_2, \cdots, t_m\}$, the set $\{Y(t_1), Y(t_2), \cdots, Y(t_m)\}$ has a joint distribution. However, it is sufficient for our purposes to examine the distributions of $Y(t)$ for each t separately. In the notation we suppress the dependence of f_y on t.

We follow an *ad hoc* screening procedure that resembles what one might do when selecting a subset of independent variables in a step-up regression analysis. Namely, we iteratively run MACCS at a sample of input values and examine input and output values to select one or more "important" inputs. Those inputs designated as important are fixed at nominal values and the steps are repeated until variability in the output falls below a threshold. Finally, we examine the cumulative effect of the set of important inputs over the entire range of input values, not just at nominal values. We now discuss the two elements of the sequential procedure, the input sampling procedure and the indication of importance.

INPUT SAMPLING

The input sampling method is a variation of Latin hypercube sampling (McKay, Conover and Beckman, 1979) with independent replications. In an LHS of size k, the range of each input is divided into k intervals of equal probability content. One value is selected from each interval according to the input's conditional probability distribution. Values across inputs are matched at random and without replacement to form k input vectors. In the variation, the probability midpoint of each interval, rather than a sampled value, is used. As a result, an independently replicated sample uses the same values for

each input but matches them with different values across inputs. If we denote the number of replicated samples by r, then the total sample size is $n = r \times k$. The reason this type of design was chosen is to accommodate estimation of the importance indicator described in the next section.

For the MACCS study we chose arbitrarily $r = 10$ and $k = 50$ giving $n = 500$ runs. It is very likely that we would have obtained similar results with $r = 5$, and, even, $k = 25$. Sample size requirements were not investigated. The first column of Fig. 1 shows $Y(t)$ for the 50 runs constituting the first LHS replicate within the 500 runs. The variability (uncertainty) in the output as the 36 inputs vary across the input space is apparent. The 81 values of t in this study have been arbitrarily labeled 1, 2, and so forth.

IMPORTANCE

Interest lies in importance of inputs relative to uncertainty in the output. Assuming a suitable definition of importance is found, one could try to determine the importance of each input separately, or try to identify most important subsets of inputs of size 2, 3 and so forth. For this study, we look at the simple case of trying to find a subset of the 36 inputs which accounts for essentially all of the variability in Y.

Suppose we have a partition of inputs into two sets, $X = S_x \cup S_x^c$. Upper case S_x means a subset of p inputs and lower case s_x means the numerical values of the p inputs.

$$\begin{aligned} S_x &= \{X_{i_1}, X_{i_2} \cdots, X_{i_p}\} \\ &= \text{a subset of } p \text{ inputs.} \\ s_x &= \{x_{i_1}, x_{i_2}, \cdots, x_{i_p},\} \\ &= \text{numerical values of the } p \text{ inputs.} \end{aligned} \tag{2}$$

If S_x effectively identifies important inputs, then the family of conditional distributions $f_{y|s_x}$ indexed on the numerical values of the inputs in the subset S_x will be widely dissimilar. (See, for example, the right side of Fig. 2.) On the other hand, if S_x contains only unimportant inputs, the family of conditional distributions $f_{y|s_x}$ will be similar among themselves and to the marginal distribution of the output, f_y. (See, for example, the left side of Fig. 2.) One motivation for this approach comes from the following consideration. If Y depends only on S_x, then it is stochastically independent of all the other inputs, S_x^c. In that case, S_x^c would be clearly a set of "unimportant" inputs and $f_y = f_{y|s_x^c}$ for all numerical values of the inputs in S_x^c. Realistically, though, importance is not an either-or attribute.

The importance of S_x is related to degree of dependence, in the probabilistic sense, between Y and the subset of inputs S_x. Although there is no universally accepted, unique measure of dependence, one can begin by comparing the distribution f_y to the family of conditional distributions $f_{y|s_x}$ through the popular variance formula (Parzen, 1962)

$$V[Y] = V[E(Y \mid S_x)] + E[V(Y \mid S_x)]\,. \tag{3}$$

The term on the left side of Eq. 3 is a property of f_y. The inner expectations of the terms on the right side are properties of $f_{y|s_x}$. They represent the mean (E) and variance (V) of the conditional distribution $f_{y|s_x}$. Finally, the outer expectations (V and E) are with respect to the probability distribution f_{s_x} of S_x.

SCREENING

Eq. 3 can be used to form the basis of a screening process where inputs are identified, individually, as potentially important. McKay *et al.* (1992) used the quantity

$$\lambda_j = \frac{V[E(Y \mid X_j)]}{V[Y]} \tag{4}$$

as an importance indicator for input number j. An equivalent indicator

$$I_j = \sqrt{V[Y] - E[V(Y \mid X_j)]} \tag{5}$$

was used by Hora and Iman (1986) and Iman and Hora (1990).

Because of the sampling design used, λ_j can be estimated in a straight forward manner. Each input X_j is represented in the sample by k distinct values repeated r times. For each input X_j, we can label the n output values by y_{st} with $s = 1, 2, \cdots, k$ corresponding to the k distinct values of X_j, and $u = 1, 2, \cdots, r$ corresponding to the r times each value is repeated. Now, we write the common analysis of variance sum of squares partition

$$\sum_{s=1}^{k}\sum_{u=1}^{r}(y_{su} - \overline{y})^2 = r\sum_{s=1}^{k}(\overline{y}_s - \overline{y})^2 + \sum_{s=1}^{k}\sum_{u=1}^{r}(y_{su} - \overline{y}_s)^2 \tag{6}$$

$$\text{SST} \;=\; \text{SSB} \;+\; \text{SSW}$$

where

$$\overline{y}_s = \frac{1}{r}\sum_{u=1}^{r} y_{su} \text{ and } \overline{y} = \frac{1}{k}\sum_{s=1}^{k}\overline{y}_s \,.$$

In the usual manner, $V[Y]$ is estimated by the sum of squares total (SST) divided by $r \times k - 1$, and $V[E(Y \mid X_j)]$ is estimated by the sum of squares between (SSB) divided by $k - 1$. Thus, we see that the usual

$$R^2 = \text{SSB} \,/\, \text{SST} \,. \tag{8}$$

is proportional to a ratio of estimators of the two components of variance. That is, the importance indicator can be estimated by

$$\widehat{\lambda_j} = R^2\left(\frac{rk - 1}{k - 1}\right) . \tag{9}$$

Eq. 9 shows that one can use R^2 from sample data as an indicator of importance in place of $\widehat{\lambda_j}$. The probability distribution of R^2 depends on the true distribution of Y. However, if Y is approximately normally distributed and independent of X_j, then R^2 has, approximately, a beta distribution that depends on r and k. Thus, percentage points from the beta distribution might be used for guidance in evaluating the observed size of R^2. An interpretation of R^2 as a measure of degree of stochastic dependence needs to be researched. For now, we point out the obvious: if Y depends exclusively of X_j, then R^2 attains its maximum value of 1. Also, R^2 can be used as an indicator for importance for both individual inputs and subsets of inputs.

We calculate R^2 with both original and rank transformed output values. The rank transformation seems to have advantages for screening when some of the output values appear as outliers.

A SEQUENTIAL PROCEDURE

From many possibilities, we present here a simple, sequential procedure for building S_x which can be used to display the effect of inputs progressively. In a sequence of steps, the output is computed for a sample of input values where the number of inputs fixed becomes progressively larger. For the first step, no inputs are fixed, all 36 inputs vary, to produce representative output traces $Y(t)$ and $R^2(t)$ for each input in the first column of Fig. 1. For the second column of Fig. 1, 9 of the inputs are fixed at their nominal values and the remaining 27 assume the same sample values as in step 1. The spread in output values is noticeably reduced by fixing those 9 inputs. For the final column of Fig. 1, 16 of the 36 inputs are held fixed at their nominal values. At each step, additional inputs to fix are selected according to values of R^2.

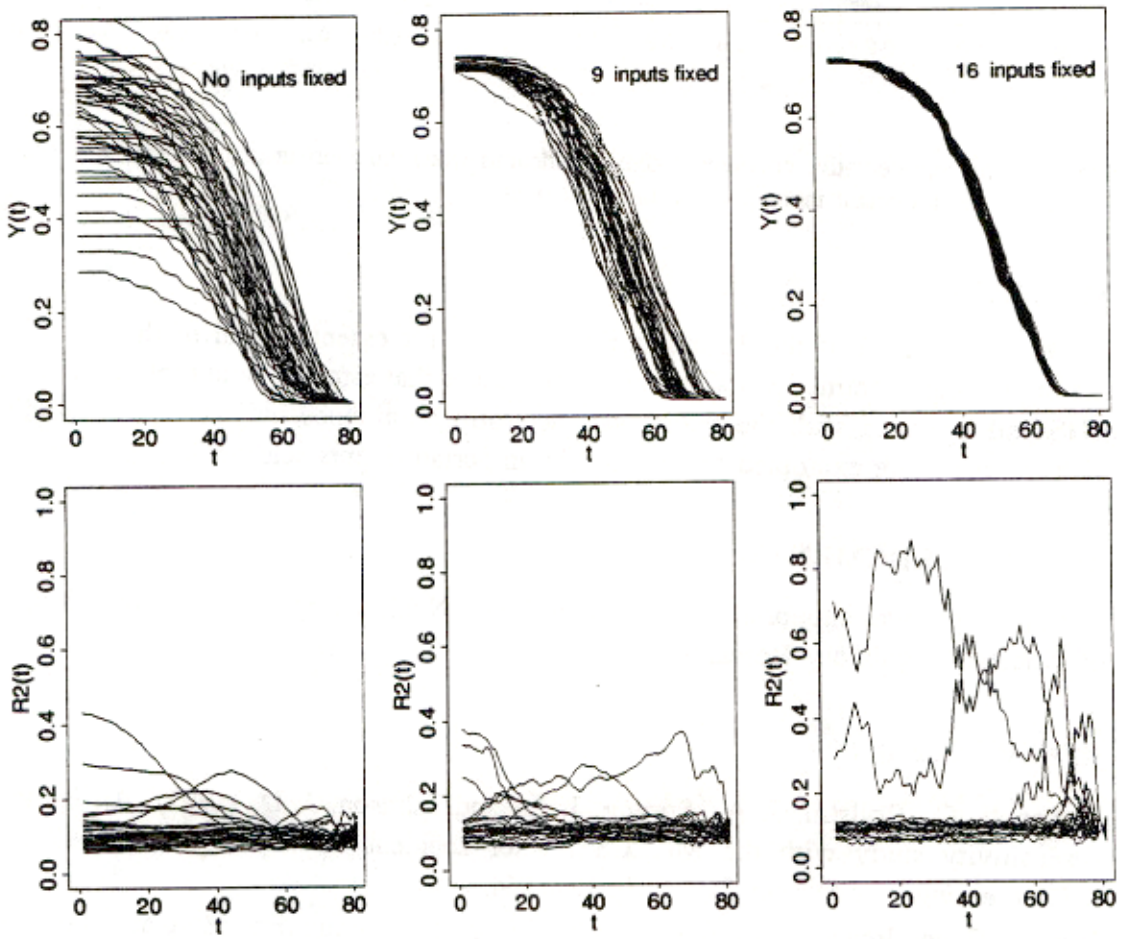


Figure 1. Representative $Y(t)$ and $R^2(t)$ for three steps

VALIDATION

Figure 1 indicates that fixing the 16 inputs in S_x at their nominal values greatly reduces variability in the output. To understand more fully the effects of the inputs in S_x and of the 20 unimportant inputs in S_x^c, we display two sets of probability distributions in Fig. 2 for $Y(t=1)$. It is important to note the difference in vertical scales in the figure. The left side gives 50 conditional density functions $f_{y|s_x^c}$ where the unimportant inputs take on 50 representative, fixed values. The similarity among these densities indicates how little the unimportant subset affects the distribution of $Y(t=1)$. On the right side of Fig. 2, the

large dissimilarity among the conditional density functions $f_{y|s_x}$, which correspond to 50 representative values of the important inputs, indicates the effects of the important subset.

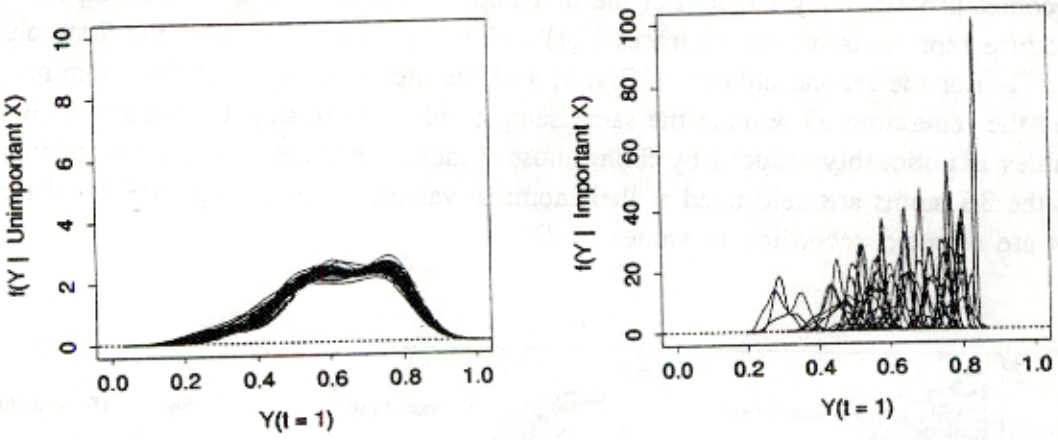


Figure 2. 50 representative conditional density functions when unimportant inputs are fixed, on the left, and when important inputs are fixed, on the right.

SUMMARY

A subset of 16 of the 36 inputs that accounts for essentially all of the variability in the output was identified via a sequential procedure that sampled with replicated, modified LHS and screened with the scaled variance-ratio importance indicator R^2. Conditional distributions were examined to validate the important inputs selected.

ACKNOWLEDGMENTS

This work was supported by the United States Nuclear Regulatory Commission, Office of Nuclear Regulatory Research.

REFERENCES

Helton, J. C., Rollstin, J. A., Sprung, J. L., and Johnson, J. D. (1992). An exploratory sensitivity study with the MACCS reactor accident consequence model. *Reliability Engineering and System Safety*, 36:137–164.

Hora, S. C. and Iman, R. L. (1986). A comparison of Maximum/Bounding and Bayes/Monte Carlo for fault tree uncertainty analysis. Technical Report SAND85–2839, Sandia National Laboratories, Albuquerque, NM.

Iman, R. L. and Hora, S. C. (1990). A robust measure of uncertainty importance for use in fault tree system analysis. *Risk Analysis*, 10(3):401–406.

McKay, M. D., Beckman, R. J., Moore, L. M., and Picard, R. R. (1992). An alternative view of sensitivity in the analysis of computer codes. In *Proceedings of the American Statistical Association Section on Physical and Engineering Sciences*, Boston, Massachusetts, August 9–13.

McKay, M. D., Conover, W. J., and Beckman, R. J. (1979). A comparison of three methods for selecting values of input variables in the analysis of output from a computer code. *Technometrics*, 22(2):239–245.

Parzen, E. (1962). *Stochastic Processes*. Holden Day, San Francisco, p. 55.

UNCERTAINTY AND SENSITIVITY ANALYSIS OF EARLY EXPOSURE RESULTS WITH THE MACCS REACTOR ACCIDENT CONSEQUENCE MODEL

J. C. Helton,[1] J. D. Johnson,[2] M. D. McKay,[3] A. W. Shiver,[4] J. L. Sprung[4]

[1] Arizona State University, Tempe, AZ 85287
[2] GRAM, Inc., Albuquerque, NM 87112
[3] Los Alamos National Laboratories, Los Alamos, NM 87545
[4] Sandia National Laboratories, Albuquerque, NM 87185

INTRODUCTION

As a result of the extensive interest that exists in the assessment of the uncertainties in predictions made by reactor accident consequence models, a joint project has been initiated by the Commission of European Communities (CEC) and the U.S. Nuclear Regulatory Commission (NRC) with the following objectives: (1) to formulate a generic, state-of-the-art methodology for uncertainty estimation that is capable of finding broad acceptance, (2) to apply the methodology to estimate the uncertainties associated with the predictions of reactor accident consequence models, and (3) to better quantify and obtain more valid estimates of the uncertainties associated with reactor accident consequence models, thus enabling more informed and better judgments to be made in the areas of risk comparison and acceptability.[1]

An important part of this project will be the use of an expert review process to assess the uncertainties in variables used as input to reactor accident consequence models. Such reviews involve the participation of many individuals, require extensive organization, and as a result, are expensive. For the preceding reasons, the number of input variables that can be subjected to a formal expert review process is limited and is certainly substantially less than the several hundred variables that comprise the complete input to a reactor accident consequence model. As a result, the variables selected for a formal review must be carefully chosen so that necessarily limited resources (i.e., time, people, money) can be directed at the variables for which a reduction in uncertainty will result in the largest reduction in the uncertainty in model predictions.

In preparation for its participation in this project, the NRC is supporting a sequence of uncertainty/sensitivity studies[2-4] with the MACCS reactor accident consequence model[5-7] to identify the input variables that have the greatest impact on the uncertainty in predicted consequences. These variables will then be candidates for formal review in the joint CEC/NRC project. This presentation describes the uncertainty/sensitivity study conducted for early exposure results (i.e., for fatalities, injuries and doses due to radiation exposure incurred within seven days of a reactor accident).[2]

TREATMENT OF UNCERTAINTY

An uncertainty/sensitivity study for a reactor accident consequence model such as MACCS actually involves two types of uncertainty: stochastic uncertainty and subjective uncertainty. Stochastic uncertainty results when the system under study can behave in many different ways (e.g., many different types of weather are possible at the time of a reactor accident). Subjective uncertainty results from the existing state of knowledge with respect to the correctness of the assumptions used in an analysis (e.g., what is the appropriate dry deposition velocity to use for a particular combination of release characteristics and weather). Thus, stochastic uncertainty is a property of the system under study, and subjective uncertainty is a property of the analysts performing the study. The importance of maintaining a distinction between these two types of uncertainty has been emphasized by many authors.[8-13]

The ordered triple representation for risk proposed by Kaplan and Garrick[13] provides a useful conceptual model for maintaining this distinction. In this representation, risk is expressed as a set $\mathcal{R}$ of ordered triples of the form

$$\mathcal{R} = \{(S_i, pS_i, \mathbf{cS}_i), i = 1, 2, ..., nS\}, \tag{1}$$

where S_i is a set of similar occurrences, pS_i is the probability for S_i, $\mathbf{cS}_i$ is a vector of consequences associated with S_i, nS is the number of sets selected for consideration, and the sets S_i have no occurrences in common (i.e., the S_i are disjoint). This representation formally decomposes risk into what can happen (the S_i), how likely things are to happen (the pS_i), and the consequences of what can happen (the $\mathbf{cS}_i$). The information contained in the probabilities pS_i and consequence vectors $\mathbf{cS}_i$ are usually summarized in complementary cumulative distribution functions (CCDFs).

Subjective uncertainty enters when the computational reality of evaluating the risk representation in Eq. (1) must be addressed. In practice, evaluation of the expression in Eq. (1) requires extensive computation and, in turn, this computation requires many inputs. If these inputs are represented by a vector

$$\mathbf{x} = [x_1, x_2, ..., x_{nV}], \tag{2}$$

where nV is the number of such inputs, the representation in Eq. (1) becomes

$$\mathcal{R}(\mathbf{x}) = \{[S_i(\mathbf{x}), pS_i(\mathbf{x}), \mathbf{cS}_i(\mathbf{x})], i=1, 2, ..., nS(\mathbf{x})\}. \tag{3}$$

If $\mathbf{x}$ was known with certainty, $\mathcal{R}(\mathbf{x})$ could be evaluated and presented as the unambiguous outcome of the analysis. However, $\mathbf{x}$ is not known with certainty is most analyses.

The uncertainty in $\mathbf{x}$ is characterized by developing a distribution

$$D_j, \; j = 1, 2, ..., nV, \tag{4}$$

for each variable x_j in $\mathbf{x}$. These distributions describe a degree of belief as where the appropriate value to use for x_j is located given that the analysis has been structured so that only a single value of each variable x_j is required in the determination of the set $\mathcal{R}(\mathbf{x})$. Correlations and other restrictions between the x_j are also possible. The distributions developed for the x_j are characterizing subjective uncertainty as they indicate the possible

In the present analysis, stochastic uncertainty arises from the different types of weather that could exist at the time of a reactor accident. Further, subjective uncertainty arises from a lack of knowledge with respect to the appropriate value to use for each of the 34 variables listed in Table 1 (i.e., $nV = 34$ in Eq. (2)).

EXAMPLE RESULTS

This analysis uses a source term associated with internally-initiated accidents at the Surry Nuclear Power Station that was determined as part of the NUREG-1150 probabilistic risk assessments.[14-16] A NUREG-1150 source term was selected due to the wide interest in

Table 1. Imprecisely known variables sampled in analysis. The distributions and correlations used with these variables to characterize subjective uncertainty are listed in Table 5 of Ref. 2.

BUILDH	Reactor building height. Defines initial vertical height of plume. Range: 15 - 35 m.
BUILDW	Reactor building width. Defines initial horizontal width of plume. Range: 15 - 100 m.
CSFACTE	Cloudshine shielding factor for evacuees. Range: 0.9 - 1.
CSFACTN	Cloudshine shielding factor for nonevacuees. Range: 0.6 - 0.95.
CSFACTS	Cloudshine shielding factor for individuals who shelter. Range: 0.5 - 0.7.
CWASH1	Linear term in wet deposition model. Range: 3.1×10^{-5} - 3.1×10^{-4} h/mm s.
CWASH2	Exponent in wet deposition model. Range: 0.7 - 0.9.
DOSHOT	Projected seven day dose used to initiate hot-spot relocation. Range: 0.25 - 1.0 Sv.
EFFACA1	Early fatality hazard function alpha value for bone marrow exposure. Range: 2.5 - 5.5 Gy.
EFFACA2	Early fatality hazard function alpha value for lung exposure. Range: 8 - 12 Gy
EFFACA3	Early fatality hazard function alpha value for gastrointestinal exposure. Range: 10 - 20 Gy.
EFFACB1	Early fatality hazard function beta value for bone marrow exposure. Range: 4 - 8 Gy.
EFFACB2	Early fatality hazard function beta value for lung exposure. Range: 9 - 14 Gy.
EFFTHR1	Early fatality threshold dose for bone marrow exposure. Range: 1 - 2 Gy.
EFFTHR2	Early fatality threshold dose for lung exposure. Range: 4 - 6 Gy.
EIFACA1	Early injury hazard function alpha value for prodromal vomiting. Range: 1.5 - 2.5 Gy.
ESPEED	Evacuation speed. Range: 0.9 - 3.6 m/s.
EVFRAC	Fraction of population in emergency response zone (i.e., within 10 miles of reactor) that does not evacuate. Range: 0.005 - 0.05.
GSHFACE	Groundshine shielding factor for evacuees. Range: 0.3 - 0.7.
GSHFACN	Groundshine shielding factor for nonevacuees. Range: 0.2 - 0.75.
GSHFACS	Groundshine shielding factor for individuals who shelter. Range: 0.1 - 0.3.
PHS2T2	Time at which individuals are relocated if their projected dose exceeds *P2DOS1*. Range: 0.5 - 2 days.
P2DOS1	Projected seven day dose used to initiate normal relocation. Range: 0.05 - 0.5 Sv.
PROTINN	Inhalation protection factor for nonevacuees. Range: 0.2 - 0.8.
PROTINS	Inhalation protection factor for individuals who shelter. Range: 0.1 - 0.4.
SCLADP	Plume rise scaling factor for stability classes A through D. Range: 0.5 - 1.5.
SCLEFP	Plume rise scaling factor for stability classes E through F. Range: 0.5 - 1.5.
SCLCRW	Critical wind speed scaling factor. Range: 0.5 - 2.
TDELAY	Time from warning to start of evacuation. Range: 1.25 - 3.25 hr.
TIMHOT	Time at which individuals are relocated if their projected dose exceeds *DOSHOT*. Range: 0.25 - 1 day.
TTOSH2	Time from warning to start of sheltering. Range: 0.25 - 0.75 hr.
VDEPOS	Dry deposition velocity. Range: 0.003 - 0.03 m/s.
YSCALE	Scaling factor for sigma-y (i.e., horizontal dispersion). Range: 0.33 - 3.
ZSCALE	Scaling factor for sigma-z (i.e., vertical dispersion). Range: 0.423 - 3.81.

this analysis, a desire to use a source term from a published probabilistic risk assessment rather than one "invented" specifically for this uncertainty/sensitivity study, and recognition of the fact that this study is part of a process intended to lead ultimately to an assessment of the impact of consequence modeling uncertainty on NUREG-1150 results. A source term for internally-initiated accidents at Surry was selected because this particular performance assessment is often used to illustrate properties of the NUREG-1150 analyses. As this study addresses early health effects, a relatively large release must be considered; otherwise, there will be no early health effects. In particular, a source term due to fast-developing accidents associated with steam generator tube ruptures was selected (i.e., the source term SUR-11-3 in Table 3.4-4 of Ref. 14, which has the following release fractions: iodine ~ 0.47, cesium ~ 0.43, tellurium ~ 0.25, strontium ~ 0.07, ruthenium ~ 0.002, lanthanum ~ 0.006, cerium ~ 0.008, barium ~ 0.06). The evacuation timing for this source term results in the evacuees being caught under the plume. A late evacuating source term was chosen so that the effects of uncertain variables on evacuees could be observed. Although evacuation preceding a release is the typical situation in the NUREG-1150 analyses, this is not very interesting in a sensitivity analysis because the evacuees avoid exposure, and as a result, the effects of the uncertain variables cannot be observed. The full input files used with MACCS in this analysis are listed in Ref. 17.

The effect of subjective uncertainty in the 34 variables listed in Table 1 on MACCS predictions was assessed by generating a Latin hypercube sample[18,19] of size 100 from these variables according to their assigned distributions and then performing a MACCS calculation for each of the 100 sample elements. This produced 100 sets of risk results of the form shown in Eq. (3). As an example, the resultant distribution of 100 CCDFs for number of early fatalities is shown in the left frame of Fig. 1, which can be summarized with mean and percentile curves as shown in the right frame.

One possible way to perform sensitivity analysis on the CCDFs in Fig. 1 is by calculating partial rank correlation coefficients (PRCCs) or standardized rank regression coefficients (SRRCs) between the exceedance probabilities associated with individual

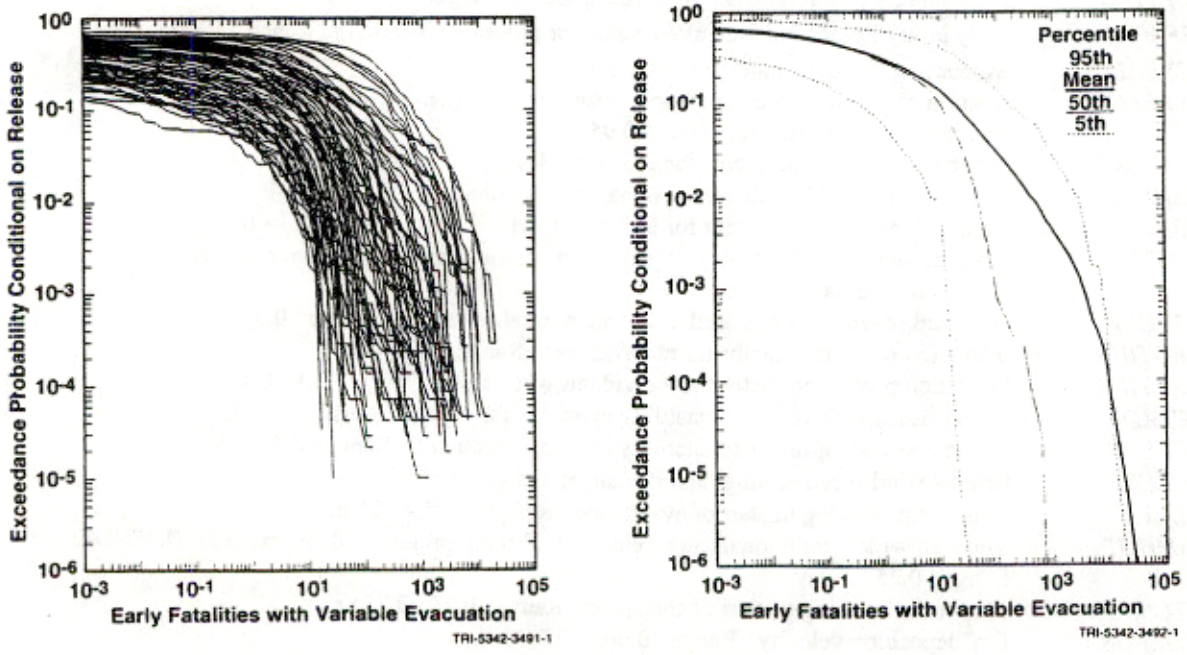


Figure 1. Distribution of CCDFs for number of early fatalities with variable evacuation (Figs. 2 and 7, Ref. 2). The descriptor "Variable Evacuation" refers to use of the variable *EVFRAC* in Table 1.

values on the abscissa and the individual sampled variables in Table 1.[20,21] The use of rank-transformed data often reduces the effects of nonlinear relationships and outliers. An example of such an analysis with PRCCs is presented in Fig. 2.

The individual CCDFs in Fig. 1 maintain a separation between consequence magnitude and consequence probability. However, each CCDF can also be reduced to a single mean result through the calculation

$$E[cS(\mathbf{x})] = \sum_{i=1}^{nS} pS_i(\mathbf{x})\, cS_i(\mathbf{x}), \tag{5}$$

where cS_i is an element of $\mathbf{cS}_i$. As an example, the preceding calculation reduces the distribution of CCDFs in Fig. 1 to the distribution of mean results in Fig. 3. Sensitivity analyses can also be performed for distributions of mean results of the form shown in Fig. 3. As illustrated in Table 2, one possibility is to use stepwise regression analysis.[22] In this example, analyses with logarithmically-transformed data and rank-transformed data[21] considerably outperformed the analysis with raw (i.e., untransformed) data.

ANALYSIS SUMMARY

Uncertainty and sensitivity analysis techniques based on Latin hypercube sampling, partial correlation analysis and stepwise regression analysis were used in an investigation with the MACCS model of the early health effects associated with a severe accident at a nuclear power station. The primary purpose of this study is to provide guidance on the variables to be considered in future review work to reduce the uncertainty in the important variables used in the calculation of reactor accident consequences. The effects of 34 imprecisely known input variables on the following reactor accident consequences were studied: number of early fatalities, number of cases of prodromal vomiting, population dose within 10 mi of the reactor, population dose within 1000 mi of the reactor, individual early fatality probability within 1 mi of the reactor, and maximum early fatality distance. When the predicted variables are considered collectively, the following input variables were found to

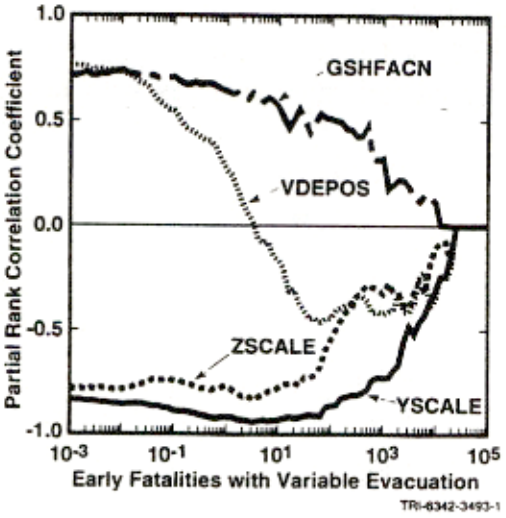


Figure 2. Partial Rank Correlation Coefficients for Probability that Specified Number of Early Fatalities with Variable Evacuation will be Exceeded (Ref. 2, Fig. 8).

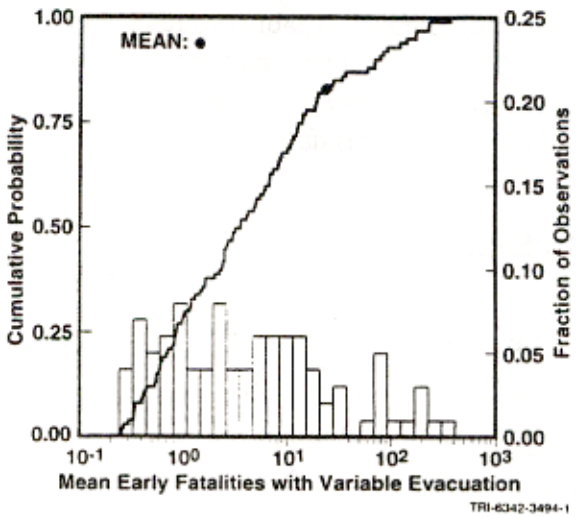


Figure 3. Distribution of Mean Number of Early Fatalities with Variable Evacuation (Ref. 2, Fig. 9).

Table 2. Stepwise regression analysis results for mean number of early fatalities with variable evacuation (adapted from Tables 6 and 28 of Ref. 2).

	Raw Data		Rank-Transformed Data		Log-Transformed Data	
Step[a]	Variable[b]	R^{2c}	Variable[b]	R^{2c}	Variable[b]	R^{2c}
1	*YSCALE*	0.16(-)	*YSCALE*	0.63(-)	*YSCALE*	0.64(-)
2			*ZSCALE*	0.70(-)	*ZSCALE*	0.71(-)
3			*EFFACA1*	0.76(-)	*EFFACA1*	0.76(-)
4			*ESPEED*	0.81(-)	*ESPEED*	0.82(-)
5			*GSHFACN*	0.87(+)	*GSHFACN*	0.87(+)
6			*EVFRAC*	0.89(+)	*TIMHOT*	0.89(+)
7			*TIMHOT*	0.90(+)	*EVFRAC*	0.90(+)
8			*CSFACTN*	0.91(+)	*VDEPOS*	0.91(-)
9			*SCLCRW*	0.92(-)	*SCLCRW*	0.92(-)
10			*VDEPOS*	0.92(-)		

[a] Steps in stepwise regression analysis.
[b] Variables listed in order of selection in stepwise regression analysis.
[c] Cumulative R^2 value with entry of each variable into regression model, with the "+/-" in parentheses after the R^2 value indicating whether the variable selected at that step has a positive (+) or a negative (-) regression coefficient.

be the dominant contributors to uncertainty: scaling factor for horizontal dispersion, dry deposition velocity, inhalation protection factor for nonevacuees, groundshine shielding factor for nonevacuees, early fatality hazard function alpha value for bone marrow exposure, and scaling factor for vertical dispersion. The following results were obtained in tests to check the robustness of the analysis techniques that produced the preceding set of variables: two independent Latin hypercube samples produced similar uncertainty and sensitivity analysis results; setting important variables to best-estimate values produced substantial reductions in uncertainty, while setting the less important variables to best-estimate values had little effect on uncertainty; similar sensitivity analysis results were obtained when the original uniform and loguniform distributions assigned to the 34 imprecisely known input variables were changed to left-triangular distributions and then to right-triangular distributions; and analyses with rank-transformed and logarithmically-transformed data produced similar results and substantially outperformed analyses with raw (i.e., untransformed) data.

REFERENCES

1. F. T. Harper, et al., these *Proceedings*.
2. J.C. Helton, et al., NUREG/CR-6135, SAND93-2371, 1994.
3. J.C. Helton, et al., NUREG/CR-6136, SAND93-2372, 1994.
4. J.C. Helton, et al., NUREG/CR-6134, SAND93-2370, 1994.
5. D.I. Chanin, et al., NUREG/CR-4691, SAND86-1562, Vol. 1, 1990.
6. H.-N. Jow, et al., NUREG/CR-4691, SAND86-1562, Vol. 2, 1990.
7. J.A. Rollstin, et al., NUREG/CR-4691, SAND86-1562, Vol. 3, 1990.
8. J.C. Helton, *Nucl. Tech.* **101**, 18-39 (1993).

9. J.C. Helton and R. J. Breeding, *Rel. Eng. Sys. Safety* **39,** 129-158 (1993).
10. IAEA, Safety Series Report No. 100, 1989.
11. G.W. Parry, *Rel. Eng. Sys. Safety* **23,** 309-314 (1988).
12. M.E. Paté-Cornell, *Nucl. Eng. Des.* **93,** 319-327 (1986).
13. S. Kaplan and B.J. Garrick, *Risk Anal.* **1,** 11-27 (1981).
14. R.J. Breeding, et al., NUREG/CR-4551, SAND86-1309, Vol. 3, Rev. 1, 1990.
15. R.J. Breeding, et al., *Nucl. Eng. Des.* **135,** 29-59 (1992).
16. U.S. NRC, NUREG-1150, 1990.
17. J.L. Sprung, et al., NUREG/CR-4551, SAND86-1309, Vol. 2, Part 7, Rev. 1, 1990.
18. M.D. McKay, et al., *Technometrics* **21,** 239-245 (1979).
19. R.L. Iman and M.J. Schortencarier, NUREG/CR-2624, SAND83-2365, 1984.
20. R.L. Iman, et al., NUREG/CR-4122, SAND85-0044, 1985.
21. R.L. Iman and W.J. Conover, *Technometrics* **21,** 499-509 (1979).
22. R.L. Iman, et al., SAND79-1472, 1980.

010 Computer-based Systems and Plant Models

Chair: P. Kafka, Gesellschaft fur Reaktorsicherheit (GRS)

Use of System Simulation to Support Automated Fault Tree Construction
A. Carpignano (Politecnico Torino, Italy)

Plant Specific PSA Supported and Enhanced by a Computer Based Failure Mode and Effect Analysis (FMEA)
H-P. Balfanz (TUV-Nord)

Identification of Components to Optimize Improvement in System Reliability
L. Painton (Carnegie Mellon U), J. Campbell (SNL)

An Introduction to Dynamic MPLD Model
Y-S. Hu, M. Modarres (U. Maryland)

USE OF SYSTEM SIMULATION TO SUPPORT AUTOMATED FAULT TREE CONSTRUCTION

Andrea Carpignano

Dipartimento di Energetica
Politecnico di Torino
Corso Duca degli Abruzzi 24
10129 Torino, Italy

INTRODUCTION

Informatic tools devoted to fault tree construction were proposed by several researchers since the '70s but most of them, in particular the first ones, were characterized by a drastic simplification of the system model to make the automatic treatment of the system description possible. In fact automatic construction, by traditional informatic programs, requires a simple and well-defined organization of the system description. Consequently it obliges one to work using a poor model of the system behaviour, e.g., a logical description of the physical process performed (flow *yes/no*, current *yes/no*) and presents a limited ability to investigate system configurations that are complex from the functional viewpoint (Carpignano and Poucet, 1993). A direct consequence of these problems is the low accuracy of the resulting trees. These allow conservative estimates to be made for the system reliability but rarely represent an accurate model of the system functioning or malfunctioning. Hence numerical results became broadly approximate (Hassan and Aldemir, 1990).

Several efforts have been made to improve these approaches and new perspectives have been offered by the recent developments of artificial intelligence. Researchers have refined their methods taking into account for the qualitative behaviour of the physical process performed by the system up to performing a real simulation according to the naive physics theory (Waters and Ponton, 1989; Rich and Venkatasubramanian, 1987). On the other hand, artificial intelligence offers now the expert system technology to overcome the inflexibility of traditional informatic tools in the management of the knowledge. This allows the treatment of a more general and exhaustive model of the system under analysis (Carpignano, Del Tin, 1993) that can take into account for all the aspects of a complex systems description: the structure (hardware), the behaviour (process evolution) and the functions (roles and goals of system and sub-systems).

When an analyst is working manually, he takes into account for all of the aspects mentioned above. Experience allows him to integrate all this kind of knowledge to direct the analysis towards the crucial goals of system management (functional aspects), performing a more detailed analysis of the sub-systems that are relevant to modify the process parameters of interest (behavioural aspects) and, obviously, following system layout and component structure (structural aspects).

All the automated approaches devoted to complex plants, available up to now, treats structural aspects correctly and extensively. Some of them also treat system behaviour in a qualitative way. Quantitative approaches are not available, and none takes into account for the functionality that is the most abstract level and which requires the management of a large amount of information regarding the system itself, the strategy used to operate the system and the context in which the system is inserted.

This paper does not treat the problem of the functional representation but intends to show how some results better than those available can be obtained by making more detailed the representation of the system behaviour according to a quantitative point of view.

This new approach applies the quantitative simulation of system components in order to establish how the system enlarges or quenches process parameter deviations with respect to boundary conditions and component states (failed or good). Hence it highlights if the branches of the tree built are representative of realistic or unrealistic scenarios. This assessment assures more accurate reliability models, e.g., fault trees, and better estimate of the system reliability. The functional aspects are still left to the analyst: he has to define the context in which the analysis has to be performed and can modify, interactively, component models in order to adapt them for the particular context.

THE STARS FAULT TREE CONSTRUCTOR

The new approach bores in the STARS environment (Poucet, 1990) and it is based on the introduction of a tool for simulation as a support for the logical constructor already available and hereafter briefly described. The constructor (XFTCON - Xwindow Fault Tree CONstructor) allows both the interactive or automatic approaches (Carpignano, 1993). It has been structured according to the expert system technology. The inference engine has been derived from the CAFTS algorithms (Poucet, 1983) while the knowledge support is offered by the STARS environment.

XFTCON works using a structural and behavioural model of the system. The behavioural model is local and qualitative: the "local" attribute means that a global behavioural model of the system is not available, but it is obtained by linking, according to system structure, the behavioural models that are available for each component. These models are expressed as a set of logical rules (IF-THEN) which describe how the component propagates the deviations of process variable, according to its control and its functioning or failure mode.

CLASS: *Motor_operated_valve*
IF from connection 2 veryhigh flow AND valve_opened THEN from connection 1 veryhigh flow
IF from connection 2 high flow AND valve_opened THEN from connection 1 high flow
IF valve_closed THEN from connection 1 verylow flow
IF from connection 3 low curr THEN valve_closed
c: $DefaultPos = ask_to_open
IF /close_rupture THEN valve_opened
c: $DefaultPos = ask_to_close ...

Figure 1. Qualitative behavioural model for a motor operated valve.

The process variable deviations are qualitative and can be split into several set points (e.g., *very_low*, *low*, *high*, *very_high*). An example of a logical/qualitative model for a valve is given in figure 1. Each rule can be constarined by one or more conditions (*c:$...*) that define the context in which the rule can be applied such as a particular system working phase or a particular component functioning mode. This is a way to introduce a sort of functional information during the compilation of the system model.

The inference engine performs the construction by propagating the top event through the system topology, according to component nominal (component is good) and failure models. The propagation is obtained by the backward chaining of rules that characterizes component behaviour. Some appropriate procedures have been developed to assure tree consistency, to cut logical loops and to check model conditions in order to evaluate which component rules are applicable in the given context.

A simple example of an application of this tool is shown in figure 2. The system, a heater, provides hot water at the node *C*. Line *BG* protects the pump against the interruption of the main flow. The system is manually driven. The pump is running. All the valves are opened. The top event consists of the production of low temperature water at the output of the heat exchanger (connection 2 of the component named "hex").

If component models are correct, the resulting tree is correct and conservative and can be directly analyzed to obtain system reliability and the Minimal Cut Set list. In any case the reliability estimate could be very approximate. The problem of approximate result is due to the poor treatment of the system behaviour. This aspect requires a more extensive discussion: an experienced analyst, that has to draw the same tree shown in the example, immediately recognizes the role or "function" of the pump minimum flow line *BG*. He knows that in general deviations in the minimum flow-line mass flow cannot significantly affect the main line mass flow. Thus he does not take into account for faults related to this secondary line and searches for the causes of the top event in the main flow line. The automatic constructor cannot recognize the different role of these two lines because it is not supported by a functional model of the system. Therefore it gives the same importance to both lines and the resulting tree is greater: more factors seem to be able to cause the top event even if this is not true in the real world. The analyst's interaction during the inference allows the adaptation of the model to the working context and hence can bring forth a better solution.

The next section shows how the behavioural model of the system can be refined to enable the automatic constructor to solve this kind of problem, avoiding the intervention of the analyst (at least in the simpler cases).

QUANTITATIVE SIMULATION TO SUPPORT FAULT TREE CONSTRUCTION

Although a functional model of the system is not available, good indications about the system can be obtained using a refined behavioural model. In particular a quantitative behavioural model is able to simulate the system and hence it can evaluate how the system reacts to process variable deviations, due to component faults or boundary stresses. This information is very useful in fault tree construction because it drives the constructor to the subsystems that are able to modify, in a significant way, the process evolution, and neglects the analysis of the portions of the system that are able to absorb its failure effects.

The main idea on which this approach is based is the following. Each branch of the fault tree in practice is representative of a scenario. Quantitative simulation is able to help the fault tree constructor to recognize if the new scenario created is realistic or not, checking if the scenario leads to the top event under study. In particular, it checks if the deviation in the process parameter mentioned in the top event is significant or negligible from a technical viewpoint. In the first case the branch is kept and the constructor continues its development.

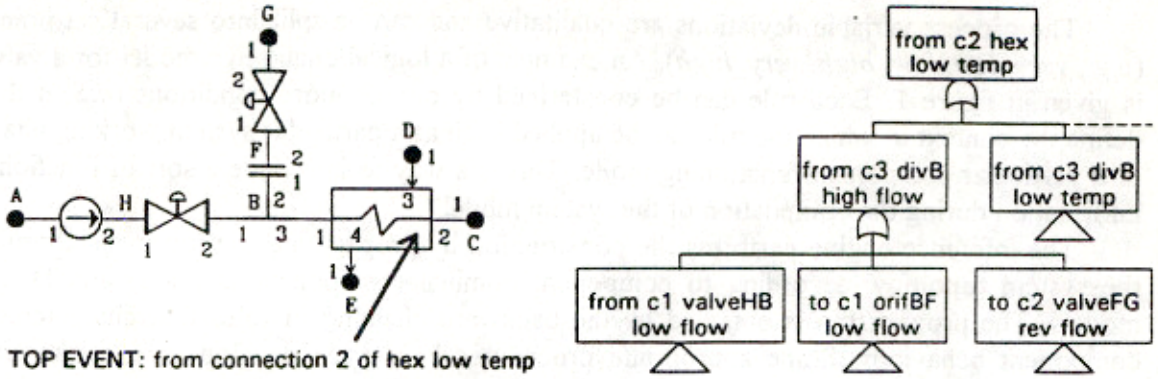


Figure 2. Application of the STARS XFTCON tool.

Otherwise the branch is cut, and a new one is investigated. The simulator runs in parallel with the logical constructor. The constructor creates a new branch and simultaneously the simulator checks it and decides if it has to be retained or not.

The decision about the importance of the parameter deviation and it propagation through the system requires a quantitative simulation approach. Other methods, based on the qualitative physics, were investigated in the past, but they presented a lot of problems related to the uncertainty in qualitative algebra. These difficulties causes the exponential explosion of the problem (Rich, Venkatasubramanian, 1987; Waters, Ponton, 1989).

This approach requires the upgrade of the system models in order to introduce the description of their quantitative behaviour. This is made by creating, in the knowledge base, a new component attribute containing the quantitative transfer functions that describe how the component propagates parameter deviations according to its functional or failure state and its control. Obviously the model can assume several levels of detail according to the requirements of the analysis and the complexity of the system. Moreover each component has to be characterized by other attributes containing the values that process parameters assume in normal operation: in the absence of system failures (different operational phases can be characterized by different values). One must also to incorporate the constraints that are important to bound parameter deviations in order to maintain the physical integrity of the system. These threshold values will be used to evaluate if a scenario is realistic or not.

To start the check of the construction, the analyst has to calibrate the meaning of the logical top event. This can be done by the introduction of the "adaptive condition" that explains in quantitative terms the top event (e.g., *low temp* => $T < 234\ K$). The inference engine propagates this condition through the system using the component transfer functions, following the propagation of the logical constructor. The propagation of the adaptive condition introduces new quantitative constraints, in other nodes of the system, that have to respect the acceptable range for process parameters as indicated in component models (threshold values).

As an example, the heater already mentioned can be considered (figure 3): the analyst starts the construction by introducing the top event (*from connection 2 of hex low temp*) and the related adaptive condition ($T2hex<353\ K$). The constructor searches for the rules which can be applied in the heat exchanger qualitative/logical model and finds the rules

IF from connection 1 high flow THEN from connection 2 low temp
IF from connection 1 low flow THEN from connection 2 low temp.

These rules imply that the "*low temp*" can be caused by a "*high flow*" or a "*low temp*" in the input at the tube side of the exchanger. The above rules allow the introduction in the tree, below the top event, of an OR gate linking the two events mentioned above. Now each event has to be checked.

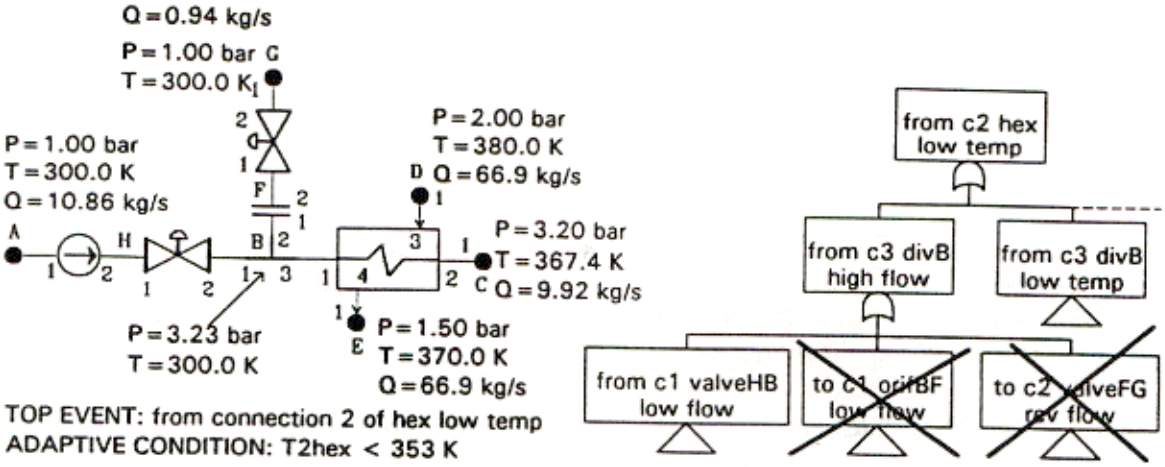


Figure 3. Application of the constructor supported by the simulator.

To check the first one the simulator propagates the adaptive condition through the hex component, using the transfer functions that link the temperature *T2* with the mass flow *Q1*, obtaining a new constraint or adaptive condition for *Q1* (e.g., *Q1 > 12.5 Kg/s*). This constraint is then transferred to the related field variable, the pressure, obtaining *P > 3.24 bar*, under the assumption that the output pressure is nominal and all the shell side of the heat exchanger works correctly. This last assumption is correct and it is not restrictive because we are simulating the scenario shown by the fault tree and it does not foresee any fault or deviation for these system legs. Now the simulator is ready to check if the constraint found for the pressure at the input of the heat exchanger is compatible with the threshold limits set during the system modelling for the heat exchanger. If the pressure value is acceptable the event "*high flow*" can be retained; otherwise it has to be rejected. The same procedure has to be performed for the "*low temp*" event and all the events that are recursively generated by the logical constructor.

The main problems of concern are the check of events belonging to *AND* operators and the combination of the rules rejected because the scenario was not realistic. *AND* operators introduce some trouble because, in this case, the adaptive condition has to be propagated and split onto two or more other variables. This is the case of the rule

IF from connection 1 low flow AND from connection 1 high temp THEN from connection 2 high temp

for which the constraint related to *T2* has to be distributed on the process parameters *T1* and *Q1* (or *P1*). The problem of fault tree completeness arises again when some scenarios are rejected because, if two or more of them that are independent (*OR* logic) are rejected in the same location of the tree, there is the possibility that their intersection (*AND* logic) gets through the check. In fact, in this case, the adaptive condition is split onto two or more new process variables and becomes less restrictive (Carpignano, 1993).

A prototype tool that applies the above methodology has been implemented in the STARS environment. Using it, the heater shown in figure 3 has been studied with good results. The constructor, using the support of the simulation tool, is able to obtain the same result as the expert does manually, without any intervention of the analyst during the inference. Consider the following example. The propagation of the adaptive condition allows the simulator to recognize that a deviation of the temperature at the output of the heat exchanger, of the declared extent cannot be generated by a deviation of the process parameters in the pump minimum flow line if there is not an extremely high reversed flow in that line. However this high flow can be justified only by an extremely high pressure that is

not compatible with the integrity of the system. Therefore the hypothesis is rejected and the related logical gate in the tree is pruned.

CONCLUSIONS

The introduction of a behavioural quantitative model to support automated fault tree construction creates new possibilities from which more accurate trees may be built and better approximations in system reliability evaluation may be obtained.

The sample application shown is very simple. In this particular case the expert system obtains the same result as the experienced analyst. The approach offers very interesting prospects for complex situation as well. In these cases the agreement is not as good but it is better than in absence of the simulation tool. Moreover the interactive stamp of the approach allows the intervention of the analyst to be at a new and more "intelligent" level, obtaining better results.

The method allows the possibility dynamic systems (e. g., tank filling or heat heap), up to now left at the analyst intervention, to be treated as well. This can be done by introducing the solution of differential transfer equations, in order to relate integral parameters, such as levels or temperatures, with the mass flows or the heat fluxes.

Another very interesting aspect, which has been tested, is the possibility of using the tool in order to build "constrained trees" that can be very useful in other phases of safety analysis or as diagnostics. The experiments performed show clearly how the tree results to be modified in consequence of changes in the value set for the adaptive condition.

Interesting development of the work could be the link of this approach with a functional model of the system in order to automate the management of system operating phases and to assist the analyst during the selection of top events and adaptive conditions.

ACKNOWLEDGMENTS

Thanks are due to Andre Poucet who gave me essential support during all phases of the work and to Stefan Scheer for his contribution during the implementation of the simulation prototype.

REFERENCES

Carpignano, A., 1993, "Simulazione del Comportamento Fisico dei Sistemi per una Modellizzazione Affidabilistica più Accurata", PhD Thesis, Politecnico di Torino, Italy.

Carpignano, A., and Del Tin, G., 1993, Object oriented plant models to support design and management, Proceedings of the conference "NUCLEAR ENERGY IN CENTRAL EUROPE: Present and Perspectives", June 13-16th 1993, Portoroz, Slovenia.

Carpignano, A., and Poucet, A., 1993, Computer assisted fault tree construction: a review of methods and concerns, *Reliab. Eng.*, in press.

Hassan, M., and Aldemir, T., 1990, A data base oriented dynamic methodology for the failure analysis of closed loop control systems in process plants, *Reliab. Eng.*, 27:275.

Poucet, A., 1983, "Computer Aided Fault Tree Synthesis", EUR 8707 EN, Commission of the European Communities. Ispra (VA), Italy.

Poucet, A., 1990, STARS: Knowledge based tools for safety and reliability analysis, *Reliab. Eng.*, 30:379.

Rich, S. H., and Venkatasubramanian, V., Model-based reasoning in diagnostic expert systems for chemical process plants. *Comp. Chem. Eng.*, 11:111.

Waters, A., and Ponton, J. W., 1989, Qualitative simulation and fault propagation in process plants, Chem. Eng. Res. & Des., 67:407.

Plant Specific PSA Supported and Enhanced by a Computer Based Failure Mode and Effect Analysis (FMEA)

Hans-Peter Balfanz, TÜV-Nord

Hamburg, Oct. 1993

Introduction

Today, plant specific PSA is a standard tool for reviewing NPP safety design and operational features.
The methodological approach of analysis is the top down procedure of Event and Fault tree analysis (ETA and FTA) by selecting the most critical plant incident events that can cause a core melt accident.
The advantage of this method is that the selecting process of the analysis deals only with those components that are relevant to the defined top event. This keeps the effort of analysing within reasonable boundaries.

The analysis results are such as

. Risk profile of plant safety features
. Weak point identification
. Ranking backfitting measures and safety issues
. Optimization of maintenance, test and operational procedures.

Adequate use of this analysis can strongly support plant staffs' work in respect of safety assurance.

Of disadvantage is the complexity of method: it cannot be used by non-PSA experts. So far, support of a PSA expert for handling a PSA in a form as currently documented is generally necessary.

To bridge this deficiency, improved computer-aided systems can help, so that non-PSA experts get familiar with the analysis.

A primary point of this task is the one of giving answers on the importance of each plant component and its functioning and to reveal hidden assumptions of analyses. The current PSA only give answers to such items that are explecitly modeled. But there are many items not modeled or explicitly shown in the analysis, so that the applicant receives no answer to these items.

The well-known Failure Mode and Effect Analysis (FMEA) can fill this gap, but it is a time-consuming process applying the analysis for some thousands of NPP components that have to be reviewed.

Computer-aided Safety Analysis and Information System - SAIS

SAIS is developed to support PSA use for plant staffs /1/. For this purpose, the SAIS computer package system contains both types of analyses: the top down process of ETA and FTA as well as the FMEA bottom up procedure (Fig. 1).

All analysis steps are backed up by additional explanations so as to reveal as far as possible the so-called hidden assumptions of analysis.

Based on these objectives, the SAIS system was built up from a great number of standardized data sheets for the purpose of describing every analysis step. In this system, the FMEA plays a key element of methodology.

The SAIS-structure is devided into six levels of analysis, whereby on each level unique functions of analysis are defined
(Fig. 1).

E: Initiating events as modelled in event trees of Level 1 PSA

F: Safety system functions (event tree functions) to be used for all event trees

S: System functions to be used in system train fault trees (macro-FT)

K: Component functions converted into component failure modes and modelled in component fault trees (micro-FT)

I: Incident events of components and transients through plant operation

P: Probabilistic input data based on data under item I.

The main elements of analysis are displayed in a set of scrollable tables (Page Editor) for at user's selection (Fig. 2).

In addition, all functional dependencies on initiating events via safety functions and system functions down to the component function level are stored in the unique data base of SAIS and can be identified at user's selection.

The corresponding data sheets to the analysis elements (see Fig. 2, lower part) offer descriptions of the system's elements and functional dependencies.

This structure has been developed according to the principles of PSA methodology and contains all elements of a PSA level 1 to be used for living PSA (see Fig. 1, lower part). The integrated PSA code is RISA+ /2/, which is linked to the SAIS data base as

well. The system can fundamentally be applied as an engineering tool with or without the PSA part.
The engineer-directed part of integrated data sheets is self-explanatory for the engineer.
In combination with PSA, the system enables the engineer to get more insight in the PSA methodology.

SAIS Methodology

The analysis procedure of SAIS as a whole corresponds with the conventional PSA methodology.
On system and component levels, however, the analysis approach in SAIS is much broader than generally applied in PSA.
In SAIS, a complete list of system functions for each system will be defined to cover all specified safety and operational tasks of a system. This information will be described in the data sheets of

SO: System description and
SS: System specification

and is stored in the SAIS data base.
Experience with SAIS application shows that this step of system analysis is not trivial, because identification of all safety tasks to be involved in a system design is generally not described in a unique plant documentation, so that it cannot easily be found.
For the reference plant of SAIS, in this case a PWR, the number of system functions varies between 5 functions of emergency diesel generator system and 20 functions of emergency core cooling system. On the system function level, each component function and component failure mode will be identified in the KS component data sheet, (Component specification) (Fig. 3).
Every correlation of system and component functions is identified in the KS-matrix by

u: direct correlation
m: indirect correlation
e: no correlation.

The user can explain each correlation in an extra KM data sheet (Failure mode and effect analysis). By this procedure all components of each system function are identified whether or not a component is modelled in the FTs.
On component level, the component items such as pump, motor, gear and the component-related connections to its support systems, are compiled in the KB-data sheets, e.g. to be used for failure event investigation.
The component's support systems, such as electric supply, component control equipments (e.g. part of reactor protection system) and component cooling systems, are compiled in the KI-data sheets (component interfaces), e.g. to be used for FTA (see Fig. 2).

The correlations of electric and control supply equipments with each component function are also recorded in the computer files of plant documentation and are used here to verify the correct and completeness of component FT-models.

This part of analysis of system and component levels qualifies the PSA and enables the non-PSA expert, e.g. the plant staff, to understand what is and what is not modelled in the plant-specific PSA. The experience of SAIS application by plant staffs shows the tendency towards giving more notes and explanations of system and component correlations than commonly done in a conventional PSA. To this application the SAIS data sheets will be used as a note-book in storing all safety-relevant information currently available.

Discussing this application with the plant personnel will result in that much more plant-based experience will be integrated in the PSA process and will enhance the PSA modells with regard to completeness and realism.
The computerized data base of SAIS stores all data and information so as to enable the user to handle the huge amount of information (see Fig. 2).
The best data support will be obtained if the data base is directly linked to the plant data base of the system and component documentation as far as it is available at the plant.

In our application we received from the NPP computer data files of several thousands of components with related technical data. This data set could automatically be transfered in the SAIS data base. Approximately 1000 components were identified for their use in the FT models and will support failure event evaluation and reliability data assessment.

The other components with the related technical data are also stored in the database and are latently available for use, e.g. to support the question, whether or not the component is safety-relevant.

Conclusions

The main results of SAIS applications are:

1. The effort involved in filling-in the comprehensive set of data sheets describing the component and system features and the linkages to the PSA models is much more extensive as compared to conventional PSA development. However, once this basic information will be available the work expenditure of continuing PSA development will be substantially smaller.

2. The PSA methods used in SAIS in connection with the stored technical information result in a strong increase of PSA quality in respect of modelling plant equipment and accident phenomena. The SAIS data sheets can be used as a note book for storing all safety-relevant information currently available.

3. For Living PSA application and PSA review, the models in SAIS are more self-

explanatory than it is known from other PSA applications, e.g.:

- the PSA expert is used to and can start reviewing PSA models right at the initiating event level and move top down through the PSA logic into the component and subcomponent levels.

- the plant engineer and the system designer are used to and can start at the component level and move up into the system functions and PSA logic (Fig. 1).

For these applications SAIS contains much more technical information than currently available in a PSA. So far, the use of SAIS is not restricted to PSA application, it can be used in the current safety investigation process of plant operation and it stimulates technical specification improvements.

Further system developments are intended, such as building up a PSA-based analysis structure of the reactor protection system, Tech.Spec. improvements and a stronger intergration of accident analysis parameters, assumptions and results.

References

1. H.-P. Balfanz, S. Dinsmore, U. Hussels, W. Musekamp and Stüber "Safety analysis and information system (SAIS - A living PSA computer system to support NPP- safety management and operators" Reliability Engineering and System Safety, 38, 181-191, (1992)

2. RISA+ Reference Manual, RISA-GmbH, Berlin, Germany, June, 1993.

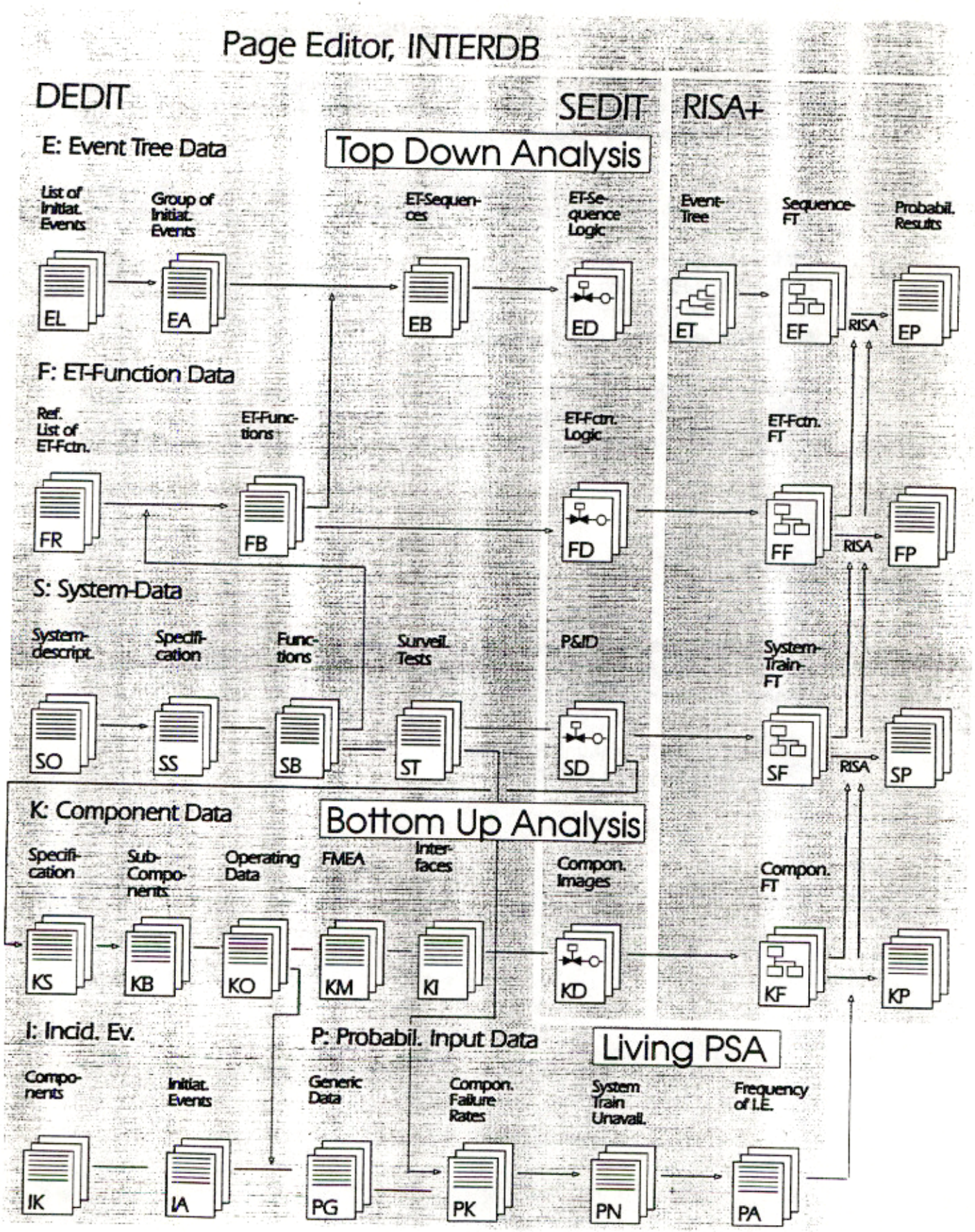


Fig. 1: SAIS-Structure

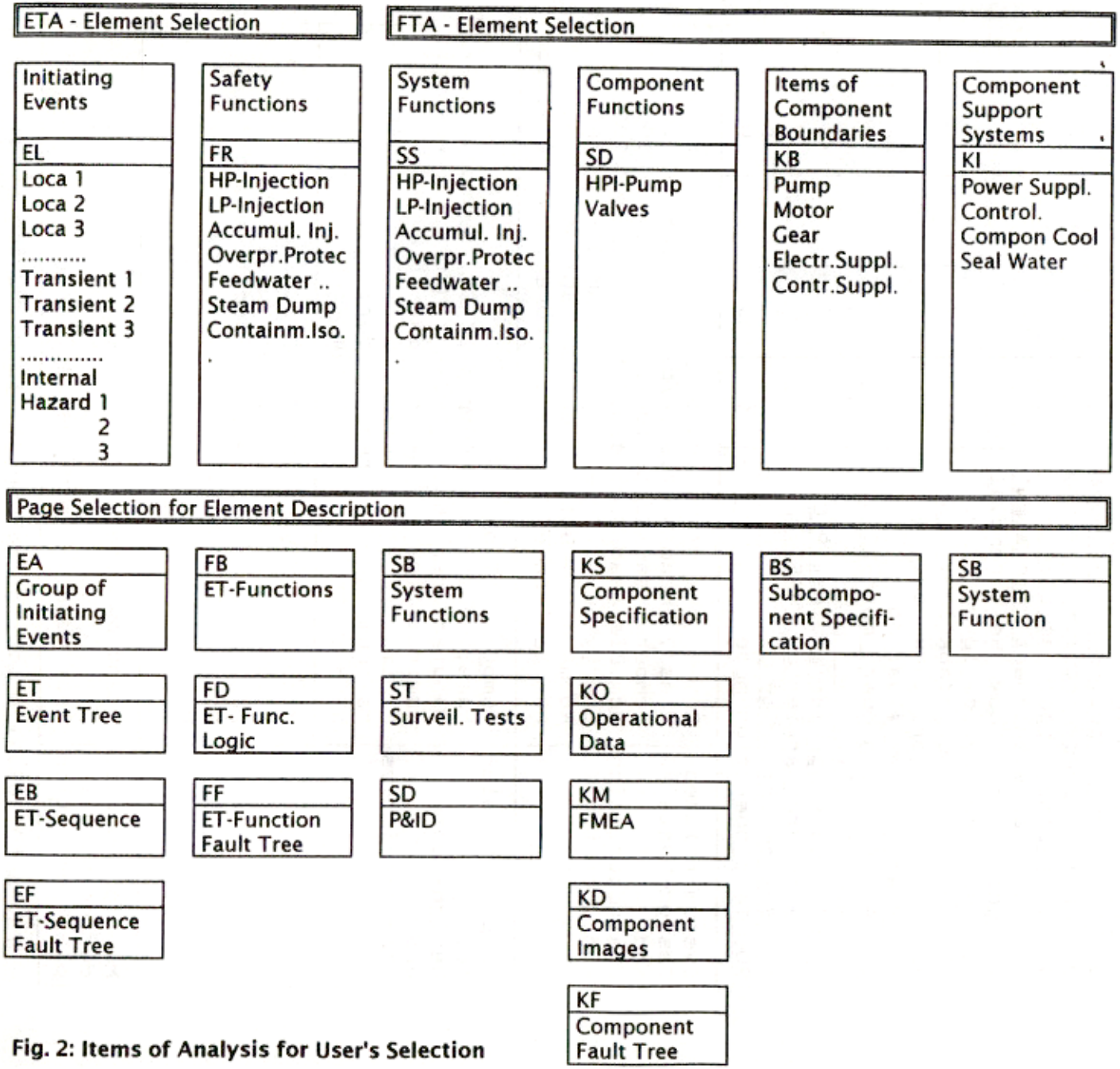


Fig. 2: Items of Analysis for User's Selection

S A I S	Component- Specification		Pumps		KS DP
KBR	05TH15D001	06TH25D001	07TH35D001	08TH45D001	

Name: High Pressure Injection Pump
KG-Alphanum.: TH(15-45)D001 FB-Bezeichn.: HPSI Pump

Systemcode: TH
Emergency Core Cooling System

Systemfunctions TH01 - TH20	Component Functions start A5	operate A7	swit. off A6	remai sw.of F3	Integrity M3	
01. High pressure injection	U	U	E	E		
02. HPSI shut off			U	U		
03. Accumulator injection						
04. Accumulator shut off						
05. Low pressure injection			E	E		
06. L.P.sump circul. + heat removal			E	E		
07. HP + LP sump circul.+ heat rem.	U	U	E	E		
08. Containment isol. at LOCA						
09. External event heat removal						
10. operat. shut down Heat removal				M		
11. Heat rem. by low level of P.C.				M		
12. Fuel el. stor. tank cool. 18/48				E		
13. Fuel el. stor. tank cool. 10/40				E		
14. Reactor room floating						
15. Purification oper. mode 20/30						
16. ACCU refill	U	U				
17. Pressure barrier against P.C.						
18. Pressure barrier ag. HPSI oper.				M		
19. System integrity				E		
20. Test operation mode	U	U	U	U		

System-related Design- Data and Characteristics and Location

		refere.
QA Head/Suct.side :	B/2 / B/2	2.TH01
Press. Head/Suct.side/bar:	145 / 50	2.TH01
Temper. Head/Suct.side/°C :	100 / 100	2.TH01
Nom.Dia.Head/Suct.side DN :	125 / 200	2.TH01
Energy Supp. Type	: AM 01-EN-DZACAPB	5.A.AKB
Room : B0112 B0133	B0153 B0165	2.TH01
Pump on socle- h. .... cm/overflow protection		

Component-related Design- Data and Characteristics

Pump Type:		
Name: Centrifugal Pump / 13-St./hydrodyn.Seal.		
Manufacturer: BALKE_DUERR Material: Austenit		
Nominal flow kg/s / bar:	/	
Minimum flow kg/s / bar:	4 / 110	1.TH01
Maximum flow head bar:	110	3.4.2.8
NPSH / m :		
Motor Type: 1RN7569-2XZ80Z		5.A.AKB
Name: Motor with Air/Water Cooling		
Manufacturer: Siemens acc.time/sec:		5.A.AKB
Nom.-power kW: 620 Nom.Volta.KV: 10		5.A.AKB
Nom.-Current A: 43 cos. Phi: 0,89		5.A.AKB

Mode of operat. during normal plant operation

stand by mode

Test mode: 10 min/Test = 2 h/a

TÜV-N. 07.05.91 designed: Wohlst. 12.02.92 approved:
Revision: 0 modified: approved:

IDENTIFICATION OF COMPONENTS TO OPTIMIZE IMPROVEMENT IN SYSTEM RELIABILITY

Laura Painton

Engineering and Public Policy
Carnegie Mellon University
Pittsburgh, PA 15213

James Campbell

Sandia National Laboratories
Manufacturing Systems Reliability
Albuquerque, NM 87185

INTRODUCTION

The fields of reliability analysis and risk assessment have grown dramatically since the 1970s. There are now bodies of literature and standard practices which cover quantitative aspects of system analysis such as failure rate and repair models, fault and event tree generation, minimal cut sets, classical and Bayesian analysis of reliability, component and system testing techniques, decomposition methods, etc. In spite of the growth in the sophistication of reliability models, however, little has been done to integrate optimization models within a reliability analysis framework. That is, often reliability models focus on characterization of system structure in terms of topology and failure/availability characteristics of components. A number of approaches have been proposed to help identify the components of a system that have the largest influence on overall system reliability. While this may help rank order the components, it does not necessarily help a system design team identify which components they should improve to optimize overall reliability (it may be cheaper and more effective to focus on improving two or three components of smaller importance than one component of larger importance). In this paper, we present an optimization model that identifies the components to be improved to maximize the increase in system MTBF, subject to a fixed budget constraint. A dual formulation of the model is to minimize cost, subject to achieving a certain level of system reliability.

Although the optimization model can be generalized, it is presented in the context of a specific reliability analysis software program called RAMP (Reliability Analysis and Modeling Program). RAMP is PC based software designed for reliability modeling of repairable and non-repairable systems [Campbell et al., 1993]. Block diagram models or fault trees are used to model complex systems by breaking down the system into its individual failure modes or basic events. Results of model analysis include system reliability (for non-repairable systems) or system mean time between failures (MTBF), mean time to repair (MTTR), and availability (for repairable systems). RAMP was developed by Sandia

National Laboratories and has been applied to manufacturing equipment, weapons systems, medical equipment, and automotive subsystems.

RAMP provides basic uncertainty and sensitivity analysis capabilities to rank component failure modes in terms of their contributions to variability in system performance and contributions to system unreliability. However, experience with industrial applications has shown that simply ranking reliability problem areas is not enough. Design engineers need specific guidance on how much reliability improvement is needed in each design area to meet a system reliability objective for minimum effort.

OPTIMIZATION FORMULATION

We developed an optimization model to help a system design team identify which components should be improved to optimize overall system reliability. Note that this is a difficult optimization problem. There are distributions on the input failure rates to RAMP, and RAMP produces a distribution on output measures such as system MTBF and availability by repeatedly sampling the input distributions using Latin Hypercube sampling. Thus we are faced with a problem in which we want to optimize an output measure when both the inputs and outputs are represented by distributions, not point values. Further, the output often cannot be easily represented as an analytic function of the inputs.

One of the first problems, therefore, is defining what exactly one wants to optimize. The objective function to be optimized will be a function of one or more output distributions of interest. For example, if the output measure is MTBF, the objective may be to maximize the expected value of MTBF, or the probability that MTBF is greater than 500 hours, or the 5th percentile of the MTBF distribution. Note that the uncertainties in the input failure rates imply that some type of Monte Carlo or Latin Hypercube sampling will have to be performed at each system configuration examined. This increases the computational needs of the optimization no matter which method is used to solve it.

Traditional optimization methods include gradient descent techniques, Newton's method, and various types of mathematical programming such as linear, non-linear, mixed-integer, etc. These algorithms usually act in an iterative scheme, with one point of the solution space evaluated, then derivative and possibly second derivative information being used to determine the next direction of search. In a stochastic framework, the function and constraint evaluation would occur multiple times with multiple input values being sampled.

Special stochastic optimization schemes have been developed, but most of the literature in this area is restricted to small scale linear and nonlinear programming problems with special form [Nemhauser et al., 1990; Ross, 1983; Davis and Vinter, 1985]. These solution techniques often involve a highly formalized structure, require certain distributions on the uncertainties or restrictions in the form of the objective function, often require convexity of the feasible set and quasi-concavity of the probability measure, and typically do not involve large numbers of varying quantities. For these reasons they are inappropriate for optimization of large black box computer models such as RAMP.

Our approach to the stochastic optimization of reliability problems is to discretize part of the space and turn the optimization into a combinatorial problem. The discretization of the space refers to defining the decision variables so that they are discrete, not continuous. In the reliability modeling example, the inputs are component failure modes that have failure rate distributions. Certain improvements can be made on each component which will change the nature of that component's failure rate distribution. In some cases, the improvements could be defined as a continuous function of cost, but in most cases it is more natural for design engineers to think about discrete improvements: if improvement #1 is made, it costs $C1 and will change the distribution to D1. If improvement #2 is made, it

costs $C2 and will change the distribution to D2, etc. In this manner, if each component failure mode has 2 possible improvements (along with the option to do nothing) and there are 50 failure modes, the number of combinations of possible improvements is 3^{50} or approximately 10^{24} (see Figure 1). The size of these combinatorial problems is huge. Note that although we have discretized the space by making the decision variables discrete levels of improvement per component, the uncertainty is still present. That is, for each system combination (a combination of each component failure mode set to a certain level of improvement), RAMP samples from the input level distributions repeatedly to determine the output measure for that system combination. We propose to use a relatively new technique for combinatorial optimization, the genetic algorithm, as the solution method.

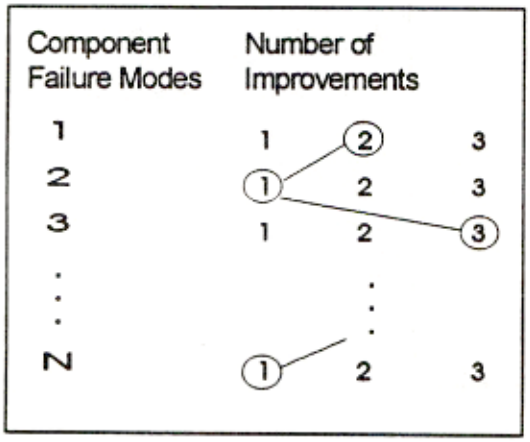


Figure 1: Combinatorial Explosion

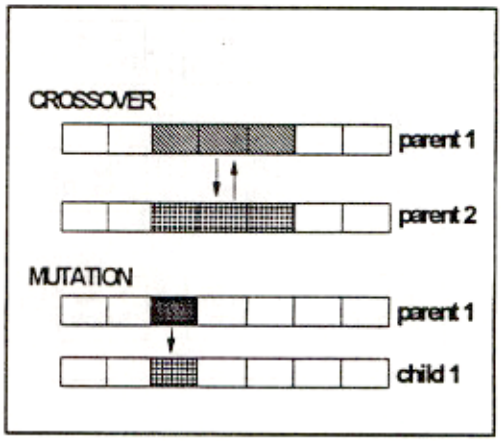


Figure 2: Crossover and Mutation

GENETIC ALGORITHMS

Genetic algorithms take their analogy from the physical world. Genetic algorithms operate by creating an initial "population" of solutions, often represented as bit strings, that "evolve" over successive generations. The solutions with high "fitness" are "mated" with other solutions by crossing parts of a solution string with another. Solution strings are also mutated (Figure 2). Over time, the operations of weeding out poor fitness solutions and reproducing by crossing high fitness solutions at random points act to randomly sample a large part of the huge state space very efficiently. Artificial reproduction schemes were first developed in the 1970s [Holland, 1975] and became popular in the 1980s [Goldberg, 1985, Forrest, 1993]. The reason they work so well is that each population member samples all the possible "schema" or building blocks to which its bits belong. For example, the bit string 1001110 samples the region of the space 1------, where - represents either 0 or 1. It also samples -00----, etc. In this way, many more regions of the space are effectively sampled than the population size.

EXAMPLE PROBLEM AND RESULTS

To test the genetic algorithm approach, we used an example case of personal computer (PC) reliability. This example has twelve failure modes, eight in series and two sets of two in parallel, where we have assumed that the PC has two floppy drives and two hard drives but can be operated with just one of each. This redundancy arrangement assures the system

reliability is nonlinear. A block diagram of the component failure modes for the PC is given in Figure 3. The problem for the design engineer is to improve the reliability of the current PC design. Suppose we know (perhaps from warranty data) that 5% of PCs have a MTBF of less than 2100 hours. We take as a goal to improve reliability to be 95% certain that MTBF is greater than 4000 hours, within a budget allocation of at most $200 per PC.

We identified three potential levels of improvement for each of the twelve component failure modes for this problem. Note that this example has $3^{12} = 531{,}441$ combinations of potential improvements. This problem is ideal for use of genetic algorithms because it has a natural formulation: each solution "chromosome" is a string of "genes," where each gene represents the improvement level on that component.

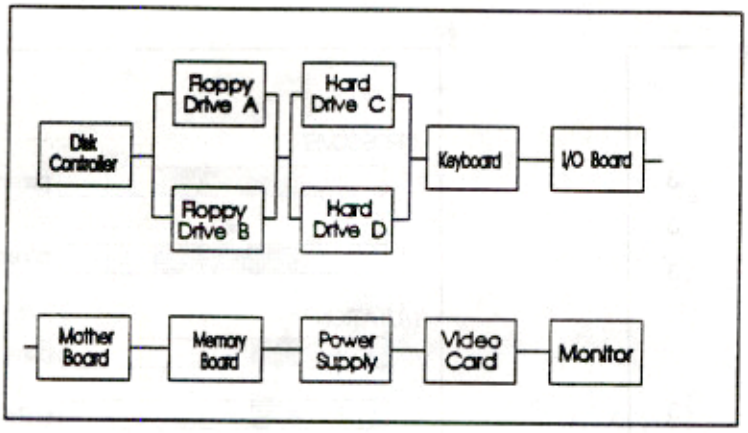


Figure 3: PC Reliability Example

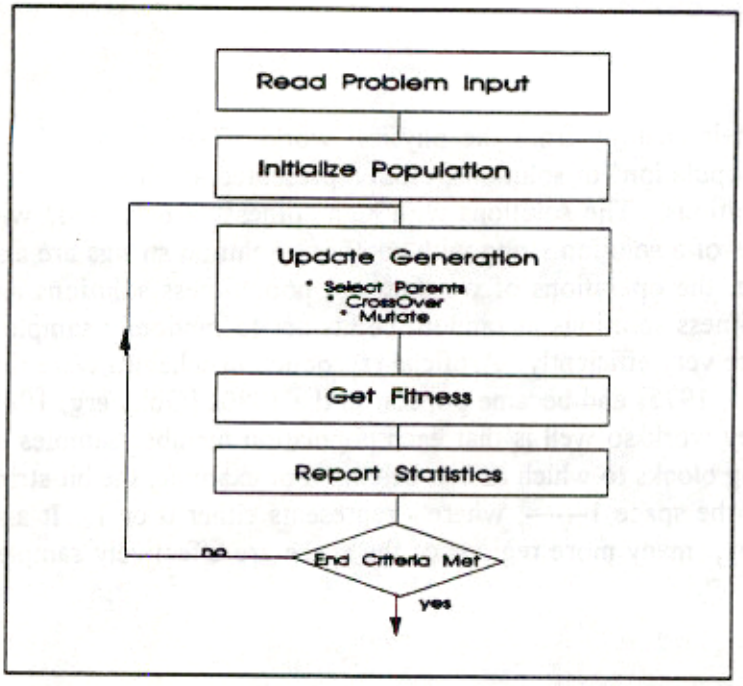


Figure 4: Outline of Algorithm

The genetic algorithm was programmed for use on a PC (see Figure 4 for a flowchart of the code). Our implementation is a fairly straightforward genetic algorithm. Selection of

parents is done through tournament selection: the algorithm randomly picks two solution vectors and chooses the one with the higher fitness as the parent. Mutation randomly flips one "gene" to another possible improvement level. Crossover involves randomly selecting two sites on one solution vector and switching the intermediate bits with those of another. We allowed crossover rate to increase and mutation rate to decrease exponentially with the number of generations. At each generation, approximately fifty percent of the new generation was composed of vectors from the previous generation, and fifty percent were formed by crossover and mutation operations.

The objective function to be optimized had a hard constraint: solution fitness was zero if the combination was over the budget of $200. If the combination was under budget, the fitness was proportional to how closely the 5th percentile of the solution MTBF attained the goal of 4000 hours:

$$\text{if Cost} > \text{Budget, Fitness} = 0$$

$$\text{if Cost} < \text{Budget, Fitness} = \omega_1 * \frac{(MTBF - Base)}{(Goal - Base)} \quad \text{if MTBF} < \text{Goal}$$

$$= \omega_1 + \omega_2 * \frac{(MTBF - Base)}{(Goal - Base)} \quad \text{if MTBF} > \text{Goal}$$

where $\omega_1 = 0.5$, $\omega_2 = 0.3$, Goal = 4000, and Budget = 200.

We ran a complete enumeration (531,441 evaluations) of the space to test the performance of our genetic algorithm. Note that for each combination we ran 200 trials to get the necessary statistics on MTBF, cost, and our fitness function as defined above. The results of the optimization are excellent. Three solutions, or 0.0006% of the space, had a fitness level above 0.9. The genetic algorithm found a solution (with population size 100, running 200 samples per combination) of .912 (Figures 5). The associated cost was $195 and the solution MTBF was 6625 hours. The genetic algorithm ran in 10 minutes on a 66MHz PC with a 486 processor while the complete enumeration took 10 hours. The dual problem, that of minimizing cost subject to satisfying the 4000 MTBF reliability criteria, was also run. The algorithm found a solution that is on the low end of the cost distribution ($100) but satisfies the reliability requirement with solution MTBF of 4184 hours.

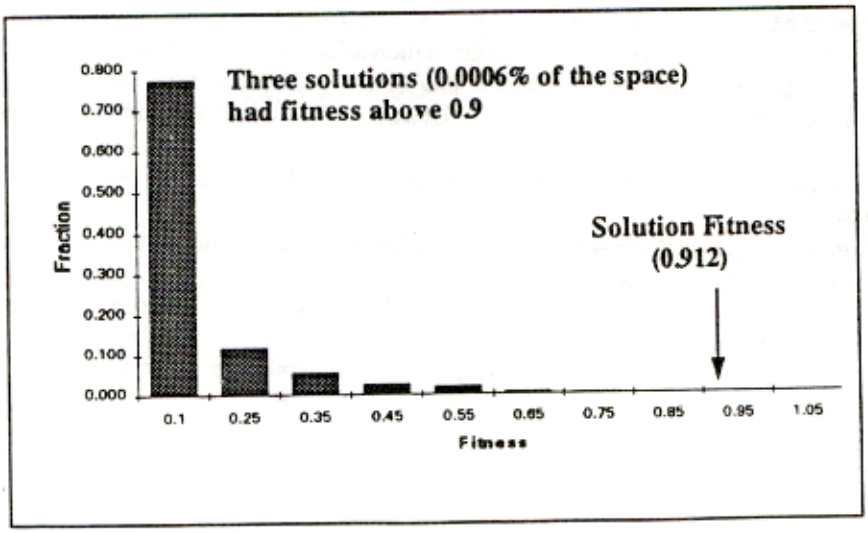


Figure 5: Solution Fitness

One finding of our work was the sensitivity of the algorithm to the robustness of the statistic used. When optimizing an output measure such as a 5th percentile of a distribution, a large number of samples must be taken at each combination so that the statistic does not vary too much over subsequent runs. For example, the 5th percentile of a gamma distribution can vary 8% from the "true" 5th percentile if only 50 samples are taken. The variation of the statistic used as a function of the number of trials must be taken into consideration, as it can add "jitter" to the space, which makes it very hard for the genetic algorithm to settle on one optimal vector. Even with a large number of trials, it may not be possible to find one optimum, as the optimum may vary from run to run because of the input uncertainties and their propagation though the space.

CONCLUSIONS

Our work thus far has shown that genetic algorithms are able to find the optimum of an example system that has three improvement possibilities on each component (where each improvement corresponds to a different *distribution* on component failure rate, not just a point value). We have demonstrated the need for a robust statistic used in the optimization so the run-to-run variation doesn't swamp the optimization search. Future work will include analysis and optimization of more complex systems, such as semiconductor manufacturing equipment and medical equipment. In conclusion, genetic algorithms combined with reliability modeling and uncertainty analysis can provide a powerful design-for-reliability tool.

Acknowledgments

This work was supported in part by the Computational Science Graduate Fellowship Program of the Office of Scientific Computing in the Department of Energy.

REFERENCES

Campbell, J.E., Thompson, B.M., Longsine, D.E., and O'Connell, P.A.,1993, *RAMP (Reliability Analysis and Modeling Program) Version 2 User's Reference Manual,* Sandia National Laboratories, Albuquerque, NM.

Campbell, J.E., Thompson, B.M., Longsine, D.E., O'Connell, P.A., Cranwell, R.M., and Atkins, J., 1993, *A Tutorial on Reliability Modeling Using RAMP,* Sandia National Laboratories, Albuquerque, NM.

Davis, M.H.A., and Vinter, R.B., 1985, *Stochastic Modelling and Control,* Chapman and Hall, London.

Forrest, S., 1993, "Genetic Algorithms: Principles of Natural Selection Applied to Computation," *Science,* **261,** 872-878.

Goldberg, D.E., 1989, *Genetic Algorithms in Search, Optimization, and Machine Learning,* Addison-Wesley, Reading, MA.

Holland, J.H., 1975, *Adaptation in Natural and Artificial Systems,* Univ. of Michigan Press, Ann Arbor. Reprinted in 1992 by MIT Press, Cambridge MA.

Nemhauser, G.L., Ronnooy Kan, A.H.G., and Todd, M.J., 1989, *Optimization: Handbooks in Operations Research and Management Science,* Vol. 1, North-Holland Press, New York.

Ross, S. M., 1983, *Introduction to Stochastic Dynamic Programming,* Academic Press, San Diego.

AN INTRODUCTION TO DYNAMIC MPLD MODEL

Y-S. Hu, M. Modarres

Center for Reliability Engineering
Department of Materials and Nuclear Engineering
University of Maryland
College Park, MD 20740, U.S.A.

INTRODUCTION

The procedure for transferring system knowledge into a computer acceptable representation is a two-stages process:

1. development of a logical representation of the general system and its component interactions,
2. development of a dynamic representation describing physical behavior of the system and its components.

Among recently developed codes such as those in references[1-5], these two stages are modelled separately and independently. For example, in the first stage, STARS[1] uses the fault tree method, RSAS[2] and FAX[3] use the Goal Tree Success Tree (GTST) method, SMART[4] and REX[5] rely on the Master Plant Logic Diagram (MPLD) method. In the second stage, most of these codes do not consider the dynamic behavior, but they show a "snapshot" representation of the system by applying the rule-based knowledge representation (e.g., STARS and RSAS). While these are powerful codes, they have limitations to model the behavior of complex systems. The problem is that time-dependent effects, partial effects and uncertainty of system failures are not modelled because of limitations of the Boolean logic.

One can use dynamic simulation to solve the problem. However, this would be very costly, inefficient, and most of the time unnecessary. Some researchers such as de Kleer[6] and Felkel[7] have proposed some dynamic models based on naive physics to simplify the mathematical relationships of systems. Other researchers[8-12] have used fuzzy logic concept for modelling dynamic relationships. The naive physics has high potential for representing complex relations. The problem is that, for a large system with many interacting components, the complexity of the knowledge will be difficult to handle if we simply use rules or equations to model the system. A decomposition algorithm (e.g., MPLD) can alleviate some of the shortcomings.

In complex physical systems such as a nuclear power plant, the MPLD has proven to be a powerful method for performing the first stage described earlier. This is because MPLD

clearly shows the interrelationship between functions, systems, subsystems and components that need to work together to achieve an objective or mission, as shown in Figure 2. The MPLD can logically and hierarchically display the functions, subfunctions and the manner in which various hardware interact with each other to achieve these functions. While the system logic based on MPLD provides a nice and compact representation of a complex interacting system and shows ultimate effect of a failure on the whole system, it fails to show the behavior of the system (i.e., the second stage).

Since one important characteristic and advantage of the MPLD is its hierarchic representation, it allows for an easy integration of fuzzy logic concept into the classical MPLD. In this concept, the physical behavior is assumed to be represented by interactions between various levels of hierarchy. The degree of interactions can be represented using fuzzy logic. Accordingly, the logical relationships modeled in an MPLD are accompanied by their physical relationships in form of fuzzy relationships. Therefore, it is highly desirable to develop a new diagram that combines the MPLD (the first stage process) and the fuzzy logic concept (the second stage process) together to perform the dynamic effect or behavior of the system due to an incipient failure. In our research, we have integrated the MPLD and time-dependent fuzzy logic into a new logic diagram called Dynamic Master Plant Logic Diagram (DMPLD). By the DMPLD, experts can conclude the degree of success (or failure), approximate values, and transition effects in the system.

Study Example

To better illustrate the problem, let's consider a heat exchanger system and its control system. The simplified Piping & Instrumentation Diagram (P&ID) of this system is shown in Figure 1. This system is designed to reduce the temperature of water pumped from the source tank ***S*** to the target tank ***T*** by using the heat exchanger ***TE***. Cold water is also pumped through the shell side of the heat exchanger as coolant. The objective of this system is to maintain the water entering tank ***T*** at a given temperature and level. To improve the reliability of the source water, redundant tank ***B*** is designed as a backup source tank. If sensor/alarm ***SR*** detects low water level in tank ***S***, the operator ***OP*** will be notified through an alarm. The operator opens valve ***V*** to enable tank ***B*** to deliver its contents. Water pump ***WP*** shares the same power source ***PS*** with coolant pump ***CP***.

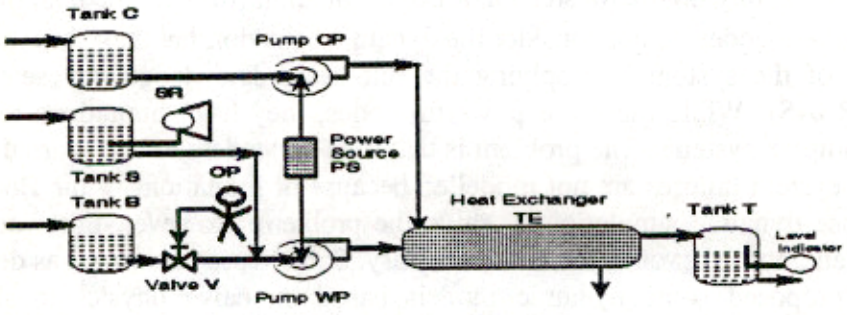


Figure 1. A heat exchanger system and its control system

MPLD and Limitations of Boolean Logic

An MPLD for the heat exchanger system and its control system is shown in Figure 2. The MPLD clearly shows the interrelationships among the independent parts of the systems, including all of the support items. In essence, the hierarchy of the MPLD is displayed by the dependency matrix. For each subsystem, hardware, human, etc., the success paths are shown

on the top. On the left side of the matrix, the set of supporting elements needed are displayed. Since within these supporting elements may be part of more complex systems, another hierarchy and interrelationship may be shown to display this complexity. Informal relationships such as common cause failures may be modeled in MPLD structures too. More details about MPLD is discussed by Hunt and Modarres[13] and Dezfuli and Modarrea[4].

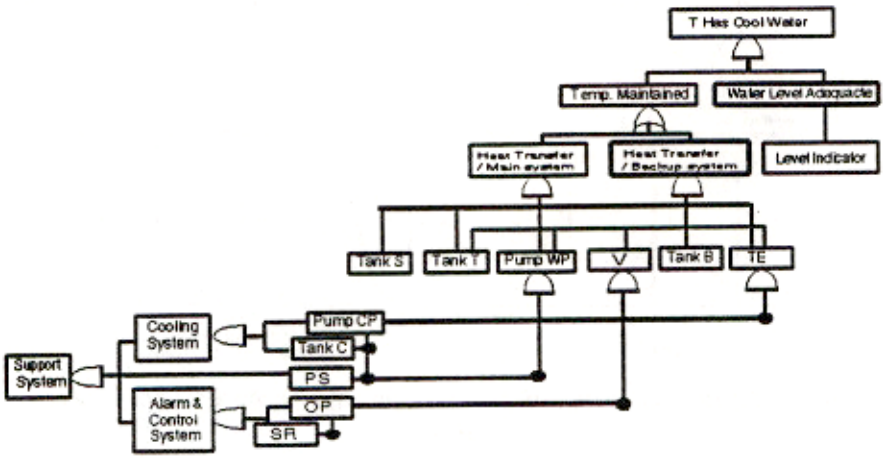


Figure 2. MPLD for the heat exchanger system and its control system

Since MPLD is based on Boolean logic, its use in modelling time dependent systems or multi-state are very difficult. ***Partial failures***, ***transition failures*** and ***uncertainty*** are three examples of such difficulties. These are described below.

Partial failure is a degraded state of a device that does not represent total loss of its functions. For example, assume that we have power ***PS*** oscillation or low voltage. Such a degraded state, which may provide some unsatisfactory output, may damage pumps ***CP*** or ***WP*** in a future instant of time, even if the system may appear functionaly normal.

Transition failure is a failure that may or may not happen after the device loses its supports. It depends on the events that happen during the transition time. In the previous example, because of the low voltage of ***PS***, the input flow of tank ***T*** could be less than its output flow. The system will fail after tank ***T*** hits a low water level. Here the transition failure will depend on the water level of the tank. If ***PS*** is back to normal before the tank runs out of water, the state of the system remains successful during the whole event. Otherwise, the system will fail after the transition time.

Uncertainty addresses possibility of different outcomes. For example, suppose low water level in tank ***S*** triggers alarm ***SR***. Different operators may respond differently and they may act at various times.

Consideration of partial failures, transition failures and uncertainty are very important for system that have unrecoverable damages after a period of time under abnormal operation. MPLD cannot model them because of limitations of Boolean logic. In the next section, an attempt is made to remedy this shortcoming.

FUZZY LOGIC

Since applying Boolean logic to model partial failure, transition time and uncertainty is not easy, we apply time-dependent fuzzy logic to improve the MPLD model. As for the necessity of fuzzy algorithms, Zadeh[11] notes that "most realistic problems tend to be complex, and many complex problems are either algorithmically unsolvable or, if solvable

in principle, computationally infeasible". In the past decade, a variety of studies on fuzzy modelling have been discussed[8-12]. The basic ideas of fuzzy logic are multiple states, overlapped boundary and degree of truth. As shown in Figure 3 (a), Boolean logic has only two states with sharp boundary and full degree of truth. Fuzzy logic considers that states change smoothly from one to another with unclear boundary. One physical value can belong to two or more different states which are distinguished from degree of truth as shown in Figure 3 (b). In this case, power source states have degrees of membership 0.97 for NORMAL, and 0.29 for LOW (sum of degrees does not need to be unity) for a given value of 101 V.

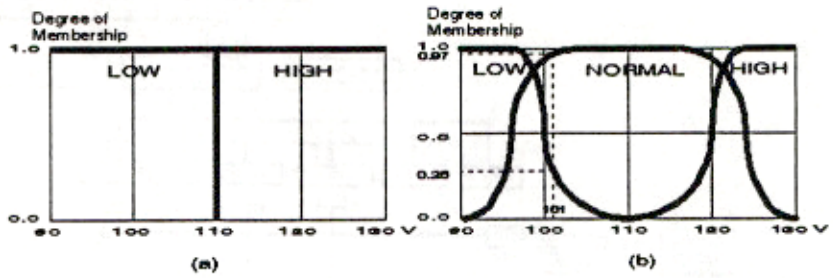


Figure 3. (a) Boolean Logic; (b) Fuzzy Logic representation for power source

We may also transfer fuzzy states back to numerical values by defuzzification procedures[8,10]. The time-dependent logical operations are defined in terms of arithmetic operations on these values regarded as "degrees of membership" to truth. This is (taking lowercase letter as a logic variable, and the corresponding capital letter as its degree of membership at a given time t_i):

$z = x(t_x)$ AND $y(t_y)$	**–**	**$Z = \min(X(t_x), Y(t_y))$, degree of true relationship),**
$z = x(t_x)$ OR $y(t_y)$	**–**	**$Z = \min(\max(X(t_x), Y(t_y))$, degree of true relationship),**
z = NOT y	**–**	**Z = 1- Y.**

DYNAMIC MASTER PLANT LOGIC DIAGRAM (DMPLD)

DMPLD is a logic diagram which is based on the MPLD decomposition method and the time-dependent fuzzy logic. Experts can organize their knowledge by using the decomposing procedure of MPLD. Instead of using two-state (i.e., success and fail), experts may assume multiple states in a specific node which obeys time-dependent-fuzzy-logic operations. However, not all components are time dependent. The design of the DMPLD is to provide a consistent representation that shows the details of the relationship and transition behaviors between components. Since Boolean logic is a degeneration form of fuzzy logic, which has two fuzzy states with full degree of membership, we may use both Boolean and fuzzy logic concepts simultaneously in the DMPLD concepts.

Notations

Figures 4 and 5 show two examples for modeling DMPLD, which will be discussed in details later. There are some new symbols used in DMPLD. Basically, ***fuzzy sets of states*** are grouped sequentially in the component nodes. Regular logic gates and ***transition logic gates*** (time-dependent gates) are used to represent the time-dependent fuzzy logic relations. The ***uncertainty*** is associated with the dependency-matrix to represent degree of true relations.

Transition logic gate is a regular gate with transition time inside. It means that the stated

transition time is required for applying the respective gate. For an 'AND' transition gate, if a new value is reached before its previous value is sent out, the new value will override the old value, and the transition time is recounted accordingly. For an 'OR' transition gate, the values will be sent out sequentially according to their arrival times. Transition gates are used to keep the past values of specific device nodes.

Five different dependency-matrix nodes are used in DMPLD: uncertain node; certain node; uncertain negation node; certain negation node; and independent node. For an uncertain node, the number inside the node represents the degree to which the relationship may be true. The minimum between the input degree of membership function (dmf) and the uncertainty is selected as the output. A solid bullet (i.e., certain node) represents a certain relationship that directly propagates the input dmf to the output dmf. Hollow nodes (with no number inside) means certain negation. The output dmf of a certain negation is (1 - input dmf). The uncertain negation is a hollow node with a bar above the degree of certainty inside. The output dmf of a uncertain negation is the minimum between the uncertainty and (1 - input dmf). A simple-crossed line means no relationship (i.e., independent node).

Using these notations, we may organize a DMPLD to improve the MPLD to represent the time dependency and the uncertainty of the components.

DMPLD for Rule-Based Relations

Since it appears that experts can best represent their knowledge in the form: "IF . . . , THEN . . ." rules, we first discuss the procedure for integrating rules into a DMPLD. As an example, suppose we want to model the alarm-operator relationship in the left bottom side of Figure 4(a) highlighted by a circle. From our knowledge, we may summarize the following rules:

Rule 1 : IF the sound of alarm SR is ADEQUATE, operator OP will response 90% of time ON-TIME, and 10% of time in DELAY time.

Rule 2 : IF SR is Medium-Low (ML), operator OP will response 70% of time ON-TIME, 20% of time in DELAY time, and 10% of time No Response (NR).

Rule 3 : IF SR is LOW, operator OP will response 40% of time ON-TIME, 40% of time in DELAY time, and 20% of time no response.

Rule 4 : IF SR does not sound, OP will not respond.

The DMPLD for the alarm-operator relations can be represented as shown in Figure 4(b), where the rest of the DMPLD is the same as Figure 4(a). When SR is 0.8 LOW and 0.4 Medium-Low (ML), OP will have an outcome of 0.2 NR (no response), 0.4 DELAY and 0.4 ON-TIME as shown in Figure 4(c). Assuming that the reference value is 1 minute for ON-TIME, 5 minutes for DELAY, and 10 minutes for NR. This may be defuzzified to an expected response time of 4.4 minutes. This concludes that the operator highly delays because of the low alarm sound.

The conclusion is passed up to the upper layer of Figure 4(a). We may know that tank ***T*** will lost its input in about 4.4 minutes. Accordingly, if the water level would hit a low level in 4.4 minutes, the system could fail; otherwise, the system will remain operational. The behavior of tank ***T*** can also be modelled by DMPLD with three fuzzy states (normal, reducing and low). As such, DMPLD can represent all detail-transition behaviors.

DMPLD Representation of Physical Models

DMPLD can also be used to approximate physical models represented by mathematical relations. For example, consider a reactor flow loop, shown in Figure 5(a). We are interested in determining the time it takes the coolant, initially at rest, to reach a steady-state flow level once the pump is turned on. Assume the time-dependent flow of an incompressible, inviscid

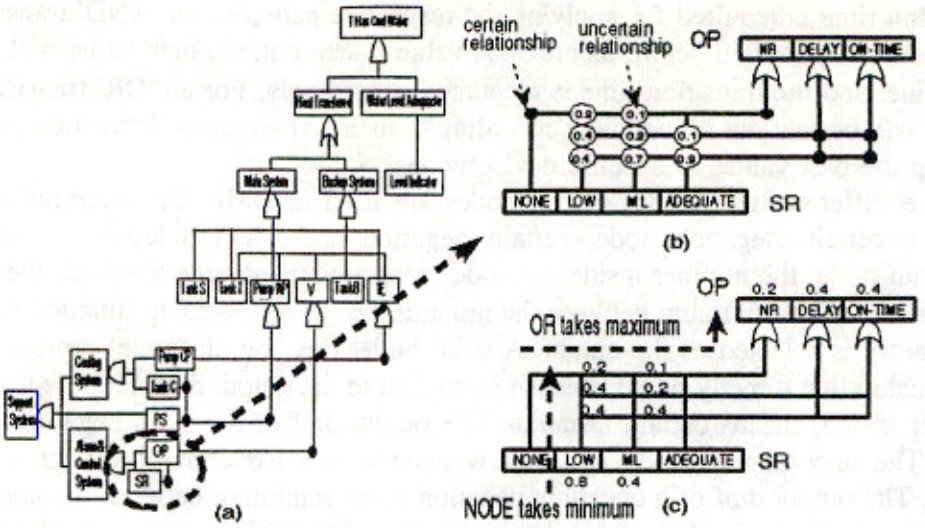


Figure 4. (a) MPLD, (b) DMPLD for alarm-operator relation, (c) compute degree of membership.

fluid created by the pressure difference between two ends of the pump. The incompressible flow rate M_f is space-independent that gives[14]

$$\left(\sum_{i=1}^{i=n}\frac{L_i}{A_i}\right)\frac{dM_f}{dt} = (P_{in} - P_{out}) - M_f^2\left[\frac{1}{2\rho}\left(\frac{1}{A_5^2} - \frac{1}{A_1^2}\right)\right]$$

where t is time; ρ is the density of the water $\approx$ 1000 kg/m^3; and as shown in Figure 5(a), A_i is the cross section of component i; L_i is the length of component i; P_{in} and P_{out} are the readings of the pressure sensors on the two ends of the pump.

Because at t = 0, M_f = 0, we may integrate above equation, and get

$$M_f = \frac{1}{C}\left\{\frac{\exp\left[2C\Delta P\left(\sum_{i=1}^{i=n}\frac{A_i}{L_i}\right)t\right] - 1}{\exp\left[2C\Delta P\left(\sum_{i=1}^{i=n}\frac{A_i}{L_i}\right)t\right] + 1}\right\}$$

where $\Delta P = P_{in} - P_{out}$; and $C^2 = \frac{1}{2\rho\Delta P}\left(\frac{1}{A_5^2} - \frac{1}{A_1^2}\right)$ Thus, we see that as $t \to \infty$, $M_f \to 1/C$. Hence, at steady state there is a balance between the pressure driving force and the acceleration pressure drop.

To construct the DMPLD, instead of integrating the equation, we may approximate the differential equation by using the following difference equation:

$$M_f(t) = M_f(t-\Delta t) + \Delta t\left(\sum_{i=1}^{i=n}\frac{L_i}{A_i}\right)^{-1}(\Delta P - \Delta P\, M_f(t)^2 C^2)$$

Accordingly,

$$M_f(t) = \frac{-1 + \sqrt{1 + 4C_p(M_f(t-\Delta t) + C_t)}}{2C_p}, \qquad \text{where} \quad C_t = \Delta t\,\Delta P\left(\sum_{i=1}^{i=n}\frac{L_i}{A_i}\right)^{-1}; \quad \text{and} \quad C_p = C_t\,C^2$$

Thus we may see $M_f(t)$ has self-updating capability once the pump in turned. The DMPLD representation for the M_f-pump relationship is shown in Figure 5(b), which refers the $M_f(t)$-$M_f(t-\Delta t)$ relationship above as shown in Figure 6(a). Transition logic gates are used to represent transition delay and past-current data relations. We may find that the DMPLD can represent not only the mathematical equation of flow rate, but also the logic relationship

between flow rate and pump. Once the pump turns on, the DMPLD will update M_f automatically. Figure 6(b) shows a comparison between the mathematical solution and the DMPLD estimation for M_f. When more fuzzy states is assumed, the DMPLD estimation becomes more accurate.

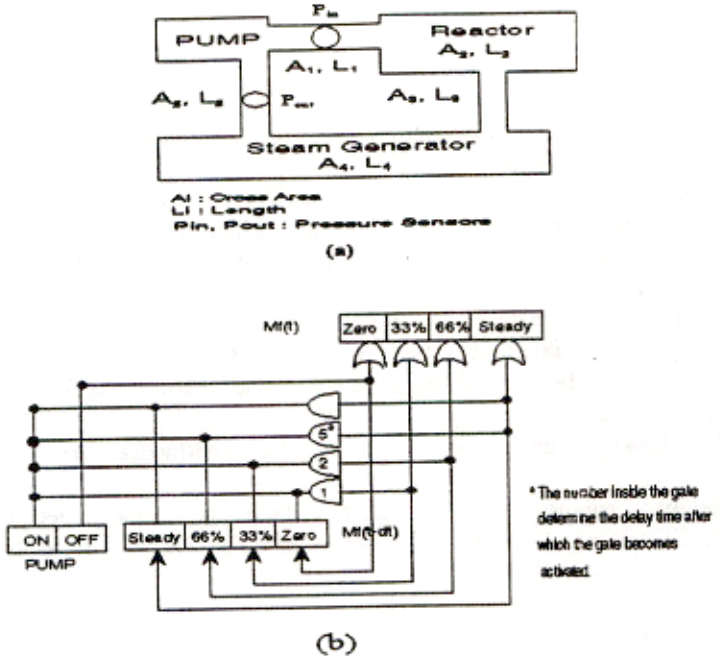


Figure 5. DMPLD for the reactor flow loop.

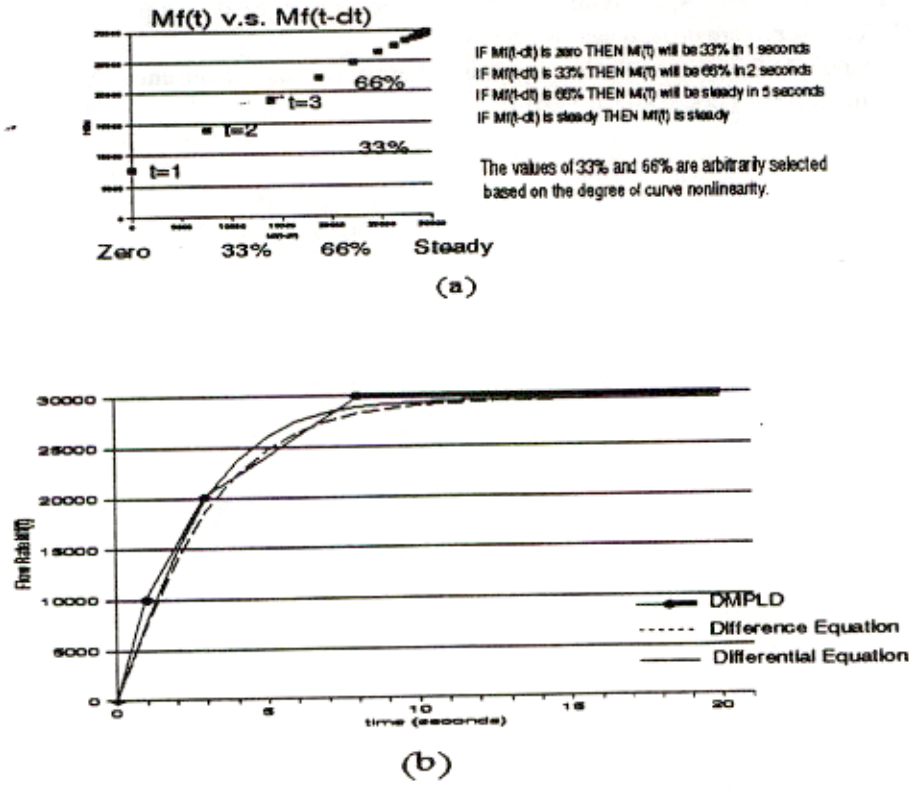


Figure 6. A comparison between mathematical solution and the DMPLD estimation.

By applying DMPLD, experts can decompose complex systems, access their dynamic behavior and conclude the degree of success (or failure). Since fuzzy qualitative states can be transfered back to numerical values by defuzzification, we may make a full-scale simulation for specific components or systems.

REFERENCES

1. A. Poucet, STARS: Knowledge based tools for safety and reliability analysis, *Reliability Engineering and System Safety*, 30: 379-397 (1990).
2. D. Sebo, D. Marksberry, M. Modarres, RSAS: A reactor safety assessment system, *Proc. of the 7th Power Plant Dynamics, Control and Testing Symposium*, Knoxville, TN (May 1989).
3. L-W. Chen, M. Modarres, A hierarchical decision process for fault administration, *Computers and Chemical Eng. J.* Vol. 16, No. 5: 425-448 (1992).
4. H. Dezfuli, M. Modarres, Probabilistic safety assessment using SMART, *Probabilistic Safety Analysis (PSA-93), ANS Topical Meeting*, Clearwater, FL (Jan. 1993).
5. J. Wang, M. Modarres, REX: An intelligent decision and analysis aid for reliability and risk studies, *Reliability Eng. & Syst. Safety J.*, 30: 195-218 (1990).
6. J. De Kleer, J.S. Brown, A qualitative physics based on confluences, *Artificial Intelligence*, 24: 7-83 (1984).
7. L. Flekel, Modeling techniques for on-line expert systems in nuclear power plants, *Proceedings of the Topical Meeting on Advances in Human Factors research on Man/Computer Interactions: Nuclear and Beyond*, Nashville, TN (June 1990).
8. M. Sugeno, T. Yasukawa, A fuzzy-logic-based approach to qualitative modeling, *IEEE Transactions on Fuzzy Systems*, Vol. 1, No. 1: 7-31 (1993).
9. B. Kosko, "Neural Networks and Fuzzy Systems: A Dynamical Systems Approach to Machine Intelligence," Prentice-Hall International Editions, Englewood Cliffs, NJ (1992).
10. D. Dubois, H. Prade, R.R. Yager, "Fuzzy Sets for Intelligent Systems," Morgan Kaufmann Publishers Inc., San Mateo, CA (1993).
11. L.A. Zadeh, Outline of a new approach to the analysis of complex systems and decision processes, *IEEE Trans. Syst.*, Man. Cybern., Vol. 3: 28-44 (1973).
12. A. Kandel, "Fuzzy Expert Systems," CRC Press, Boca Raton, FL (1992).
13. R.N. Hunt, M. Modarres, Performing a plant specific PRA by hand — a practical reality, *the 14th Inter-RAM Coference*, Toronto, Canada (May 1987).
14. N.E. Todreas, M.S. Kazimi, "Nuclear Systems I Thermal Hydraulic Fundamentals," Hemisphere Publishing Corporation, New York, 353-356 (1990).

011 PSA for Dynamic Systems: Modeling Approaches

Chair: M. Marseguerra, Univ. of Milan

A Theoretical Analysis of DYLAM-Type Event Tree Sequences

J. Devooght (U. Libre de Bruxelles); C. Smidts (U. Maryland)

Probabilistic Dynamics: A Numerical Comparison Between a Continuous Event Tree and a DYLAM-Type Event Tree

C. Smidts (U. Maryland); J. Devooght (U. Libre de Bruxelles)

Assessing DYLAM Methodology in the Frame Montecarlo Simulation

G. Cojazzi, P. Vestrucci (CEC- JRC, Ispra)

A THEORETICAL ANALYSIS OF DYLAM - TYPE EVENT TREE SEQUENCES

Jacques Devooght

Service de Métrologie
Nucléaire
Université Libre de Bruxelles
50, Av. F.D. Roosevelt
B - 1050 Brussels (Belgium)

Carol S. Smidts

Dept. Material and Nucl.
Eng.
University of Maryland
College Park, MD 20742-2115
U.S.A.

1. INTRODUCTION

Dynamic event tree methodology involves two competing solution techniques : Monte-Carlo[2] and simulation of most probable event sequences (see for instance[3]) as in DYLAM-DETAM type softwares. This paper is a sequel to ref. 1 where a numerical comparison is made between both approaches and we plan to give here a theoretical basis for the number of sequences to be expected in dynamic event trees, as a function of all their characteristics.

2. QUALITATIVE ANALYSIS OF THE PROBLEM

We shall first introduce the main ideas of this paper in a qualitative way. The dynamic state of the sytem is characterized at time t by the triple $(\overline{x},i,t)$ where $\overline{x}$ is the current vector of physical variables and i the label of the components state. The history of a transient is a trajectory in phase space $(\overline{x},i)$. Our objective is to enumerate all sequences starting from a given point in phase space. However we have an denumerable number of sequences only if we discretize the possible transients, a basic procedure in simulation tools of type DYLAM-DETAM. Moreover we introduce a stopping procedure which gives a finite number of sequences.

The stopping procedure involves two possibilities :

- either the trajectory crosses a safety boundary in $\overline{x}$ subspace, or enters a forbidden (absorbing) state i
- or the probability that the sequence has reached is below some given level.

The first possibility is common to Monte-Carlo methods of simulation. The second possibility is characteristic of DYLAM-DETAM procedures, since in Monte-Carlo it is automatically taken into account : very rare sequences do not occur. To take care of the second possibility we must add one dimension to our phase space. Let $p(t)=e^{-\theta(t)}$ be the probability of a given sequence at time t if the starting point of all sequences is t=0. Every time we reach a branching point of the sequence into (say) N sequences, we split the probability into a sum of probabilities, each one attached to one of the newborn sequences. The splitting preserves the total probability at least as long as no sequence is terminated.

Since p(t) decreases monotonously, $\theta(t)$ is monotonous by increasing. If the stopping procedure includes a low probability level P_{lim}, we have a maximum value $\theta_{lim} = - \ln P_{lim}$ for all sequences.

We characterize now the starting point of a sequence by $(\bar{x},i,\theta,t)$. Point $(\bar{x},i,\theta,t)$ can be reached in many different ways. Indeed if we start all sequences in $(\bar{x}_o,i_o,0)$, there will be in general many paths or sequences leading to $(\bar{x},i,t)$, none of which - in general will have however the same probability, i.e. the same value of θ.

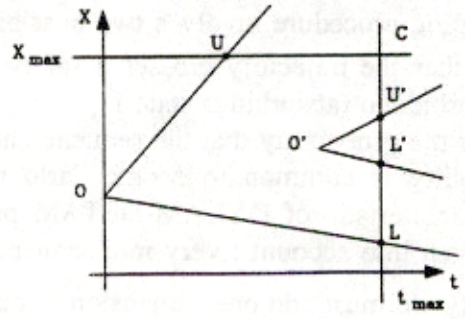
If we are interested in the progeny of the sequence defined by $(\bar{x},i,\theta,t)$ it should be, if possible, a function of $(\bar{x},i,\theta,t)$ only and independent of the past, i.e. the way through which a sequence defined by $(\bar{x},i,\theta,t)$ has been reached. This markovian requirement is satisfied for $\bar{x}$,i since we have a deterministic initial value problem $\frac{d\bar{x}}{dt}=\bar{f}_i(\bar{x})$ interspersed by markovian transition between component states i. However the probability of a given sequence passing through $(\bar{x},i,\theta,t)$ is the product of the probability $p(t)=e^{-\theta(t)}$ by the probability of having a given progeny, i.e. a sequence issued from $(\bar{x},i,t)$. Introduction of $\theta(t)$ has not only the advantage of making the process markovian, but also to make the process additive in the sense that $\theta(t)$ has a finite increment every time we reach a branching point.

Let us call $S(\bar{x},i,\theta,t)$ the total number of different sequences issued from $(\bar{x},i,\theta,t)$. We remember that in a Monte-Carlo sample the number of sequences is a stochastic variable, although in our case it is a deterministic variable entirely determined by $\bar{x},i,\theta,t$, the branching rules and the stopping procedure. Since every point $A(\equiv\bar{x},i,\theta,t)$ in phase space has a finite number of children $B_1, B_2 \ldots B_n$, the number of sequences S(A) is simply

$$S(A) = \sum_{i=1}^{n} S(B_i) \qquad (1)$$

Therefore if we start from a stage where S is known and running the sequences backwards, equation (1) will give the number of sequences issued earlier, a procedure which suggests that the number of sequences obeys an "adjoint" equation, a fact we will prove below. However we are interested in S(0) where 0 is some initial state : not all $B_{i,s}$ will have 0 as an ancestor, and therefore if we run the sequences backwards we must start from those which belong to the reachable set from 0, or in the language of hyperbolic equations theory, the domain of dependence[5]

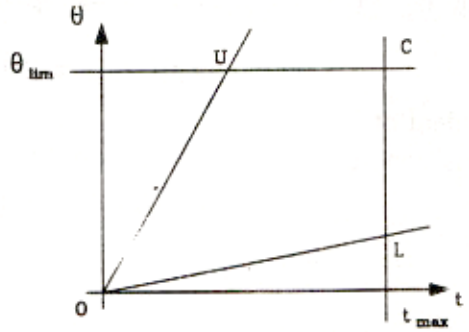
To illustrate this, let us consider a subspace (x,t) where, for the sake of simplicity, x can only take positive values. The stopping procedure is either $x=x_{max}$ or $t=t_{max}$.



All possible trajectories will be localized between an upper line OU and a lower line OL, granting that we have a dynamics : $\frac{dx}{dt}=f_i(x)$ for each state i. At each point (x,t) the

reachable points at $t+\Delta t$ are given by the set $\{x+f_i(x)\Delta t\}$, i.e. the curves OU, OL are the envelope of the allowed trajectories, taking into account the fact that we may have markovian transitions from state i to j with probability $p(i\rightarrow j)$. The reachable set from 0 on the stopping boundary is UCL: if we run the trajectories backwards the domain of dependence of 0 is also UCL. Had we started from 0', the domain of dependence would be smaller : U'L'.

Similarly for the subspace (θ,t) we have the envelope (OU, OL)



where the slope $\frac{d\theta}{dt} \triangleq \lambda(t)$ is always nonnegative and can be defined as an instantaneous transition rate out of the sequence, by branching to sequences of its progeny.

To obtain $S(\bar{x},i,\theta,t)$ we shall define a transport procedure in phase space by analogy with particle transport : a particle follows a trajectory and splits (by "fission") into a greater number of particles at each branching point. Therefore the number of sequences is the number of particles in a branching or multiplying process issued from a given starting particle. This is typically the "importance" (in the language of neutron transport) of the starting point (here the number of possible different sequences issued from this point) which will be a solution of an adjoint transport problem.

3. A PSEUDO TRANSPORT PROBLEM FOR SIMULATION SEQUENCES

We shall now define the transport process more precisely but we make first two preliminary remarks :

1. Whatever are the branching and stopping rules of DYLAM, no stochastic element appears in their definition and therefore the transport process is purely deterministic, even if we use a probabilistic description of the process.
2. The Boltzmann - like equation obtained for S could be solved for instance by Monte-Carlo to investigate the proper combination of parameters compatible with a given value of the number of sequences which is directly proportional to the computational work. Here we shall give, in a very simple example, a complete analytical solution.

We use the following notation[4] :

$P=(\bar{x},\theta,i,t)$

$C_a(P)$	:	probability of absorption, i.e. of stopping of a sequence
$C_f(P)=1-C_a(P)$	:	probability of continuation, i.e. of "fission"
$q_n(P)$	:	probability that the number of direct offsprings is n, i.e. $\sum_n q_n(P)=1$
$C(P',P'')$	:	the collision kernel, i.e. the probability that if a collision (i.e. branching) occurs in P', it will transfer the state to P"

$T(P,P')$: the transition kernel, i.e. the probability that a sequence issued from a branching point at P will have its next branching point at P'.

The branching rules, as given in DYLAM, are the following :
If the component state is i, the branching time is a multiple of an interval Δt, i.e. $k_i\Delta t$ where k_i is a positive integer, such that $e^{-\lambda_i k_i \Delta t}$ is close to a probability W_{lim}.

We shall disregard below the difference between k_i (integer) and k_i obtained from

$$\lambda_i k_i \Delta t \equiv \sigma = \ln W_{lim}^{-1} \tag{2}$$

with σ independent of i.

The transition kernel is given therefore by

$$T(P,P') = \delta(\bar{x}-\bar{g}_i(\tau,\bar{u}))\delta(\theta-\theta_o-\sigma)\delta(\tau-k_i\Delta t) \tag{3}$$

where $P=(\bar{u},\theta_o,i,t)$

$P'=(\bar{x},\theta,i,t+\tau)$

The field $\bar{g}_i(t,\bar{u})$ is the solution of the initial value problem

$$\frac{d\bar{x}}{dt} = \bar{f}_i(\bar{x}) \tag{4}$$

with $\bar{g}_i(o,\bar{u})=\bar{u}$.

Equation (3) embodies the fact that the transport is from $\bar{u}$ to $\bar{x}$ during interval $\tau=k_i\Delta t$, and the probability is decreased from $e^{-\theta_o}$ to $e^{-\theta_o-\sigma}$. The collision kernel is[4]

$$C(P',P'') = C_a(P')\delta(P'-P'') + (1-C_a(P'))\sum_1^\infty n q_n(P') C_n(P',P'') \tag{5}$$

where $C_n(P',P'')$ is the probability to have a transition from a state labeled $P'=(\bar{x},\theta,i,t+\tau)$ to a state $P''=(\bar{x},\theta+\Delta\theta,j,t+\tau)$.

We consider all branches issued from a branching point P' equiprobable because we are interested in <u>counting</u> the number of branches. If N is the total number of component states, $C_n(P',P'')=\frac{1}{N}$ and $q_n(P)=\delta_N^n$. Therefore

$$C(P',P'') = C_a(P')\delta(P'-P'') + (1-C_a(P')) \tag{6}$$

Having defined a deterministic transport process, we must now associate to it a score function which allows to count the number of sequences. The first term means that if a sequence is terminated, P'=P". The score associated with the point P is S(P), the number of different sequences starting from P. If the initial sequence has direct children, the score will be the sum of the scores of the children; if there is no offspring we attribute to that point a score $f_a(P)$. Since scoring is attributed at the branching point, the stopping rule means that although branches are issued at the branching point, no further branching point will be met along certain branches which are terminal, to which we attribute a score equal to 1.

Finally

$$S(P) = \int T(P,P')C_a(P')f_a(P')dP' + \int T(P,P')\int C(P',P'')S(P'')dP'dP'' \tag{7}$$

The stopping rule is the following : sequences are stopped whenever one of the

conditions is fulfilled

(a) $\bar{x}$ leaves domain E;

(b) $t > t_E$;

(c) $\theta > \theta_{lim}$.

The "safety domain" E is defined by the user of DYLAM when the simulation fulfills its objective : to determine the probability of occurrence of some accidental sequences.

Let E be the cartesian product of all three domains (a)(b)(c) : when P enters E, the sequence stops. We define $H_E(P)$ the characteristic function of E, i.e.

$$H_E(P) = 1 \text{ if } P \in E$$
$$H_E(P) = 0 \text{ if } P \notin E$$

We have $C_a(P') = f_a(P') = H_E(P')$.

The branching process involves $\hat{p}(i \to j)$ the conditional probability that if a change of component state i occurs, it will switch to state j, i.e. $\sum_{j \neq i} \hat{p}(i \to j) = 1$. Therefore if a sequence in state i reaches the branching point it will either stay in state i with probability $e^{-\sigma}$ or have a transition to state j with probability $(1 - e^{-\sigma})\hat{p}(i \to j)$.

We may split the increment of θ in two parts :

(1) during the transport phase in state i, the increment is θ

(2) during the collision phase we have a further increment

$$\Delta\theta_{ij} = -\ln[(1 - e^{-\sigma})\hat{p}(i \to j)] \tag{8}$$

for sequences leading to $j \neq i$. If $\hat{p}(i \to j)$ is very small, the large increase $\Delta\theta$ may bring the current value θ over the limit θ_{lim} and DYLAM stops the search of further sequences from state j.

We may now write explicitly eq. (7) and with some lengthy intermediate calculations obtain :

$$S(\bar{u},i,\theta_o,t_o) = 1 + \frac{\lambda_i}{\sigma} \sum_{j \neq i} \int_{t_o}^{t_E} S(\bar{g}_i(t - t_o,\bar{u}),j,\theta_o + \Delta\theta_{ij} + \lambda_i(t - t_o),t)dt \tag{9}$$

where t_E is the smallest time necessary to reach the boundary of E starting from $(\bar{u},\theta_o,t_o)$. Eq. (9) is an elaboration of eq. (1) : either there is no offspring of $(\bar{u},i,\theta_o,t_o)$ (and we count one sequence), either there are offsprings and we sum over all possible offsprings, which is the sum of eq. (9) : sequences generated from time t correspond to a starting point $\bar{g}_i(t - t_o,\bar{u})$, where a branching from i to j occurs with the consequence that the total increment of θ is $\Delta\theta_{ij} + \lambda_i(t - t_o)$. Factors λ_i/σ control the increase of offsprings:

(1) if the rate λ_i out of component state i is high, branching points are more numerous

(2) the same conclusion appears if σ is small, i.e. Δt small, i.e. W_{lim} close to 1.

Indeed W_{lim} controls the discretization of DYLAM-DETAM simulations which are the more realistic, the closer W_{lim} is to 1.

The summation over j in (9) is implicitly limited by the fact that $\theta_o + \Delta\theta_{ij} + \lambda_i(t - t_o)$ should be no larger than θ_{lim}.

We may convert (9) into a partial differential equation :

$$\left[\frac{\partial}{\partial t_o} + \lambda_i \frac{\partial}{\partial \theta_o} + \bar{f}_i(\bar{u})\bar{\nabla}_u\right] S(\bar{u},i,\theta_o,t_o) + \frac{\lambda_i}{\sigma} \sum_{j \neq i} S(\bar{u},j,\theta_o + \Delta\theta_{ij},t_o) = 0 \tag{10}$$

to which we must append boundary conditions. If we take the limit $t_o \to t_E$ in (9) we obtain S=1 on every point of the boundary of E. System (10) is not classical in the sense that we

have a differential-difference equation because of $\Delta\theta_{ij}$.

4. SOLUTION OF THE PROBLEM IN THE CASE OF TWO MARKOVIAN STATES

We refer to the benchmark problem : $\frac{dx}{dt}=\omega_i x$, i=1,2.

Let $\Delta\theta_{ij}=\Delta=-\ln(1-e^{-\sigma})$ for $i\neq j$. Using the concept of characteristics[5] for the system of hyperbolic equation (10) we introduce variables α, β by

$$u=\frac{\hat{\omega}_2\alpha-\hat{\omega}_1\beta}{\hat{\omega}_2-\hat{\omega}_1} \quad , \quad \theta=\frac{\alpha-\beta}{\hat{\omega}_2-\hat{\omega}_1} \quad , \quad \hat{\omega}_1=\frac{\omega_i}{\lambda_i} \quad , \quad u=\ln x \tag{11}$$

We examine here only the limit case where t_{max} is very large.

Reducing (10) to $$\frac{\partial S_1(\alpha,\beta)}{\partial\beta}=CS_2(\alpha-\hat{\omega}_1\Delta,\beta-\hat{\omega}_2\Delta)$$

$$\frac{\partial S_2(\alpha,\beta)}{\partial\alpha}=-CS_1(\alpha-\hat{\omega}_1\Delta,\beta-\hat{\omega}_2\Delta)$$

For small Δ we have finally

$$\frac{\partial^2 S_i(\alpha,\beta)}{\partial\alpha\partial\beta}+\hat{C}^2 S_i(\alpha,\beta) = 0 \tag{12}$$

with $\hat{C}=Ce^{-r\Delta}$, $2r\Delta e^{+2r\Delta}=4C^2\Delta(\hat{\omega}_1^2+\hat{\omega}_2^2)$, and $C^{-1}=\sigma(\hat{\omega}_2-\hat{\omega}_1)$.

Equation (12) is classical telegrapher's equation[5] and its solution involves the Green's function (here Riemann function) $R(\alpha,\beta|\xi,\eta)=J_0(2\hat{C}\sqrt{(\alpha-\xi)(\beta-\eta)})$.

From the limits $u\leq u_{max}$, $\theta\leq\theta_{lim}$ we have to solve (12) in the quadrangle : $\alpha\leq\beta+(\hat{\omega}_2-\hat{\omega}_1)\theta_{lim}$ defined by $\alpha\leq\frac{\hat{\omega}_1}{\hat{\omega}_2}\beta+(1-\frac{\hat{\omega}_1}{\hat{\omega}_2})u_{max}$ and $\alpha=0$, $\beta=0$.

General closed forms have been obtained for $S_i(\alpha, \beta)$, however too lengthy to be given here. For the case $\hat{\omega}_1=0$ examined in[1] we have for instance the limit behaviours

(a) : $u_{max}<\hat{\omega}_2\theta_{lim}$: $\ln S_1 \doteq [\ln P_{lim}]^{1/2}$

(b) : $u_{max}\geq\hat{\omega}_2\theta_{lim}$: $\ln S_1 \doteq \ln P_{lim}$

which is in good agreement with the numerical results obtained so far.

REFERENCES

1. C. Smidts, J. Devooght, this conference.
2. J. Devooght, C. Smidts, Nucl. Sc. Eng. 107, 229 (1992).
3. C. Acosta, N. Siu, Reliab. Eng. Syst. Safety 41, 135-154 (1993).
4. I. Lux, L. Koblinger, "Monte Carlo Particle Transport Methods", CRC Press (1991).
5. R. Courant, D. Hilbert, "Methods of Mathematical Physics", Vol. II, Interscience (1962).

PROBABILISTIC DYNAMICS: A NUMERICAL COMPARISON BETWEEN A CONTINUOUS EVENT TREE AND A DYLAM-TYPE EVENT TREE

C. SMIDTS

Dpt. of Materials and
Nuclear Engineering
University of Maryland
College Park, MD 20742-2115

J. DEVOOGHT

Service de Métrologie
Nucléaire (C.P. 165)
Université Libre de Bruxelles
50 ave. F.D. Roosevelt
1050 Bruxelles, Belgium

INTRODUCTION

The feeling that dynamics and their interaction with the random evolution of parameters was ill-treated in classical probabilistic safety assessment methodologies led to the development of probabilistic dynamics methodologies and the concept of dynamic PSA. These methodologies do all explicitly model the mutual influence between physical variables, operators and components but use different basic assumptions. This paper discusses a first attempt at a systematic comparison between two such classes of methodologies, namely, the continuous[1] and the discrete (DYLAM/DETAM)[2,3] event tree methodologies. Such comparison is needed if we want to reach a consensus as to which methodology should be implemented in a dynamic PSA.

The two methods differ essentially in their sequence generation process. The first allows stochastic transitions at any time whereas the second allows transitions only at given moments in time. These specific moments (or branch points) occur when simultaneously a multiple of a user-specified time step 'dtime' is reached and when the probability of the current sequence becomes inferior to a given probability threshold 'W_{lim}'. It can be shown that discrete event trees are discretized continuous event trees[4].

Continuous Event Trees find their natural implementation in Monte Carlo algorithms[5]. The analog Monte Carlo algorithm is obtained directly from the integral equation that describes continuous dynamics processes and efficient modified (biased) Monte Carlo algorithms can also be derived from the main equations that subtend the continuous event tree theory.

The Continuous Event Tree theory algorithm (Monte Carlo) is characterized by two parameters: the size of the Monte Carlo sample 'n_{trial}', and the time step 'dtime' of the Runge-Kutta algorithm which calculates the evolution of the physical variables embedded in the stochastic sampling.

Discrete Event Trees algorithms generate the tree structure in a controlled way. The

search through the tree follows a depth-first algorithm. Different mechanisms are used to control and limit the tree explosion (a cut-off frequency 'P_{lim}', probability threshold under which the sequence is purely and simply erased and a lumping of NMC sequences of low probability).

THE NUMERICAL COMPARISON

1. The Problem

To better understand the methods (i.e. the influence of the parameters on the outcome), their differences, how these differences impact the accuracy of the results, the efficiency, the stability, we designed a comprehensive and systematic numerical comparison based on examples which had known analytical solutions. DYLAM and Monte Carlo failure probability estimates are compared to this reference.

The Single Component Problem involves a bistate (operational or failed) component which regulates the behavior of a physical variable x:

$$dx/dt=\omega_i.x \quad \text{with i=1 (operational), 0 (failed)} \tag{1}$$

The study is limited to $\omega_1=0$ and $\omega_0>0$. The component is repairable: its failure rate is λ and its repair rate is μ. The unknown is the probability $p_z(t)$ that x is superior to a given threshold 'z' at time t:

$$p_z(t)=1-\int_{x_0}^{z}\sum_{i=1}^{2}\pi(x,i,t|x_0,j).dx \tag{2}$$

where $\pi(x,i,t|x_0,j)$, the probability density for an initial state x_0,j is obtained analytically.

The Multi-Component Problem. A trivial extension of (1) to a multicomponent problem is obtained easily by "adding" different single components problems (or sub-systems). If we assume that these subsystems are independent (independent transition rates and independent physical variables), we show that if :

$$dx_k/dt=\omega_{i,k}.x_k$$

where x_k and i_k are respectively the physical variable and state of the k^{th} single component problem,
then:

$$\pi(\bar{x},i,t)=\prod_k \pi(x_k,i_k,t)$$

where $\pi(x_k, i_k,t)$ is the solution for sub-system k, and $\pi(x,i,t)$ is the solution for the complete system,

and this independently of the structure of the network we build. Although trivial, this extension is significant because neither DYLAM nor Monte Carlo know that the problem can be solved by factoring it into one dimensional problems and we have an easy way to assess the influence of the number of components.

2. The Results

Failure Probability Curves. Figure 1 compares the analytic value of $p_z(t)$ for a single component, initially failed (x_0=1m, z=2m, ω_1=0u^{-1}, ω_0=10^{-1}u^{-1}, λ = 5.10^{-2}u^{-1}, μ = 5.10^{-1} u^{-1}) to its computed value obtained using DYLAM-3 and Monte Carlo (MC) algorithms. The same system is studied in Figure 2 and 3. Values of n_{trial}, W_{lim},.. are listed on the figure, dtime is equal to 0.1u, where 'u' stands for an arbitrary time unit. The figure underlines the differences between the approaches. DYLAM approximation of the solution is a staircase function; each step has the same width (w≈.8u). $P_z(t)$ is first underestimated, reflecting a problem to cope with the hedge of the distribution at t_H≈7u, and later overestimated, drifting progressively away from the solution. Estimates of $p_z(t)$ are independent of the run as the process that generates the event tree is entirely deterministic. The MC solution is an histogram with steps of length dtime=0.1u. Estimates of $p_z(t)$ vary from run to run because of the stochastic nature of the process. The algorithm constantly underestimates the true value of $p_z(t)$ and the estimate becomes worse when time increases. Degradation with time is foreseeable in each case: new tributes to $p_z(t)$ for large values of t originate from events with low probabilities which are poorly described by MC and are more likely to be cut by the discrete event tree limitation criteria inserted in DYLAM. The DYLAM steps length is related to k_0≈ln(W_{lim}^{-1})/(λ.dtime) (here, k_0=72) and k_1≈ln(W_{lim}^{-1})/(μ.dtime) (here, k_1=8) values. The first contribution to failure c_1 comes from a component that was not restored before t_H, the second contribution, c_2, comes from a component restored after k_1 time steps, failed after k_0 and not restored before t_H-.8u, etc...

Number of Sequences. Figure 2 gives S_n, the number of sequences generated by DYLAM as a function of P_{lim}, the cut-off frequency. S_n first increases with P_{lim}, then reaches an asymptotic value P_{lim}^{Min} for which most sequences are preserved, a behavior which can be predicted by studying the process that generates the event tree as is shown in a companion paper[6] (for ln(z)≪ω_0.ln(P^{-1}_{lim})/μ , ln S ≐ [ln P^{-1}_{lim}]$^{1/2}$).

Error Estimates. A comprehensive study of the two algorithms has been carried out for the single component problem and is reported in Smidts[7]. From this study we extracted Fig.3 and 4 which relate to tests carried respectively in the high and low transition rates region.

The first series of tests relates to the single component problem of Figure 1. Figure 3 shows the computing time E_t versus E_r, the relative error with reference to the analytical solution, at the mission time T_{Max}=100u, for different series of Monte Carlo and DYLAM experiments. Parameters such as W_{lim}, P_{lim}, n_{trial} were systematically varied to assess their impact on the accuracy of the results and to identify optimal combinations. Theses figures enable us to gain some insight over the relative efficiency of the two methods in the high transition rates region for a small size problem. Our measure of efficiency is E_f=($E_{t,DYL}$.$E_{r,DYL}$)/($E_{t,MC}$.$E_{r,MC}$)$^{-1}$. Given this measure of efficiency, Monte Carlo scores obviously better than DYLAM. DYLAM will run 2.10^3 seconds before reaching E_r=5.10^{-2} where Monte Carlo will run 20 seconds only to achieve the same level of accuracy (E_f=100). We should bear in mind that Monte Carlo data points are related to specific samples. However, our conclusions hold for any sample within the standard deviation bounds.

A second series of tests was designed to cover the low transition rates region. The component is operational at time 0, x_0=1m, z=2m, ω_1=0u^{-1}, ω_0=10^{-1}u^{-1}, λ = 10^{-4}u^{-1} and three different values of μ were considered: μ = 10^{-4} u^{-1}, 10^{-3}u^{-1} and 10^{-2}u^{-1}. Biased Monte Carlo (BMC) trials were added to this case as λ was sufficiently small to allow a benefit from importance sampling. We observe (see Fig.4) that even if biasing techniques improve the efficiency, DYLAM is more efficient than Monte Carlo: 75 times more efficient than BMC and 840 times more than the analog Monte Carlo (AMC).

We finally ran Monte Carlo (analog and biased) and DYLAM algorithms (for description of the runs see table I) on test problems constituted of 1, 3 and 5 identical components placed in series: the failure of anyone of the components brings the failure of the system. These components were assumed to possess same failure and repair rates, follow similar dynamics and to be characterized by same the same failure criteria, the mission time T_{Max} is 100u. Fig.5 displays the product $E_t.E_r$ for each run. E_r is assessed both with results of actual Monte Carlo runs (M1,M2) and with the corresponding standard deviations (M1',M2') to reflect the true behaviour of the algorithm. Results show the decrease of efficiency with the number of components for a given selection of parameters and demonstrate that Monte Carlo and DYLAM algorithms do respond very differently to an increase in the size of the system.

CONCLUSIONS

This paper shows the supremacy of Monte Carlo for small systems characterized by high transition rates. A probabilistic dynamics process has high transition rates as soon as some system mean transition times (MTT) match the time window of the analysis or the critical times at which significant physical thresholds are reached (i.e. the ones that define the success, failure criteria,...). Actually, we show in [7] that Monte Carlo supremacy is not only expressed in terms of lower computing times for the same level of accuracy but also in terms of stability (i.e. whether monotonic variations of the parameters translate into monotonic improvement of the results). On the other hand, for small systems with low transition rates, DYLAM supremacy can not be questioned. Supremacy here is limited to efficiency considerations.

The paper also shows that the relative efficiency of the two algorithms (DYLAM/ Biased Monte Carlo) decreases with the number of components and concurrently with the number of physical variables in such way that it makes no doubt that moderate size systems, whatever their failure and repair rates, can only be handled by a biased Monte Carlo (if $N_{phy} \approx N$, N_{phy} is the number of physical variables, N is the number of components) adapted to the problem under study. It is often claimed that handling biased Monte Carlo algorithms requires skill when it comes to finding the best fitted technique. However the problems studied in reliability have well defined characteristics such as low failure rates, high repair rates, and hence allow the existence of generic biased Monte Carlo's that would handle the whole class of availability/reliability problems.

Failures on demand have not been addressed here although they constitute the major (often the only) contributor analyzed in PSA. However results obtained for failure rates and repair rates may be used to extrapolate to failure on demands. In the case of failure/repair rates, branch points are created every time. On the other hand, demands occur only when physical thresholds are reached or when components reach given configurations. Hence the number of branch points will remain limited and DYLAM or similar techniques could then be recommended.

ACKNOWLEDGEMENTS

The authors wish to thank Giacomo Cojazzi for his explanations and fruitful comments on the DYLAM methodology. Part of the work described in this paper was founded by the CEC/JRC/ISEI, Ispra, in the frame of the Nuclear Reactor Safety Research Program 92-94, under contracts N.4827-92-06 EI ISP B and N.5002-92-10 EI ISP B.

REFERENCES

1. J.Devooght, C.Smidts,"Probabilistic reactor dynamics -I. The theory of continuous event trees", *Nucl.Sci.Eng.* 107: 229 (1992)
2. G.Cojazzi, P.C.Cacciabue, P. Parisi, "DYLAM-3. A dynamic methodology for reliability analysis and consequences evaluation in industrial plants", ISEI/SER 2192/92 Draft, Commission of the European Communities (Jan. 1992)
3. N.Siu, C. Acosta, "Dynamic event tree analysis. An application to SGTR", Proc. Int. Conf. PSAM, Beverly Hills, California (Feb.1991)
4. J.Devooght, C.Smidts," Probabilistic dynamics: The mathematical and computing problems ahead", Proceedings of the NATO workshop on Reliability and Safety of Dynamics process Systems, to be published by Springer (1993).
5. C.Smidts, J.Devooght,"Probabilistic reactor dynamics -II: A Monte Carlo study of a fast reactor transient", *Nucl.Sci.Eng.* 107: 241 (1992)
6. J.Devooght, C.Smidts,"A theoretical analysis of Dylam-type event trees", this conference.
7. C.Smidts,"A Comparison between continuous event trees and a discrete event tree model", to be published in *Reliab. Eng. and Systems Safety.*

Table 1. Parameters selected for the tests (N= 1, 3 or 5).

Parameters wich are frozen	Monte Carlo experiments		Dylam experiments	
Initial state:'111' $\lambda=10^{-3}u^{-1}$, $\mu=10^{-4}u^{-1}$ $T_{Max}=100u, x_0=1m$, $z=2m$	M_1 and M_1' (analog)	M_2 and M_2' (biased)	D_1	D_2
	ntrial= 10^6	ntrial = 2.5×10^5	dtime=.5u	dtime=.5u
	dtime=.5u	dtime=.5u	$P_{lim}=10^{-6}$	$P_{lim}=10^{-6}$
	weili[1]=0	weili=10^{-3}	$W_{lim}=.999$	$W_{lim}=.99$
			NMC=0	NMC=0

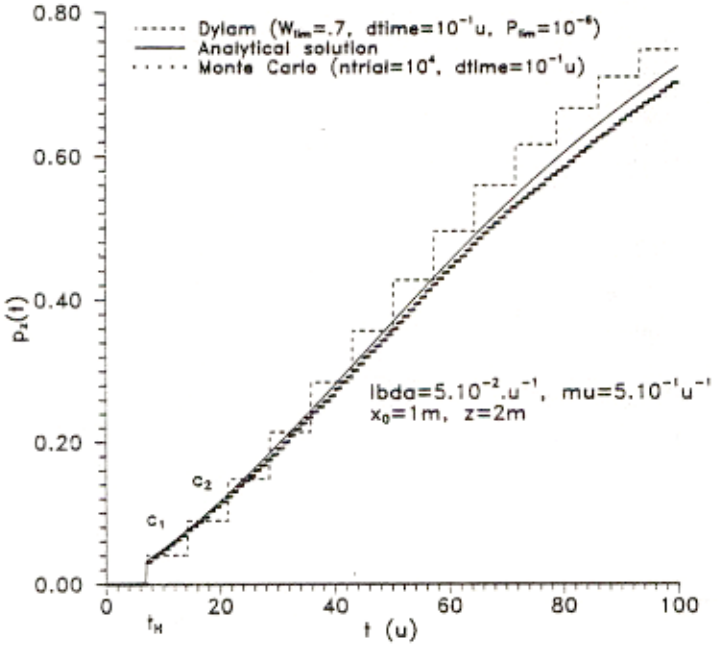


Figure 1. $p_z(t)$.

1 weili: parameter limiting the biasing process

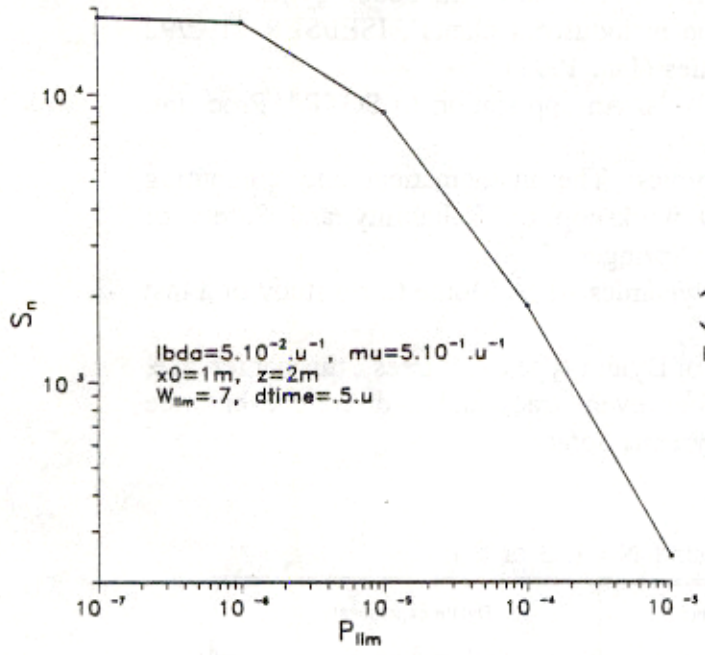


Figure 2. Number of sequences versus P_{lim} (DYLAM). (Initial state: failed, $w_1 = .0u^{-1}$, $w_0 = .1u^{-1}$)

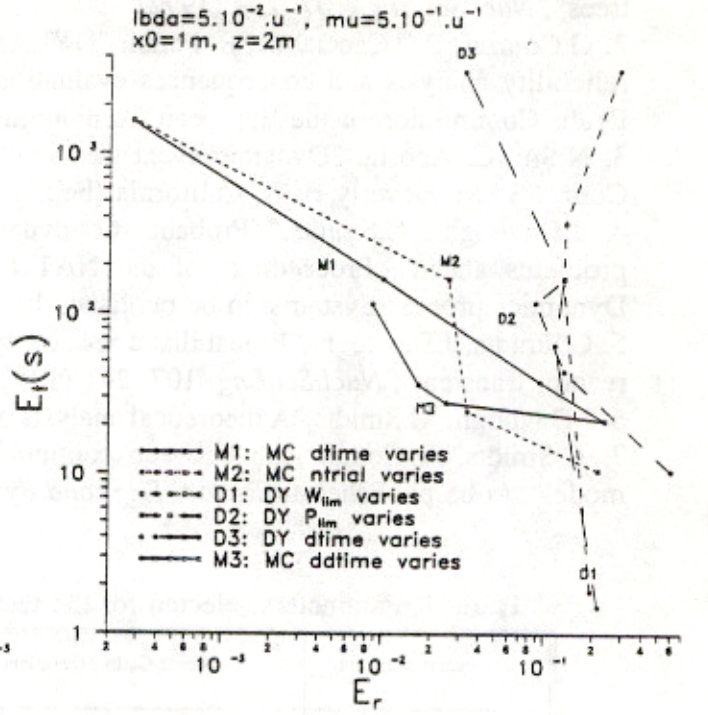


Figure 3. Execution time versus relative difference at T_{max}= 100u (Di (resp.Mi) refers to DYLAM (resp. Monte Carlo) tests)

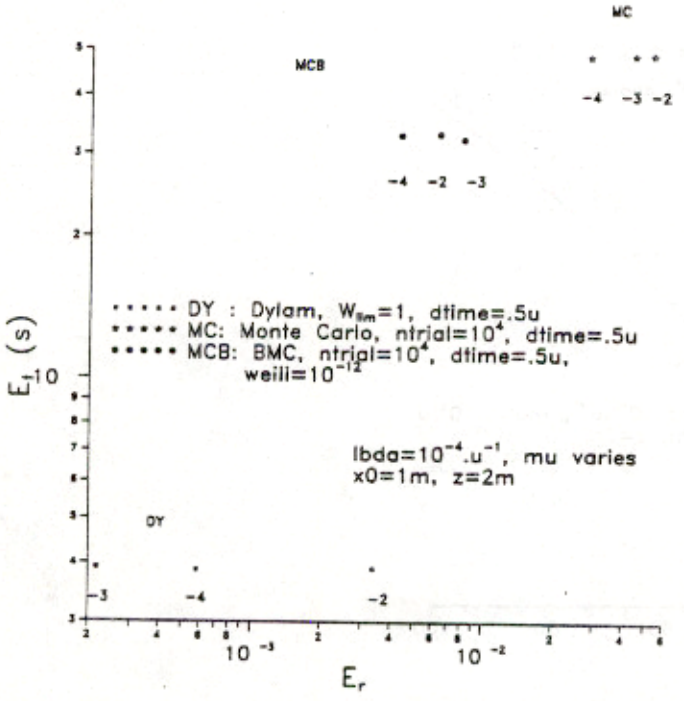


Figure 4. Execution time versus relative error.

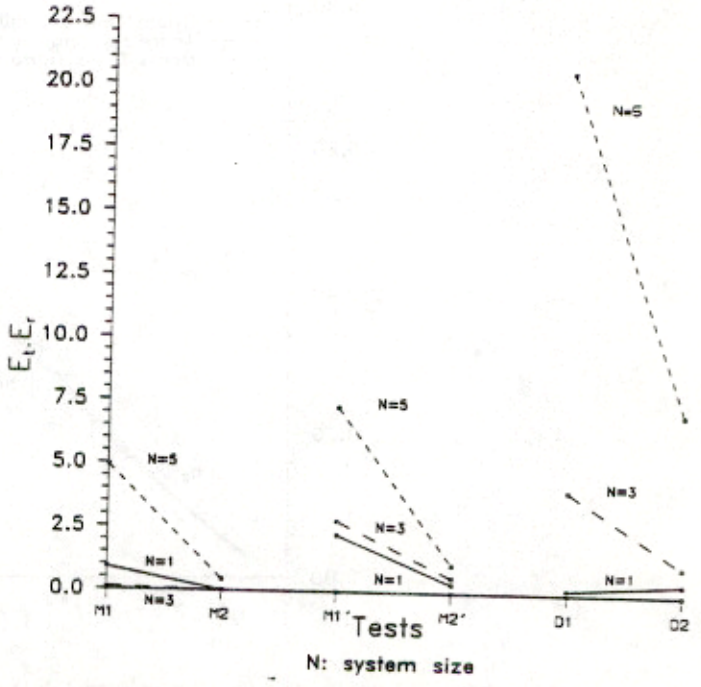


Figure 5. E_t . E_r function of DYLAM and Monte Carlo tests.

ASSESSING DYLAM METHODOLOGY IN THE FRAME OF MONTECARLO SIMULATION

Giacomo Cojazzi, Rosa Sardella, Tullio Trombetti*, Paolo Vestrucci+

Commission of the European Communities Joint Research Centre
Institute for Systems Engineering and Informatics, 21020, Ispra, Varese, Italy

*Nuclear Engineering Laboratory, Via dei Colli 16, 40136 Bologna, Italy
+Nuclear Engineering Laboratory, Via dei Colli 16, 40136 Bologna, Italy & NIER

INTRODUCTION

Advanced reliability and safety analysis may require to remove the limits of classical methods (as fault-trees and event trees), which consist mainly in ignoring the phenomenology of the system to be studied. In other words, although the time variable is taken into account through the system mission time, classical methods do not consider the time evolution of the physical variables, nor the time dependent interaction with the operator crew. In order to remove these limitations, some methods, which can be called dynamic, have been developed in order to fill the gap between the need of more realistic analysis and available methods and tools (Aldemir, 1987, 1992; Limnios, 1988; Deoss and Siu, 1989; Marseguerra and Zio, 1992). The DYLAM method (Amendola and Reina, 1981) has been the first systematic attempt to combine the stochastic behavior of the system (component failures) to the deterministic phenomenological evolution (physical state variables). Different applications of the DYLAM code have already been published in literature (Cacciabue et al, 1986, 1991, 1992), including the analysis of subsystems of real nuclear power plant.

Devooght and Smidts (1992a) developed a general theoretical framework for describing the stochastic and deterministic nature of systems subject to failures. As a result of the application of the Chapman Kolmogorov equation, which governs Markovian systems, a probability density balance is derived. An integral formulation is also given, and is shown to be equivalent to a continuous event tree. In this framework different dynamic approaches, such as cell to cell mapping (Aldemir, 1992), Montecarlo (MC) simulation (Smidts and Devooght, 1992), and the DYLAM code (Cojazzi et al. 1993) can be seen as different attempts for the solution of the general equations (Devooght and Smidts, 1992b). In particular, the integral formulation of the probabilistic dynamic equations corresponds to the classical form of a transport Montecarlo problem and DYLAM can be regarded as an approximation of the integral equations where the cumulative failure probability is a staircase function.

In this paper the DYLAM approach is revisited in the frame of MC simulation: it is shown that DYLAM way for handling stochastic transitions can be regarded as an extremely biased

Montecarlo in which instead of the true failure probability density functions, proper Dirac delta functions are used; this implies that the cumulative distributions turn out to be step functions. In this way, the so called forced collision variance reduction technique is applied in a very strong manner. Indeed the stochastic feature of Montecarlo is practically lost at this point, with the advantage of a consistent reduction of the number of histories.

THE DYLAM CODE

The basic idea of DYLAM is to evaluate the safety and reliability of a system by following the in-time evolution of the system itself, as a result of failures in the components. During the simulation a time dependent probability is evaluated by DYLAM, while the physical behavior of the system is computed in an user-supplied routine coupled with DYLAM. The probability of occurrence of a certain system top event is simply obtained by summing the probability of the sequences leading to the top event itself. For each component of the system, the user can choose amongst six different probabilistic options. Concerning its dynamic capabilities DYLAM can treat in-time transitions (failures and repairs) with constant or variable transition rates, as well as failures on demand and failures on demand combined with transitions in time.

Hereafter we report briefly the basic algorithms of DYLAM for the case of stochastic transitions with constant transition rates. For the sake of simplicity, only one component (A) with two states will be considered. The extension of the results to the multicomponent case is not straightforward and will not be presented here.

The probability for the component to remain in its initial state, say k, after a time $(t-t_0)$ is:

$$P(A_k,t)=P(A_k,t_0)\cdot e^{-\int_{t_0}^{t}\lambda_{kj}\,dt} = S(t) \quad k,j=0,1 \quad k\neq j \tag{1}$$

where λ_{kj} is the transition rate from state k to state j. In the case of constant transition rates:

$$P(A_k,t)=P(A_k,t_0)\cdot e^{-\lambda_{kj}(t-t_0)}=S(t) \tag{2}$$

Since DYLAM operates with a constant time-step Δt, all the possible branch points are evaluated at times which are multiple of Δt. If at a time t_m the branching condition is satisfied:

$$P(A_k,t_m)=S(t_m)\le P(A_k,t_0)\cdot Wlim \tag{3}$$

where *Wlim* is a user-supplied threshold, a first branch point time, $t_{BP1} = t_m$, is triggered. Equation (3) is updated at $t_n>t_m$ when

$$P(A_k,t_n)=S(t_n)\le P(A_k,t\equiv t_{BP1})\cdot Wlim \tag{4}$$

This procedure is repeated until DYLAM reaches the final time of analysis T_{MAX}. It results that DYLAM calculates the probability for the component to remain in its initial state as a staircase function $S^*(t_n)=1-\sum q_i H(t_n-t_{BPi})$, where $\sum q_i=1$ and $H(t-T)=1,\forall\, t\ge T$. The descendant sequences are generated from the transitions of the system which happen at each branch point instant. The birth probability of the j-th descendant sequence at time t_{BP1} is

$$P(A_j,t_{BP1})=P(A_k,t_0)\int_{t_0}^{t_{BP1}} e^{-\int_{t_0}^{t'}\lambda_{kj}\,dt}\,\lambda_{kj}\,dt' = P(A_k,t_0)\left[1-e^{-\lambda_{kj}(t_{BP1}-t_0)}\right]=F_1^*(t_{BP1}) \quad j,k=0,1\ j\neq k \tag{5}$$

Therefore the probability of leaving the initial state is $F^*(t_n)=\sum F_i^*(t_{BPi})=\sum q_i H(t_n-t_{BPi})$.

The iterative use of eq. (4) is sketched in figure 1 where, for simplicity, we assumed $P(A_k,t_0)=1$. Descendant sequences are generated only at branch points instants. Notice that, as a consequence of eq.s (2) and (3), branching times are all multiple of t_{BP1}.

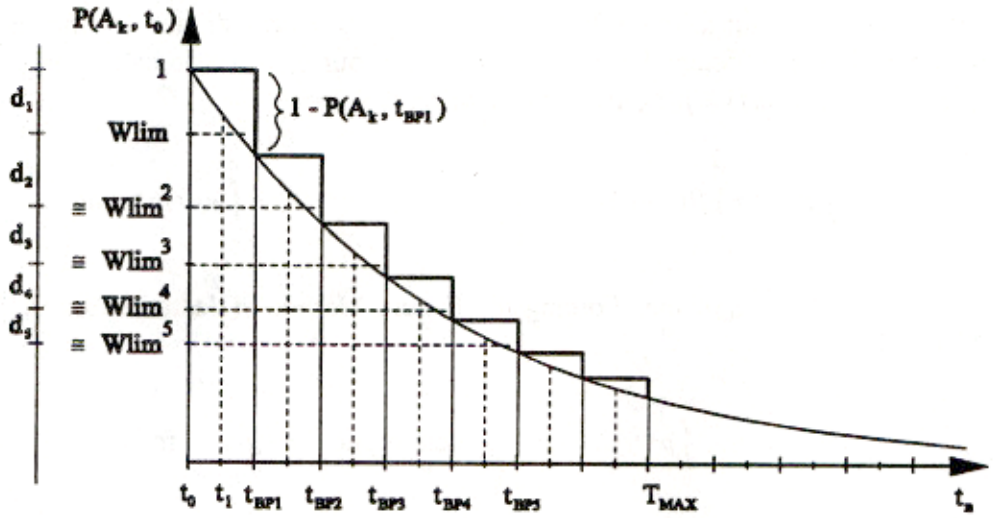


Figure 1. Probability splitting for a monocomponent system.

If no repair is considered, $S(t)$ and $F(t)=1-S(t)$ represent the true success and failure probability of the system, while $S^*(t_n)$ and $F^*(t_n)$ are the DYLAM approximations which apply for the whole mission time T_{MAX}. In the case of a repairable component the equations hold only between two consecutive branch points and $S(t)$, $F(t)$ have to be intended, as the probability of remaining and leaving the current state at the branch point time t_{BPn}. In the paper we disregard the use of the important parameters Plim and NMC (Cojazzi et al., 1993).

THE MC VARIANCE REDUCTION TECHNIQUE "FORCING THE FAILURE"

It is well known that, if T is the mission time, the failure probability $F(T)$ and the success probability $S(T)$ can be expressed in the following way:

$$F(T)=\int_0^T p(t)dt \quad , \qquad S(T)=1-F(T)=\int_T^{\infty} p(t)dt \tag{6}$$

where $p(t)$ is the failure probability density function (pdf) which, in the case of no repair and constant failure rate, is an exponential pdf, i.e. $p(t) = \lambda\ e^{-\lambda\ t}$. These integrals can be written in a slightly different mode using the usual step function $(H(t))$:

$$F(T)=\int_0^{\infty} H(T-t)p(t)dt \quad , \qquad S(T)=\int_0^{\infty} H(t-T)p(t)dt \quad . \tag{7}$$

The Montecarlo method is essentially a numerical (simulative) way to calculate integrals, like the previous one, using the well-known technique based upon random numbers generation. The variance reduction methods have been developed in order to make Montecarlo applications more efficient. These methods start from the following identity:

$$\int_0^{\infty} q(t)f(t)dt = \int_0^{\infty} w(t)q^*(t)f(t)dt \tag{8}$$

where $q(t)$ is a function with the property of a pdf and $w(t)$, $q^*(t)$ are chosen so to make integral calculation easier. The function $q^*(t)$ must have the property of a pdf too, and $w(t)$ is the "weight" relevant to $q^*(t)$. If we take $w(t)\, q^*(t) = q(t)\ \forall t$, the identity is clearly satisfied (the condition is sufficient, but non necessary). In our case, i.e. in calculating $F(T)$ or $S(T)$, we have $f(t) = 1$ and $q(t) = p(t)$, and we can write:

$$F(T) = \int_0^T p(t)dt = \int_0^{\infty} H(T-t)p(t)dt = \int_0^{\infty} H(T-t)w_f(t)p^*(t)dt = \int_0^T w_f(t)p^*(t)dt \tag{9}$$

The essential feature of the "Forcing the Failure Method" (Vestrucci, et al. 1989) is to take $p^*(t)$ such that:

$$\int_0^T p^*(t)dt = 1, \qquad \text{which implies } p^*(t) = 0 \text{ for } t > T \tag{10}$$

In other words, we force the component (system) to fail (i.e. to have a collision in the system phase space) within the mission time T. The advantage is apparent: dealing with reliability problems, systems are designed in order to have very low failure probability for a given T, yielding very difficult computational problems, while with this choice the system will certainly fail within T.

The problem now is to properly define $w_f(t)$ and $p^*(t)$, and this is usually done in two different ways: with exponential distortion or with linear distribution.

In the case of exponential distortion, we want $p^*(t)$ to be an exponential pdf too; $p(t)$ can still be used, but with a different shape as to satisfy condition (10), i.e.:

$$p^*(t) = p(t) / \int_0^T p(t)dt = p(t)/F(T) \qquad \text{for } 0 \le t \le T \text{ else } p^*(t) = 0 \tag{11}$$

It follows from (11) that $w_f = F(T)$ (independent from t).

Alternatively, the basic idea is to use a completely different pdf for $p^*(t)$, i.e. an uniform pdf (that leads to a linear cumulative distribution, hence), instead of an exponential pdf like $p(t)$. According to this choice, we take:

$$p^*(t) = 1/T \qquad \text{for } 0 \le t \le T \text{ else } p^*(t) = 0 \tag{12}$$

It follows that $w_f(t) = p(t)\, T$ (and it depends on t).

Now let us consider the success probability definition in the frame of the forcing the failure technique. In this case we must use the pdf p*(t) which is equal to 0 for $t > T$, i.e. in the success region of the time domain. Recalling eq. (7), we can write:

$$\begin{aligned} S(T) &= \int_T^{\infty} p(t)dt = 1 - F(T) = 1 - \int_0^{\infty} H(T-t)p(t)dt = 1 - \int_0^{\infty} H(T-t)w_f(t)p^*(t)dt = \\ &= \int_0^T p^*(t)dt - \int_0^T w_f(t)p^*(t)dt = \int_0^T (1 - w_f(t))p^*(t)dt = \int_0^T w_s(t)p^*(t)dt \end{aligned} \tag{13}$$

where $w_s(t)$ is the success weight. The meaning of the last equation is that the transitions s→f which happen for $t > T$ are expressed through those which happen for $t \le T$, as it must be as far as these are the only allowed transitions. If we require $w_s(t)$ to be constant, then it follows that $w_s(t) = S(T)$. We wish to point out that the use of the forcing the failure technique is appropriate if the time domain is divided in two intervals and the interest is definitely confined to only one of them. In particular, the semi-infinite interval (T, ∞) is treated in a global manner (for $t > T$, we are not interested in knowing when the system fails).

THE EXTREME CASE OF THE "TOTALLY FORCED" FAILURE TECHNIQUE

Let us suppose to apply a similar global approach to the remaining time interval $[0, T]$, in the sense that we are not interested in all the values of time in this interval, but we consider a particular value as representative of the whole interval. A natural choice is to take $t = T$; forcing the failure at T (exactly at T, and not for $t \le T$) implies that the pdf $p^*(t)$ must be:

$$p^*(t) = \delta(t - T) \tag{14}$$

where $\delta(t)$ is the Dirac delta function. After substitution in eq.(9) we obtain:

$$F(T) = \int_0^T w_f(t)\delta(t - T)dt = w_f(T) \tag{15}$$

i.e. $w_f(T) = F(T) = 1 - exp(-\lambda T)$. It is apparent that with the totally forced failure technique the problem is strongly simplified: the stochastic nature of the simulation is lost and a quasi deterministic approach is attained. The situation can be summarized as in figure 2:

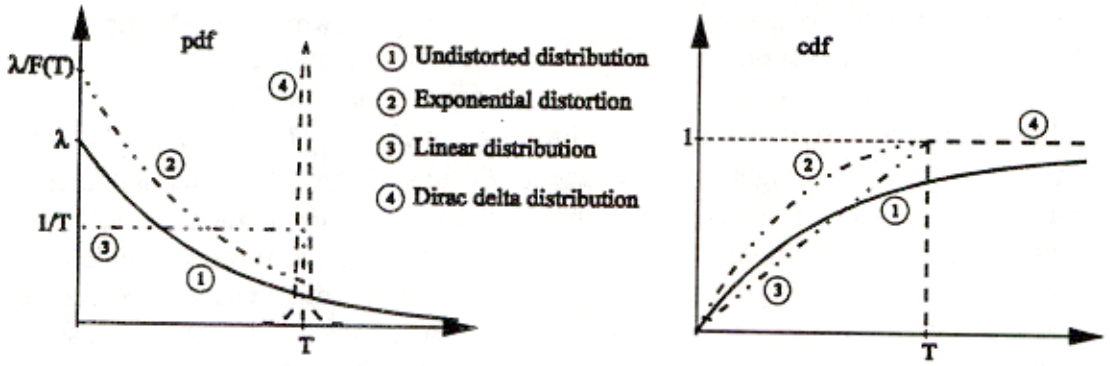


Figure 2. Different pdf and cdf failure probability.

THE DYLAM APPROACH AS A TOTALLY FORCED MONTECARLO

It should be apparent, at this point, that the DYLAM approach can be regarded as an MC simulation in which the system failure is totally forced. This forcing technique is applied, in some sense, following an inverse path respect to the above described one. In fact, once the DYLAM user has defined *Wlim*, the value of t_{BP} (which plays now the role of T) is uniquely determined as $t_{BP} = ln(1/Wlim)/\lambda$ and this is equivalent to taking a delta pdf relevant to t_{BP}, i.e. $\delta\ (t - t_{BP})$, as it can be grasped also from figure 3. Since DYLAM uses the success cdf, in

figure 3 the success cdf is employed also for the Montecarlo trials; this aspect is not essential for the analysis developed in the paper.

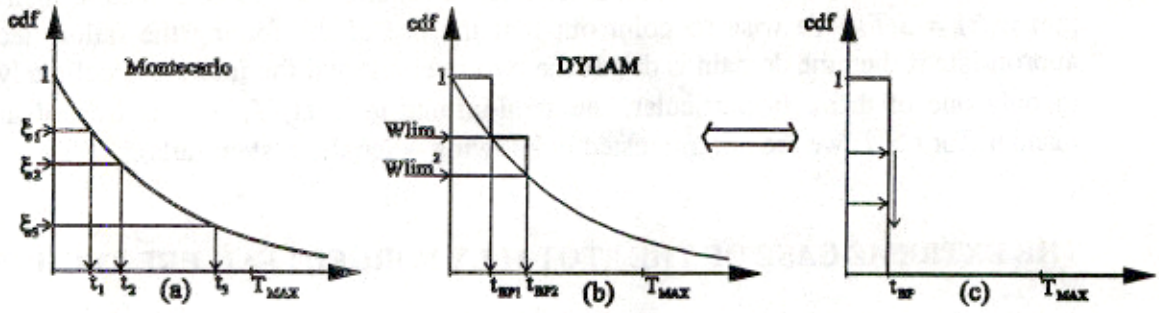


Figure 3. Montecarlo and DYLAM ways of handling transitions.

We can summarize this result by saying that DYLAM is basically a Montecarlo in which we renounce to the stochastic part of the simulation, or, in other words, it is a discretized Montecarlo in which instead of a "continuum" of possibility in history generation, we have a finite (indeed just one between two consecutive branch points) number of cases. In fact, we note that only one (deterministic) history is simulated by DYLAM: the uniform random number extraction, through which random numbers are extracted from an exponential distribution (cumulative distribution) in Montecarlo (see fig. 3,(a)), in DYLAM is substituted by a single "extraction" made in a deterministic way through *Wlim* (see fig. 3, (a), (b)). Two different values of *Wlim* will produce two different histories in the same manner as two random numbers initiate two different histories with Montecarlo. A main difference between DYLAM and Montecarlo is that with Montecarlo a large number of histories are required, while with DYLAM just one.

Now we can make an additional step in the comparative analysis, at a first glance in contradiction with the last statement: we want to explain why DYLAM results approach the Montecarlo ones (i.e. approach the exact ones) if *Wlim* goes to 1.

A feature of the forcing the failure technique is that the history at any failure can be splitted into two parts: the first one (failure), with weight $w_f(T)=1-exp(-\lambda\ T)$, and the second one (success), with weight $w_S(T) = exp(-\lambda\ T)$. In the case of monocomponent the success part of the system can continue the history and usually one or more failures can be forced again. This procedure yields to a generation of a history tree, as it is called in DYLAM method which applies to its single-history approach this Montecarlo feature. The failure is always forced through *Wlim* and the tree dimension will depend upon the choice of this parameter. At each node of the tree, a relevant probability is assessed in a consistent way completely equivalent to the weight associated by Montecarlo method to a particular history. In the case of a monocomponent system, the DYLAM method generates a new branch (or sub-history) by using again the *Wlim* parameter to the previous branch point probability. The technique can be conveniently presented as in figure 1, in which it is possible to visualize the property that the branch point time values are all multiple of t_{BPI}, or equivalently the values "extracted" in the probability domain [0, 1] are not taken in an uniform mode, as in Montecarlo, but with a power law (all these feature can be easily derived analytically). The distances between the probabilities are (using the definitions given in figure 1):

$$d_1 = 1 - Wlim,\quad d_2 = Wlim - Wlim^2 = Wlim\,(1 - Wlim),\ \ldots,\ d_N = Wlim^{N-1}\,(1 - Wlim)$$

which decrease with N. It is apparent that if *Wlim* is close to 1, the powers of *Wlim* will not go rapidly to 0 and it should be $d_1 \cong d_N$ (i.e. constant with N), at least for N not too large. In this

case DYLAM tends to perform a discretized uniform extraction in [0, 1], approximating the uniform continuos random extraction (typical of Montecarlo) with an equally-spaced points choice. Incidentally we notice that, at least from a theoretical point of view, the DYLAM could be improved by changing slightly the method of branch point generation letting the points in the co-domain be equally spaced.

CONCLUSIONS

Dynamic reliability approaches provide the way of coupling the phenomenological and stochastic aspects of the system to be studied and they are essential in order to predict particular sequences which can not be grasped through classical methods (these are of course much more practicable and efficient if only global estimations are required, such as top event probabilities or minimal cut sets analysis). The DYLAM code has been the very first attempt to study the stochastic/deterministic evolution, recently followed by other methods based on MC simulations. This paper showed, how DYLAM, at least in the case of one component, is essentially a Montecarlo with a particular variance reduction technique. This reduces as much as possible the history number, renouncing to some stochastic aspects of Montecarlo.

REFERENCES

Aldemir, T., 1987, Computer assisted Markov failure modeling of process control systems, *IEEE Trans. on Reliability*, R-36 No. 1:133.

Aldemir, T., 1992, Quantifying setpoint drift effects in the failure analysis of process control systems, *Rel. Eng. and System Safety*, 24:33.

Amendola, A., Reina, G., 1981, Event sequence and consequence spectrum: a methodology for probabilistic transient analysis, *Nucl. Sci. Engng.* 77:297.

Cacciabue, P. C., Amendola, A., Cojazzi, G., 1986, Dynamic logical analytical methodology versus fault tree: the case of the auxiliary feedwater system of a nuclear power plant, *Nucl. Tech.*, 74(2):195.

Cacciabue, P.C., Carpignano, A., Cojazzi, G., 1991, Dynamic reliability analysis by DYLAM methodology: the case study of the CVCS of a PWR, in: "Probabilistic Safety Assessment and Management (PSAM)", G. Apostolakis, ed., Elsevier, N.Y..

Cacciabue, P.C., Carpignano, A. and Vivalda, C., 1992, Expanding the scope of DYLAM methodology to study the dynamic reliability of complex systems: the case of chemical and volume control in nuclear power plants, *Rel. Eng. and System Safety*, 36:127.

Cojazzi, G., Cacciabue, P.C., Parisi, P., 1993, DYLAM-3, A Dynamic Methodology for Reliability Analysis and Consequences Evaluation in Industrial Plants, Theory and How to Use, Commission of the European Communities, EURATOM Report EUR 15265 EN.

Deoss, D.L., Siu, N., 1989, A Simulation Model for Dynamic System Availability Analysis, MITNE-287, Massachusetts Institute of Technology.

Devooght, J., Smidts, C., 1992a, Probabilistic reactor dynamics-I: the theory of continuous event trees, *Nucl. Sci. and Engng*, 111:229.

Devooght, J, Smidts, C., 1992b, Probabilistic dynamics: the mathematical and computing problems ahead, Proc. NATO ARW on the "Reliability and Safety Assessment of Dynamic Process Systems", August 24-28, 1992, Kusadasi, Turkey, to be published by Springer-Verlag in the NATO ASI series F Vol. 120, Berlin, Germany.

Limnios, N., 1988, Reliability evaluation of reservoir systems, *Rel. Eng. and System Safety*, 23:65

Marseguerra, M., Zio, E., 1992, Approaching dynamic reliability by Monte Carlo simulation, Proc. NATO ARW on the "Reliability and Safety Assessment of Dynamic Process Systems", August 24-28, 1992, Kusadasi, Turkey, to be published by Springer-Verlag in the NATO ASI series F Vol. 120, Berlin, Germany.

Smidts, C., Devooght, J., 1992, Probabilistic reactor dynamics-II. A Monte Carlo study of a fast reactor Transient, *Nucl. Sci. and Engng*, 111:241.

Vestrucci, P., Santucci, R., Calderan, R., 1991, Monte Carlo simulation of crew responses to accident sequences, *Rel. Eng. and System Safety*, 31:129.

012 Methods/Data and Applications for Improving Human Reliability in Plant Operations

Chair: G.W. Hannaman, SAIC

Human Reliability Database for In-Plant Application of Industry Data
G.W. Hannaman (SAIC); A. Singh (EPRI)

Risk Management Activities to Address the Impact of Human Errors and Human Error Variability
J.C. Higgins, J.M. O'Hara (BNL)

Generic Event Trees and the Treatment of Dependencies and Non-Procedural Actions in a Low Power and Shutdown Probabilistic Risk Assessment
J. Forester (SAIC); D.W. Whitehead (SNL); J. Darby (S&EA); J. Yakle (SAIC)

HUMAN RELIABILITY DATABASE FOR IN-PLANT APPLICATION OF INDUSTRY EXPERIENCE

G. W. Hannaman[1] and Avtar Singh[2]

[1]Science Applications International Corporation
10210 Campus Point Drive MS A1
San Diego, CA 92121

[2]Electric Power Research Institute
3412 Hillview Ave.
Palo Alto CA 94303

INTRODUCTION

Learning from both in-plant and industry experience can help enhance safety and reduce cost of plant operations. Utility engineers currently assess events that occur in nuclear plants throughout the world for in-plant applicability. Established computer information networks, documents, bulletins and other information sources provide a large number of event descriptions to help individual plants benefit from this industry experience. The activities, for coordinating reviews of event descriptions from other plants for in-plant applications, require substantial engineering time to collect, organize, evaluate and apply. Database tools can help engineers efficiently handle and sort the data so that they can concentrate on understanding the importance of the event, developing cost effective interventions, and communicating implementation plans for plant improvement.

The aim of an Electric Power Research Institute (EPRI) human reliability project is to provide utility personnel with cost effective computer tools to support the in-plant use of industry event experience for reduction of operation and maintenance costs and improvement of plant reliability. By applying lessons-learned from many events to specific in-plant tasks and activities, the overall plant reliability can be improved. The process can be applied to support plant safety, to reduce human errors, the number of licensee event reports (LERs) and unplanned reactor trips. The software tools provide the capability to increase efficiency in processing large data sets, provide data for evaluating lessons learned, and can monitor the effects of enhancements on plant reliability through trending. A software package called RECIPE (Reliability Enhancement through Classification of Industry and Plant Events) can support the activities outlined in this paper.

DEVELOPING A CLASSIFICATION FRAMEWORK

Before events can be reviewed systematically or otherwise related by similar features, the events must be classified. The need for a classification taxonomy to address human reliability issues has been recognized for years[1]. Many classification systems have been developed, each to address specific needs[2]. As the classification systems describing human error modes improved, data collected helped build new models and understanding leading to better event descriptions[3]. These in turn helped refine the classification systems for the HRA example database. The initial classification system considered reviews of over 10,000 industry documents describing events that occurred during LTFP operations at the US nuclear power plants[4]. The classification taxonomy was upgraded and modified as more data were collected and the sophistication of the queries increased.

Summary of Classification Framework

In addition to the standard event information the classification system was developed to address (l) human system interactions, (2) human errors, and (3) human reliability shaping factors. The classification system categories include the following.

- **Human -System Interactions:** that focus on the human interactions with systems, functions, shutdown operations, barriers, general and specific effects. This helps assess the key equipment lineups, system unavailability due to maintenance or testing that defeat important functions such as maintaining RCS inventory. The major categories include :significance of event, shutdown operation activity, plant systems and functions involved in event, and effects on plant systems and functions

- **Human Errors** The purpose of this classification element is to identify the types of human errors, mechanisms, and modes typically considered in human reliability assessments. Many classification schemes exist. However, in terms of human actions and errors, this structure draws upon the EPRI measurements of slips and mistakes in simulators. Slips are errors in task execution; mistakes are errors in task planning and selection. A new category of error called *circumvention* was added. This refers to setting aside rules to benefit the outage. Circumventions can occur when job performers have found by experience that existing rules have no benefits and may have adverse consequences. Alternate procedures may be adopted while official changes are being evaluated. However, adverse consequences can *unexpectedly* occur, especially when the plant is in an unusual configuration, such as during startup and shutdown events. The HRA based classification system helps isolate the role and impact of human actions in causing, controlling and mitigating each event by focusing on the human error and human reliability aspects involved. Recovery actions taken by crews include both proceduralized and nonproceduralized activities. The categories include the number of human errors in event, the personnel type, and error type, mode, and effects

- **Human Reliability Shaping Factors** This category identifies performance shaping factors associated with the tasks classified. These elements were modified and expanded during the evaluation of events. The level of detail in the event reports was not sufficient to examine specific causes, however, the reviewers were able to suggest changes that could reduce the human error potential. The categories include planning, procedures, task design, scheduling, skills development through training, communications, work space design and the task type

BUILDING A DATABASE

A sample data base for examination of human reliability issues during less than full power (LTFP) was developed from a set of event reports by:

1. Selecting a consistent set of event reports.
2. Classifying events from the perspective of human reliability
3. Reviewing the event report summaries and building a sample database for the events in terms of the classification system.

Selecting events for the sample database

Licensee event report (LER) summaries, generated by each utility in response to specified reporting requirements, were selected as example data to illustrate the application. This study selected and examined LERs submitted by plants during the low power and shutdown states. LER event summaries were retrieved through a key word coding system to screen the LERs for LTFP conditions. Additional information sources provided detailed evaluations. The example database includes ten plants to provide a representative sample of US plants. The plants selected represent different vendors, plant ages, and regions of the country. Copies of the LER summaries were provided in parallel to analysts evaluating the events from the perspectives of human errors, human reliability shaping factors, and plant

interactions. Reviewers with backgrounds in human reliability, psychology, plant design and trouble shooting used initial classification schemes to systematically review the events. The selected event reports (650 for shutdown conditions) were classified and integrated into a unifying data base.

CASE STUDIES OF LESS THAN FULL POWER EVENTS

The classifications were integrated into a unifying data base stored in a PC system to allow for queries to rapidly sort the event data. The process of integrating lessons and insights gained from single events into an overall LTFP operating insights included three steps.

1. Integrate each event's information using data base software.
2. Draw insights by queries of the data base.
3. Qualitatively verify the findings by comparing with other sources.

The data were stored in a PC-based database system to allow rapid retrieval and review of event data. The LERs were classified for their potential impact on the key safety functions during LTFP[5,6]. The safety function categories are: (1) decay heat removal, (2) reduced electric power reliability, (3) loss of reactor coolant system (RCS) inventory, (4) fuel pool or reactor cavity inventory, (5) reactivity shutdown margin, and (6) fuel handling. In each data classification system the elements were expanded to account for situations which were not accounted for in the initial classification structure. While each event was unique, the analysts recognized repeated patterns and characteristics. This resulted in a system for developing insights about human reliability during LTFP conditions. The sample database, however limited, helps focus on key parameters or causes contributing to the risk, and provides insights with regard to risk management and contingency planning.

Insights can be drawn from the data base by first defining a question. Answers to the following example questions can help engineers identify ways to reduce the causes or consequences of the errors.

1. What caused initiating events such as loss of power during outages?
2. How reliable are the QA checks during outages?
3. What are the key factors affecting human reliability during outages?

Once a question can be defined, queries of a relational data base can be used to generate data and insights. While the results are based on the generic data and may not apply to a specific plant, generic human reliability improvement opportunities for outage operations have been identified from a data base.

The results of queries can be presented as a series of numerical values derived from the relational data base by sorting on various categories. Comparisons can be made by plotting the number of events in each category. This provides identification of the most frequent contributors to incidents that occur during shutdown. The interpretations illustrate the capability to derive insights from a sample database. This qualitative example database includes human errors and causes observed during maintenance, surveillance and testing activities in less than full power and outage operations.

Insights from the Case Studies

Queries of this relational data base were also used to generate insights from this collection of LER events. The insights are based on the generic data and may not apply to a specific plant. Key insights include:

Loss of the electric power during an outage has recurred at more than three plants. These events occurred when normal electrical systems (e. g., Diesel Generators, or switch gear), were out for maintenance and concurrently scheduled activities in the switchyard accidentally caused damage to the key source of power (e.g., use of a crane grounded the high voltage lines or a truck backed into an operating transformer). A simple cost effective solution or lesson learned is to administratively stagger tasks with a significant error probability that could damage electric power sources. This example also illustrates the need

for systematic communication tools to help the on site engineers better translate and communicate the experience from other plants to avoid a repeated event.

The key human reliability shaping factors were prioritized by examination of the primary and secondary causes of initiating events. These are:

- **Procedures-** These include cases where the procedures were generic and inadequate for the task being performed, an error was in the procedures, or no procedure was available. For example, the procedure weakness led to misunderstanding of the current configuration (as a result of faulty procedures, drawings, and temporary labeling interfaces especially in the electrical and instrumentation systems).

- **Skill/experience** - The experience of the individual was less than needed to accomplish the task, and development of skills needed before an outage to reduce the error potential.

- **Planning** - The key contributors were that planning was lacking in the areas that triggered the event, the general approach to planning and specific outage planning aspects contributed to the event. Errors in planning and scheduling affected multiple activities before the outage (affecting heat removal redundancy).

- **Task Design** - This aspect relates to scheduling and other factors affecting the facilities needed to accomplish the task or work order.

- **Information Display** - This element includes cases where the information interface related to the task were improperly displayed in labels, procedures, instruments, etc. This is an important cause of misunderstanding the system configuration and can lead to wrong train wrong unit selections.

- **Communication/Coordination-** This element includes errors traceable to poor communication or lack of coordination between outage personnel.

- **Work Space** - This aspect applies to design and layout of the work space. Nearly all the events selected for this category were outside the control room in the plant facilities.

- **Other-** This category was quite large because of the difficulty in getting enough detail directly from the LERs.

The data in the LERs mainly focus on ESF actuations and losses of safety functions. Very little information is available from this source for other cost and risk aspects such as causes of delays in the outage schedule.

BENEFITS

Database computer tools help support the in-plant use of industry event experience for reduction of operation and maintenance costs and improvement of plant reliability. By applying lessons-learned from many events to specific in-plant tasks and activities, the overall plant reliability can be improved. The software tools and test database provide the capability to increase efficiency in processing large data sets, provide data for evaluating insights, and can monitor the effects of enhancements on plant reliability through trending. Utility engineers currently assess lessons learned from events that occur in plants throughout the world for in-plant applicability. Established computer information networks, documents, bulletins and other information sources provide a large number of event descriptions to help individual plants benefit from this industry experience. Each event provides the seed for an improvement opportunity that can be developed, and evaluated for its cost-benefit of implementation.

It is up to each utility to develop an in-plant process for using this information. The process can be applied, for examples, to reduce human errors, the number of licensee event reports

(LERs) and unplanned reactor trips. An aim of the Electric Power Research Institute (EPRI) human reliability enhancement project is to provide software tools that can help engineers more efficiently perform the process of understanding, assessing, and applying information contained in the events to enhance plant operation.

SOFTWARE

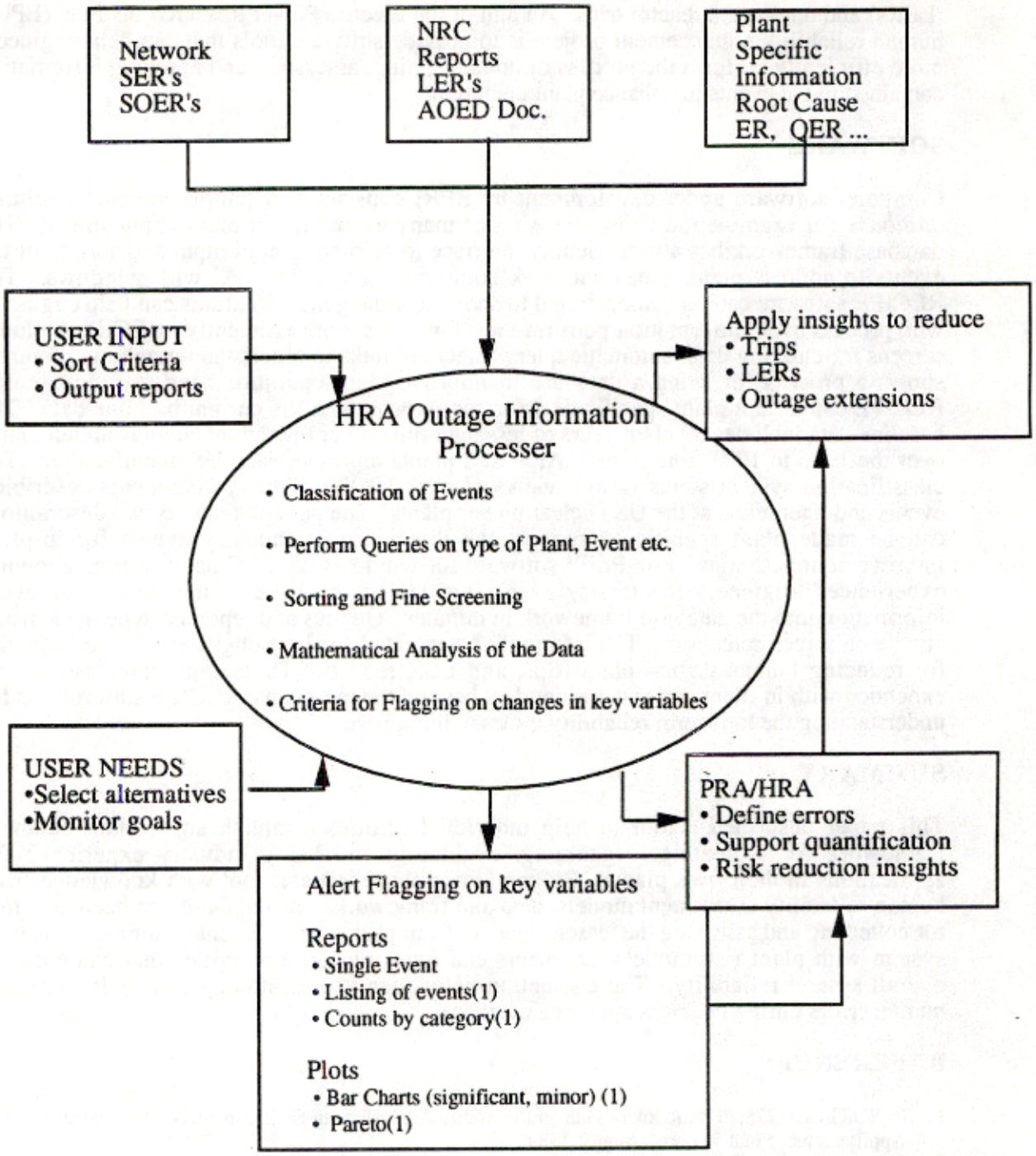
Computer software under development by EPRI consists of a sample *human reliability database* for examination and processing of many events for in-plant applicability. The database framework has a user friendly interface to help both rapid input and sorting of the events to address plant issues and seek solutions for use on a PC with windows. The RECIPE software can be demonstrated to show how the generic features can help engineers who process event information perform their functions more efficiently. RECIPE includes screens for entering data, automatic query selection, links to reports and graphing. Figure 1 shows a process for using a database to improve plant operations and to reduce costs. RECIPE can accept plant specific data for comparison with the current baseline data. The baseline data includes 60 plant years of less than full power operational data from ten plants over the 1986 to 1991 time frame. At least 2 plants represent each US manufacturer. The classification system stems from reviews of over 10,000 industry documents describing events and operations at the US nuclear power plants. The generic features and descriptions can be made plant specific to support the direct use of industry events for in-plant improvement activities. Fox Pro™ software for windows on a PC handles files allowing experienced engineers to classify events written in the LER format and enter event information into the database framework in minutes. Queries and reports can be made using simple on screen selections. The information generated can help engineers devise strategies for reducing human errors, plant trips, and LER reports. The sample database can be expanded with in-plant and sister plant data beyond the ten plants, RECIPE's usefulness for understanding the long term reliability issues will improve.

SUMMARY

This paper described a tool to help individual utilities establish an in-plant database framework for collecting, organizing, evaluating and using industry experience for applications in their own plants. By combining this computer tool with knowledge from human reliability assessment models, data and frameworks, the database can become a tool for collecting and assessing the lessons learned from past events. By integrating the database system with plant risk models, engineers can focus on those activities that can enhance overall system reliability. The evaluation helps identify technology and tools to reduce human errors during operations and maintenance.

REFERENCES

1. NUREG/CR-1278, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications: Final Report," August 1983.
2. EPRI-NP-3583, "Systematic Human Action Reliability Procedure (SHARP)," Electric Power Research Institute, Palo Alto CA, 1984. and "SHARP Methodology Report - Systematic Human Action Reliability Procedure (SHARP) Enhancement Project" EPRI Project 3206 SHARP1, Electric Power Research Institute, Palo Alto CA, Sept. 1990.
3. EPRI NP-6560-L "A Human Reliability Analysis Approach Using Measurements for Individual Plant Examination," Electric Power Research Institute Palo Alto CA, 1990.
4. EPRI RP 3333-2 ""Human Reliability Lessons Learned from Events During Less Than Full Power Operations" EPRI Project SAIC 92-1173 Rev 4, July 1993.
5. Seabrook Station Probabilistic Safety Study (Shutdown Modes 4, 5, and 6)," New Hampshire Yankee, May 1988.
6. EPS-1300, "Probabilistic Safety Assessment of Reactor Unit 3 in the Paluel Nuclear Power Centre (1300 MWe)," Electricite de France, May 1990.



1 Based on selection criteria of the user

Figure 1 Process for Using Human Reliability Data Base to Improve Plant Operations

RISK MANAGEMENT ACTIVITIES TO ADDRESS THE IMPACT OF HUMAN ERRORS AND HUMAN ERROR VARIABILITY[1]

J. C. Higgins and J. M. O'Hara
Engineering Technology Division
Brookhaven National Laboratory (BNL)
Building 130
Upton, New York 11973 USA
(516) 282-2432 FAX (516) 282-4900

INTRODUCTION

Risk to public health and safety from nuclear power plant (NPP) operation is typically evaluated by a comprehensive, integrated analysis of the plant including, systems, components, and personnel. This analysis is termed probabilistic risk assessment (PRA) or probabilistic safety assessment (PSA.) The personnel or human actions are quantified through a human reliability analysis (HRA.) The importance of human activities to overall plant safety, or conversely to plant risk, has been recognized for some time both by risk analysts and by investigators of actual events that have occurred at NPPs. The question naturally arises as to how best to improve human performance and thus limit risk from human error. The answer should be some combination of activities that addresses both actual problems endemic to a particular plant and that prevents problems which have been identified analytically and which have a high risk significance. Particularly important errors that can be identified through a PSA are the errors contained in low probability, high consequence accident sequences.

This paper will first examine various aspects of risk significant human actions or errors identified in PSAs, such as uncertainty, variability, importance ranking, and risk sensitivity. It will then address risk management activities associated with human actions, both PSA-based and otherwise. Finally, it will discuss how these risk management activities may affect the PSA error modelling.

HUMAN ERROR UNCERTAINTY AND VARIABILITY

The likelihood of failing to correctly perform a human action is estimated as a human error probability (HEP.) In PSA studies, human error modelling and HEP quantification is performed using various techniques [1,2]. There has been much work over the last decade in this area to improve the methodology for both modelling the

---

[1] Work done under the auspices of the U.S. Nuclear Regulatory Commission.

human actions and quantifying the HEPs. Nevertheless, it is still an area with the potential for substantial improvements.

HEPs, as with other PSA data, are typically given as mean values. The mean value of the HEP is somewhat difficult to precisely determine, because of both uncertainty and variability factors[3].

Uncertainty represents those sources which contribute to the analyst's inability to accurately estimate the measure of central tendency of human performance, i.e., the mean HEP. Sources of uncertainty include four major areas: lack of sufficient data on human performance in NPPs, inexactness of the HRA models, differences in task descriptions and performance shaping factors between that being modelled and the data, and the skill and knowledge of the HRA analyst[4]. Uncertainty can be thought of as being information limited. That is, as more information about a particular human action becomes available, the uncertainty in the point estimate becomes less. Improvements in modelling, highly-skilled analysts, rich data sources, and minimizing the need for generalization across tasks will all reduce uncertainty. Thus the richer the data, the lower the uncertainty.

The second category, referred to as variability, represents the fluctuation in actual human performance due to differences in personnel. Theoretically, these differences in personnel could be split into: 1) variation between individuals resulting in a fluctuation around the point estimate, and 2) a variation in entire groups of individuals due to systematic causes, which would change the point estimate itself. The differences in individual personnel performance are due to many factors such as education, motivation, and training. These personnel differences can change with time both temporarily (e.g. on a daily or weekly basis) and over longer periods, say due to maturation. The variation of entire groups of individuals due to systematic causes may occur at a given plant over time, due to changes in staffing, management, culture, training, etc. Such group variability may be reflective of different plants. As a practical matter, such a precise differentiation of variability is not feasible: hence, we combine these types of variability together.

While uncertainty can theoretically approach zero, variability in human performance cannot. Variability about the point estimate is determined by human performance shaping factors and not data limitations. Increasing the data will not reduce the variability. It may provide a stronger basis upon which to estimate variability, but improving the data available to the analyst does not reduce the variability with which plant personnel perform tasks which are modelled in the PRA. Some types of actions are more precisely known and have less inherent variability.

Values for both uncertainty and variability were determined and utilized in BNL studies on the sensitivity of risk to human errors[5,6]. The four uncertainty factors, noted above, were combined to derive a composite uncertainty error factor (the factor by which the mean HEP may be increased or decreased.) This composite uncertainty factor was between 7 and 25 depending on the type of human action in question.

Additionally, a separate study was performed at BNL[3] to examine the human performance literature and determine available data on human variability as defined above. This study, somewhat surprisingly, determined that data on this aspect of human performance was quite sparse. However, the available information indicated that for simple action execution tasks, performance typically varied up and down from the mean by a factor 2 or 3. For more complex tasks (e.g. involving diagnosis) a variability factor of 10 appeared to be more appropriate.

IDENTIFICATION OF IMPORTANT HEPs IN PSAs

Once a PSA has been completed, analyses can be performed to obtain insights on how to limit, or even reduce risk due to a variety of causes, such as human error. Importance analyses, to identify risk significant errors, can be performed using different importance measures, such as: Fussel-Vesely, Birnbaum, risk achievement, and risk reduction. These measures allow one to determine how the errors affect risk in different ways. For example, Fussel-Vesely measures the rate of change of risk relative to the error or event of interest. The Birnbaum and risk achievement importance measures show how much risk will increase if the error in question is assumed to occur (i.e. an HEP equal to 1.0). Conversely, risk reduction shows how much risk will decrease if the error is assumed to never occur (i.e. an HEP equal to zero.) The importance measure selected will depend on the insight desired.

Sensitivity analyses, where the HEPs are varied over ranges based on uncertainty and variability, can also be performed to gain insights. This type of study shows what will happen to risk as human performance varies over ranges that are feasible, either at a given plant (over time or as crews change), or between plants. Sensitivity studies performed at BNL[5,6] have shown significant risk effects when increasing or decreasing HEPs from the typically used mean values.

As an example of the type of overall sensitivity that can be expected, Figure 1 shows the effect of variability in human error probabilities on the total internal events core melt frequency (CMF) at two plants. In this analysis all of the human errors were placed into groups, such as operations errors or test/maintenance/calibration errors. Variability error factors were determined for the groups, which ranged from 2 to 10. The HEPs were then allowed to increase and decrease from the base case value (B in the Figure) as a function of the error factor for their group. The results show the effect on CMF due to changes in HEPs caused only by variability (not including uncertainty.) The points shown on the Figure were calculated and the curves themselves are least squares fits. These curves show the significant effect on risk of variation in human performance.

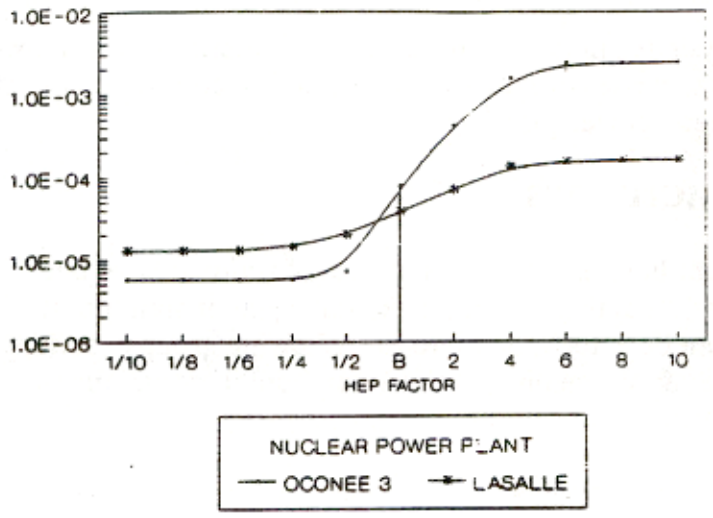


Figure 1. Human variability factor.

In addition to performing sensitivity calculations by varying all human errors, one can also vary them individually or in groups. In this way the relative sensitivity of the groups can be compared. Figure 2 employs this technique to show that the CMF is much more sensitive to the "during-accident" errors than the "pre-accident"

errors at the selected PWR plant. This can be used as one way of judging risk significance. Note that the CMF is quite sensitive to both increases and decreases in the HEPs of the during-accident errors.

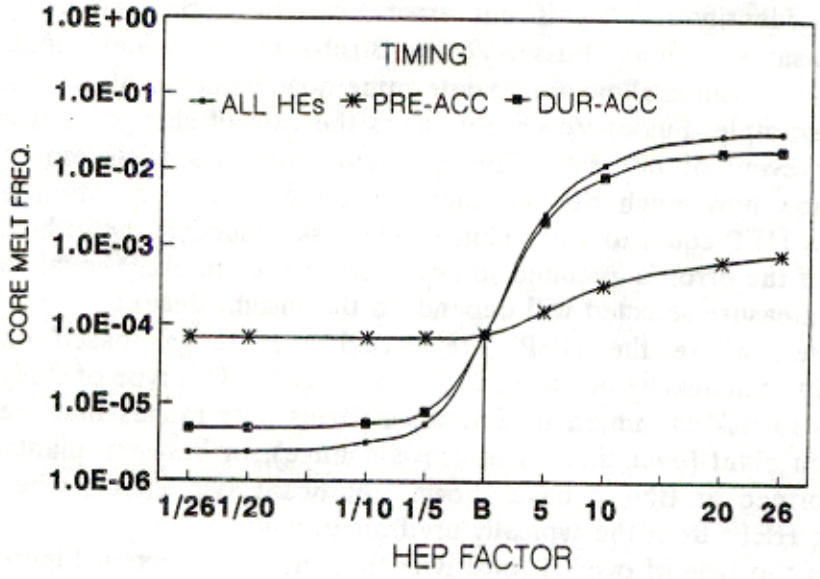


Figure 2. Sensitivity of CMF to pre-accident and during accident errors.

As an example of the sensitivity of risk to a single error, a recent BNL study for an advanced light water reactor (ALWR) design analyzed the dominant steam generator tube rupture (SGTR) sequence. This sequence consisted of a SGTR initiator, failure of high pressure safety injection, and then failure of the operator to aggressively cool down the secondary plant (and in turn the primary plant.) If the HEP of the action was increased by a factor of 15 (which is less than the typical error factor for such a human action), then the sequence frequency also increases by almost 15 times. This caused the sequence to change from 16% of core damage frequency (CDF) to 73% of CDF.

Thus, these analysis techniques can be used to determine the importance of individual human actions, classes of human actions, and overall human performance to the safety of the nuclear power plant.

RISK MANAGEMENT ACTIVITIES

Once the important human actions (or classes of actions) have been identified, there are many ways to address them from a risk management standpoint. These risk management activities can be categorized into the following groups: actions based on PSA insights, corrective & preventive actions for actual occurrences, and other general preventive activities.

I. Actions Based on PSA Insights:

1. Plant Design Modifications - Design modifications, based on important sequences have been made at many plants. PSAs have identified areas where significant credit had to be given to operators to reduce risk to reasonable levels. Design changes were instituted to correct this situation and thus reduce risk without undue dependence on operator action. In the case of new or advanced reactors (where PSA can be used in the design process), insights

from such analyses can be used to support better designs. Designers may also want to incorporate human error tolerance features into the design. PSA can help to identify candidate areas for such design concepts.

2. Procedural Enhancements - Emergency, abnormal, and normal operating procedures can be upgraded based on identified important scenarios of the PSA. Utilities, however, should be cautious not to "clutter" routinely used procedures with actions for "far-out" low probability events.

3. Training - Risk significant human actions can be incorporated into the operators' simulator and classroom training programs. This is important, since these actions are often of the type that operators rarely, if ever, get an opportunity to practice during normal operations. This training can also identify further changes needed in procedures.

4. PSA Training - Operators and other plant personnel can receive training on PSA insights, including important human actions.

5. Emergency Drills - When annual emergency drills are performed, scenarios are developed based upon an initiating accident. Use of the PSA and can result in the selection of realistic and risk significant scenarios for use, which can then provide operational training in the selected important areas.

6. Accident Management Strategies Guidance - Important PSA sequences and human actions can be useful in developing strategies that typically would go beyond the normal plant's design basis and operating/emergency procedures.

7. Prioritization of activities - The PSA and HRA can be used to prioritize a host of plant activities such as valve checks, maintenance, QA audits, inspections, testing, design reviews, etc. This prioritization can be done interactively with a PSA on-line, as well as off-line by analysis.

II. Corrective & Preventive Actions:

While the actions noted in this section are not derived from PSA studies, they are also important to address in a risk management program, since they represent actual experience from the plant in question.

1. Problem Correction - A tracking system is often set up to address particular identified problem areas (e.g. human failures.)

2. Root Cause Analysis - Events that occur at a plant need to be analyzed to determine that proper corrective action has been taken. The more significant failures (particularly the human failures) are typically analyzed for root causes, which can then be addressed through a variety of programs to better prevent the recurrence of similar problems or events.

3. Human Performance Improvement Programs - A variety of these type of programs exist at utilities. They often address the broad-based and more general root causes, as opposed to the specific root causes of particular events.

4. Human Performance Evaluation System - This is a voluntary program of the Institute for Nuclear Power Operations (INPO), that is being used at certain plants to evaluate and improve human performance.

III. General Preventive Actions:

The training in I.3 above and many of the other items noted in I and II above are targeted at specific errors and actions. The training and programs are more general and intended to improve overall performance.

1. Licensed Operator Training.
2. Non-licensed Operator Training.
3. Selected Programs at Individual Plants targeted at particular problem areas such as valve misalignment.

EFFECTS OF RISK MANAGEMENT ACTIVITIES

The broad spectrum of activities, noted above, addresses human errors from PSAs, as well as other types of human performance issues. The activities to address actual occurrences can be tracked to monitor for downward trends in the occurrences of concern.

The activities that address the HEPs of the PSA, affect risk and performance in several ways. Certain activities, such as I.1, I.2, I.3 and I.6 would tend to lower the mean HEPs of particular, identified high significance errors. Training related activities (e.g. I.3, 4, & 5, and III.1, 2, & 3) would tend to both lower the mean by improved performance and to reduce the variation around the mean by providing for more uniformity of operator response to given situations. Item I.1 and I.6 may actually remove selected errors entirely from the PSA sequences by substituting automated actions. Activities under items II and III could serve to shift whole classes of errors to lower HEP values. By taking a broad based approach that incorporates many of the above techniques, a facility could reduce the overall sensitivity of risk to human error.

REFERENCES

1. "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG-1278, Swain & Guttmann, August, 1983.

2. EPRI NP-7183SL, "SHARP1 - A Revised Systematic Human Action Reliability Procedure", December, 1990.

3. W. Brown, D. Crouch, J. Higgins, J. O'Hara, & S. Wong, "The Quantification of Human Variability and Its Effect on Nuclear Power Plant Risk", BNL Technical Report L-1170 (1) 10/90, October, 1990.

4. "PRA Procedures Guide," NUREG/CR-2300, January, 1983.

5. "Risk Sensitivity to Human Error," NUREG/CR-5319, P. Samanta, S. Wong, S. Haber, W. Luckas, J. Higgins, D. Crouch, April 1989.

6. "Risk Sensitivity to Human Error in the LaSalle PRA," NUREG/CR-5527, S. M. Wong, J. Higgins, J. O'Hara, D. Crouch, W. Luckas, March 1990.

GENERIC EVENT TREES AND THE TREATMENT OF DEPENDENCIES AND NON-PROCEDURALIZED ACTIONS IN A LOW POWER AND SHUTDOWN PROBABILISTIC RISK ASSESSMENT*

John Forester,[1] Donnie Whitehead,[2] John Darby,[3] and Jeffrey Yakle[1]

[1]Science Applications International Corporation, Albuquerque., N.M.,
[2]Sandia National Laboratories, Albuquerque., N.M.,
[3]Science & Engineering Associates, Inc., Albuquerque., N.M.

INTRODUCTION

Sandia National Laboratories was tasked by the U.S. Nuclear Regulatory Commission to perform a Probabilistic Risk Assessment (PRA) of a boiling water reactor (BWR) during low power and shutdown (LP&S) conditions. The plant chosen for the study was Grand Gulf Nuclear Station (GGNS), a BWR 6. In performing the analysis, it was found that in comparison with full-power PRAs, the low decay heat levels present during LP&S conditions result in a relatively large number of ways by which cooling can be provided to the core. In addition, because of the less stringent requirements imposed on system operability by the technical specifications for certain LP&S states, the number of system configurations possible is large and the availability of plant systems is more difficult to specify. These aspects of the LP&S environment led to the development and use of "generic" event trees in performing the analysis. The use of "generic" event trees, in turn, had a significant impact on the nature of the human reliability analysis (HRA) that was performed. This paper describes the development of the event trees for the LP&S PRA and important aspects of the resulting HRA.

GENERIC EVENT TREES

While the number of plant configurations possible during LP&S can be addressed to some extent by constraining the PRA analysis to specific plant operational states (POSs) such as cold shutdown or refueling, even within a particular POS there is still a relatively

*This work was supported by the U.S. Nuclear Regulatory Commission and performed at Sandia National Laboratories, which is operated for the U.S. Department of Energy under Contract Number DE-AC04-76DP00789.

large number of system configurations that would need to be modeled. The modeling problem is further compounded by the fact (noted above) that the low decay heat levels present during LP&S allow a relatively large number of ways to provide core cooling.

In the "usual" approach to developing event trees, the different possible system configurations would be specified "up-front" in the initiator specific event trees. However, since the plant configuration at the time of a particular accident would obviously have an impact on which operations could be used to respond to an accident, and because the number of configurations and operations possible during LP&S is large, it became clear that attempting to specify all the possible configurations up-front for each specific initiator would require the development of a unacceptably large number of specific event trees for each initiator. It was determined that the event tree development task could be significantly reduced through the use of "generic" event trees that were based on the different operations that could be applied to respond to an accident occurring in a BWR 6. In most cases, the operations possible in response to any given initiator that threatened the core would be the same (some of which are specified by procedure) and would only be constrained by the existing system configurations and availabilities. Thus, it was decided that the event trees would be developed by asking questions about the configurations possible, in the context of each of the possible operations. The result was event trees related to accident response operations, which could be used for most of the initiating events analyzed. The trees were "generic" in the sense that they were designed in terms of the general operations possible in response to an accident in a BWR 6, as opposed to being drawn as a function of a specific accident.

For example, several operations, using any of several different injection systems, are possible for providing core cooling in response to a loss of the normal means of shutdown cooling. The operations include initiating a closed-loop water solid operation per procedure, steaming the vessel at low pressure, flooding the vessel/containment, or steaming the vessel at high pressure. Separate event trees were developed for each of the possible operations and relevant questions regarding operator actions, existing system configurations and system availabilities were asked in each of the operation-specific event trees. The specific impact of a given initiating event was taken into account by setting system unavailabilities accordingly.

An example of an event tree used in the LP&S study is presented in Figure 1. The tree (the "E" tree) represents one of the operations possible in response to a loss of the normal means of shutdown cooling, which could occur in the context of many different initiating events. The operation covered is that of initiating closed-loop water solid operation with an available Emergency Core Cooling System (ECCS). Water solid operation is clearly indicated in the GGNS Off-Normal Event Procedure (ONEP) for inadequate decay heat removal. The operator decision and action for initiating ECCS water solid operation is represented by the event labeled OPECS. Depending on the pattern of successes and failures in the accident scenario prior to reaching OPECS, a number of operator actions could be required in addition to those indicated by the ONEP. For example, if the operators were initially using the Alternate Decay Heat Removal System for shutdown cooling as opposed to the Residual Heat Removal shutdown cooling system, a more complex pattern of system isolations would be required to initiate ECCS water solid operation with the Low Pressure Core Injection System. Moreover, if normal vessel "letdown" had not yet been isolated, this action would also be required at this point. The OPECS event is followed by a series of events asking questions regarding the status of the main steam isolation valves (ISMSV, OPMSV, MSIV), the status of safety relief valves (2SRV, 1SRV), whether the operators would proceed with ECCS water solid operation with only one safety relief valve open (OP1SV), the water level in the suppression pool (ISSP, SPMLV), and the availability of the ECCS systems (LPCS, LPCI, OPHIS, HPCS).

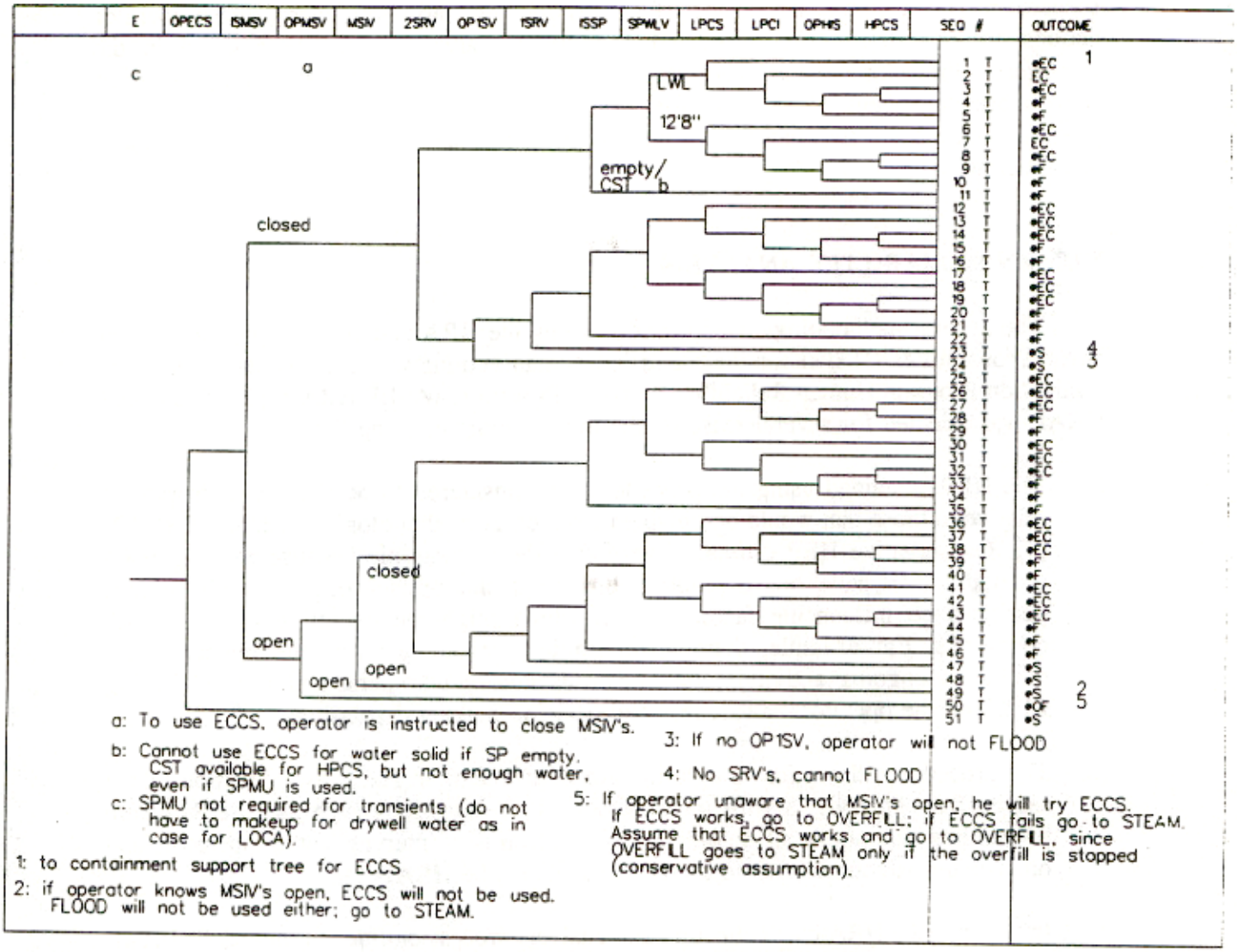


Figure 1. Event tree for initiating ECCS water solid operation after a loss of normal shutdown cooling.

Another important advantage of the use of generic event trees was that the approach allows the same event trees, or only slightly modified trees, to be used across analyses for different POSs. For example, the loss of shutdown cooling related trees discussed above would in general be applicable during most POSs such as cold shutdown, refueling with the water level at the main steam lines, and refueling with the water level raised and the upper pools connected. The use of more or less the same event trees across analyses for different POSs should, in principle, not only be more efficient, but should also allow a straightforward comparison of core damage frequency across the different POSs.

The resulting event trees were somewhat more complex and lengthy and they contained more frequent and more complex operator diagnosis/action events than is typically found in full-power PRAs. The increased complexity of the event trees and operator actions were in part due to the nature of the event trees. That is, since the trees were based on the multiple operations possible to respond to an event and, as determined by the initiator, a variety of systems could be available to support those operations, the trees and events were necessarily more complex. However, the nature of the operator actions were also different as a direct function of the LP&S environment. At full power, many of the operator action events in response to an accident simply involve the manual initiation of a system that has failed to auto-initiate. For such events, the indications and related operator diagnosis/actions are approximately the same regardless of the accident

scenario in which they occur. In the LP&S environment, however, many of the operator actions are not strictly proceduralized and are not always explicitly covered in the Emergency Procedures. Moreover, diagnosis and performance of many of the operator actions are dependent on the initiator and on what has occurred or failed to occur previously in the accident sequence. This aspect of the analysis will be discussed in more detail below.

HUMAN RELIABILITY ANALYSIS

The general methodology used for conducting the HRA and determining the Human Error Probabilities (HEPs) for the identified human actions was the Accident Sequence Evaluation Program Human Reliability Analysis Procedure (ASEP HRAP) [1]. The ASEP HRAP was selected for several reasons, the more important being that:

(1) The HEPs obtained using the procedure are considered to be slightly conservative relative to those that would be obtained from other methodologies such as "THERP" [2]. Conservative HEP estimates were considered desirable because existing HRA methodologies have not explicitly considered the impact of potentially unique performance influencing factors (PIFs) which might be operative during LP&S conditions. For example, there is no explicit way to factor in the impact of the numerous ongoing activities and numerous non-regular personnel present during LP&S on the operators' awareness and decision making capabilities.

(2) The procedure allows for straightforward adjustments in HEPs as a function of the results from interviews with plant personnel. In situations such as LP&S, where procedures may not be all encompassing, the results of interviews with operators and other plant personnel become a critical aspect of the HRA.

In general, the HRA data collection and analysis process outlined in the ASEP HRAP was followed. One exception was that the pre-accident human actions included in the analysis used the same HEP values that were used in the full-power PRA of GGNS reported in NUREG/CR-4550, Vol. 6, Rev. 1 [3]. Thus, less emphasis was placed on collecting information relevant to pre-accident human action quantification. Nevertheless, procedures related to control of work on plant equipment and facilities, protective tagging systems, outage organization, shutdown protection plans, and surveillance on shutdown related systems were obtained from GGNS and examined.

To obtain information relevant to analyzing the post-accident human actions contained in the event and fault tress, interviews with operators and other plant personnel were conducted over a two-day period. The general level of understanding conveyed by plant personnel about the various accident scenarios addressed in the analysis was used by the HRA analyst in determining the HEPs. In most cases, information obtained from interviews was used in conjunction with the ASEP HRAP in determining whether the nominal (median) HEP or the upper or lower bound value from the ASEP HRAP diagnosis model, should be used in estimating the HEP for a particular diagnosis. In some cases, interview results indicated that operators would simply not do some of the actions included in the event trees.

Treatment of Dependencies and Non-Proceduralized Actions

As discussed above, the use of generic event trees and the nature of the LP&S environment had a significant impact on the HRA. Since system configurations and

availabilities were not specified in the initial initiating event trees, they had to be considered in each of the operation related event trees. Furthermore, since the impact of failures to accomplish certain operations could have a bearing on other operations that might be attempted, it became clear that dependencies within the various accident scenarios would need to be considered. The fact that many of the possible operations were not explicitly proceduralized also indicted that a careful analysis of the sequences would be needed. Therefore, in order to accomplish a reasonably valid HRA analysis, it was necessary to do a sequence by sequence analysis of the human actions contained in the event and fault trees and to attempt to account for the dependencies among the different operator actions.

Several general guidelines were used in the treatment of non-proceduralized operator diagnoses/actions and dependencies across operator actions within an accident scenario. The guidelines included the following:

(1) In general, credit was given for operators correctly diagnosing and carrying out a non-proceduralized action if, on the basis of the site interviews, it was judged that the operators had a clear understanding of the event in question and of the requirements for responding to the event. For example, while the operation of steaming at low pressure is not explicitly described in GGNS procedures, the site interviews indicated that it would be a viable option.

(2) In most cases, credit was not given for a non-proceduralized action if a critical human action, clearly indicated by procedure, had failed earlier in the sequence being analyzed and the pattern of failures across the sequence suggested operator "confusion". For example, if the operators failed to initiate ECCS water solid operation when it was clearly indicated by procedure, credit for steaming at low pressure (a non-proceduralized action) was not taken.

(3) In determining the requirements for a particular operator diagnosis\action event in a given sequence, any human actions necessary for the success of the sequence, that had failed in earlier events, could be addressed again in an appropriate subsequent event. For example, a manual system isolation (e.g., isolation of vessel letdown) may be necessary for the success of a sequence. If a human action event which included that task had failed earlier in the sequence, but the context of a subsequent human action event in the sequence legitimately allowed that task to be addressed again, the performance of that task would be taken into account in determining the HEP for the subsequent event.

(4) Complete or zero dependence across events in a sequence was assigned as a function of the logical relationship between those events. For example, in a given human action event, it may have been possible for an operator to use any of several systems to respond to the problem. However, if limited time was available for the event being analyzed, credit for trying all the available systems may not have been taken at that point. Therefore, any subsequent events which assumed that a particular system had been initiated when it hadn't, would be set to fail. Similarly, if an event included the initiation of a system, appropriate subsequent events asking initiation of that system would be set to succeed.

The above guidelines often required subjective judgments on the part of the HRA analyst. These judgments were based on the impressions drawn from the interviews with plant personnel, on examinations of the relevant procedures, and on the basis of discussions with the other analysts on the PRA team.

Since generic event trees were used for the PRA, the operator actions asked in the analysis of the accident sequences for the different initiators were in general the same. However, because the various initiators have differing impacts on the system and therefore the nature of the accident sequences, the HEP for the same operator action could vary across initiators. Furthermore, the HEP for the same operator action could also vary within the analysis of a particular initiator as a function of the different system and operator successes and failures occurring in the different sequences. Therefore, multiple HEPs were possible for a given operator action. For example, the operator action for diagnosing and initiating ECCS water solid operation (OPECS) had 22 different values ranging from 0.003 to 1.0. A total of 115 HEPs was calculated for the approximately 40 human action events included in the analysis.

SUMMARY

The unique aspects of the LP&S environment and the resulting use of generic event trees required that each human action event be carefully examined in the context of each of the different accident sequences in which they occurred. In conducting the sequence by sequence analysis, non-proceduralized human actions had to be considered and attempts were made to address relevant dependencies across events within given scenarios. The LP&S environment appears to demand a more detailed and complex HRA than that usually performed for full-power operations.

REFERENCES

1. A.D. Swain, "Accident Sequence Evaluation Program Human Reliability Analysis Procedure," NUREG/CR-4772, February, 1987.
2. A.D. Swain and H.E. Guttman, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, August, 1983.
3. M.T. Drouin et al, "Analysis of Core Damage Frequency: Grand Gulf, Unit 1 Internal Events," NUREG/CR-4550, Vol. 6, Rev. 1, Part 1, September, 1989.

013 Nuclear Reactor PSA Applications

Chair: B.O.Y. Lydell, NUS

Application of Petri-Nets-Based Model to Reliability and Risk Analysis of Nuclear Power Plant

G. Petkov (Risk Eng., Bulgaria); S. Doytchinov (Tech. U., Bulgaria)

K Reactor Restart Configuration - Level 1 Internal Events PRA Results (U)

S.P. Tinnes, D.S. Cramer, V.E. Logan, S.V. Topp, J.A. Smith, H.A. Ford, R.T. Bailey, M.D. Brandyberry, B.G. Kingery (Westinghouse Savannah Rvr.)

Predictability Versus Availability High Flux Isotope Reactor

L. Merryman (ORNL), E. Ballon, B. Christie (RAPA)

APPLICATION OF PETRI-NETS-BASED MODEL TO RELIABILITY AND RISK ANALYSIS OF NUCLEAR POWER PLANT

George Petkov[1] and Stefan Doytchinov[2]

[1] Risk Engineering Ltd.,
3 Ogneborec St., 1619 Sofia, Bulgaria
[2] Systems Optimization Laboratory,
Department of Industrial Engineering, FA, Bl.9,
Technical University, Sofia 1156, Bulgaria

INTRODUCTION

Nuclear Power Plant (NPP) reliability and risk analysis requires: 1) proper understanding of physical and logical nature of the conditions in which the system works, of their functions and the interactions of the components and their subsystems; 2) adequate interpretation of reliability models of the above characteristics that presupposes knowledge of the modeling techniques - of their capacities and their suitability for the specific purpose.

One, even two modeling techniques cannot cover the whole variety of plant operational modes and system states[1,2]. An acceptable strategy of modeling such an object is the application of a simple technique, leading to analytical decisions and supplemented by simulation in cases, when such decisions prove to be difficult or impossible.

The paper presents an alternative method of NPP reliability and risk analysis with respect to the traditional Fault Tree (FT) method. The method is called Analysis of Topological Reliability of Digraphs (ATRD)[1] and uses Physical Modeling Graph (PMG) and Petri Nets (PN) techniques, making possible the revealing of the interactions of the components and subsystems in all operational modes. The combination of a technique leading to analytical decisions (PMG) and a technique suitable for simulation (PN) provides the possibility for directing the method to events and to processes as well.

OVERVIEW OF ATRD

ATRD modeling consists in transformation of plant schematics and operational procedures into success digraph. Modeling algorithm is structured and has two salient attributes: global and local (on this point the method is analogous to DMA[3]).

Global: System structure is modeled as it works.

Local: System components are modeled in success space.

ATRD Structural Model

ATRD structural model is defined as a directed planar graph. It includes modeling of all physical and logical connections we are interested in: fluid, electrical, controling, topological, represented as edges (arcs). Component common cause failures are similarly represented. The trivial elements are represented as nodes (places in Petri Nets terminology) and operator control is represented by adding inputs and outputs to the net.

We define nodes, edges and model expansion following the definitions used in DMA[3].

ATRD Dynamical Model

The dynamical model includes modeling the duration of the connection time transitions, the variety of the component faults through marking the places, the interaction of the processes and various operational modes of functionally connected systems through coloring the nets.

Description of Operational Mode. Operational mode is described in ATRD with the aid of state parameters included in the model digraph. They characterise the state of various system components (motor-operated valves, air-operated valves, pumps, control valves etc.). A possible visual interpretation for description of modes and presentation of transitions is coloring of the subgraphs of various operational modes.

Description of Event. In ATRD this means, once the operational mode is described, a specification of the success criterion of a component or a subsystem (a group of components or subsystems). It should correspond to the conception of the analyst, including failed components, time diagrams of technological parameters and component states. For a given event the failure mode of each component is specified by marking digraph nodes.

Description of Process. ATRD performs it by the linking the system operational modes with the aid of time transitions.

Operator's control. ATRD allows integration of analysis, check and correction of operator's actions in more general scheme. Figure 1 shows the structure of this scheme. The Fuzzy Logic System (FLS) module contains a set of fuzzy logic rules[4] to model the stored knowledge and experience of the operator, as well as rules, derived from instructions for NPP operation. The rules in the system are specified by linguistic variables denoting the state of chosen components with respect to their availability. Linguistic variables can be as follows: availability_of_element_1, availability_of_element_2 and so on. The term set is {high, medium, low} and fuzzy rules are:

IF availability_of_element_1 **IS** high **AND**
availability_of_element_2 **IS** medium **AND** .....
THEN switch_1 **IS** off, switch_2 **IS** on, ...

Consequence part consists of discrete parameters controled by the operator. We suppose they have crisp values. Availability of components is used as an integral measure of the system state and gives us more clear and common look of the state.

Component availability, as well as membership functions, is represented using weighted arcs in PN[5,6]. Output from the FLS is compared with the operator's actions in the same situation.

Success Criteria

ATRD model is designed trough tracing all physical and procedure connections including the dependence of any node (edge) on any other node (edge). Thus, the problem is modeled as reachability of digraph nodes.

As shown by Satyanarayana[7], the various problems of reachability in graph can be reduced to s-t reachability. Therefore the various success criteria are specified and solved as reachability of nodes (places) of the model digraph. When solving any digraph we derive the topological formula of its reliability. Having solved the equation system, we derive by substitution the global formula of system reliability. Such an approach makes possible lessening the errors.

Model Processing

The solution of the problem of processing the model is realized in analytical and simulation way. The well-known algorithm of Satyanarayana & Prabhakar[8] (S&P) makes possible the substitution of a subset of the net by the formula of its reliability. The algorithm permits stochastic dependence between components. When the model is used for solving various special cases, it can be simplified by postulating absolutely reliable nodes and edges, instant time transition, reduction of marking and operational mode decomposition.

APPLICATION

The model and the computer program realizing ATRD are applied to various analyses of primary circuit circulation system at 5th unit of Kozloduj NPP. It includes the reactor coolant pump (RCP) system and support subsystems.

Model Description

The edges represent physical flow, flow of information and the interaction of components in a shared location.

The nodes represent technologically discernible components of support systems of RCP system. There are two types of nodes: 1) trivial - their reliability depends only on component qualities; 2) complex - their reliability depends on component qualities and on: other components or subsystems, maintenance, actuations, common cause failure, technological parameter signals, protections and interlocks.

RCP system is decomposed into technologically independent components (trivial nodes and edges). When a dependence of various components exists it can be solved by S&P algorithm[8] or by PN simulation.

The model digraph includes the four RCPs, oil systems of RCPs (one system for two opposite RCPs), power supply of RCP system including supply and standby transformers of the unit, air supply system of the unit, protections and interlocks influencing model components and RCP subsystems in the containment. Input and output nodes, specifying the availability of the rest of the system outside the containment, are the results of other studies and expert estimations. The number of trivial edges and nodes is 2313. The number of time transitions is 175 and there are six algorithms for solving them. Equivalent complex components models are unified in module types. Such models are constructed for buses, pumps and heat exchangers. The number of complex nodes is 693.

The availability of the RCPs is modeled as a combination of failure operational mode and two general operational modes: success and standby.

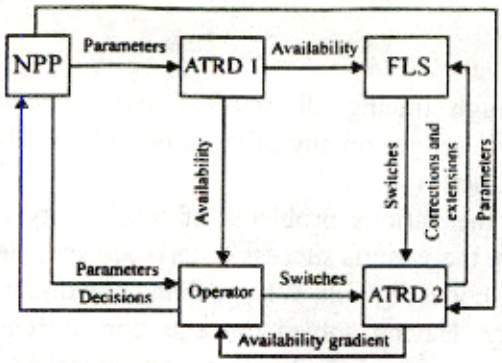


Figure 1. General Scheme of Decision Support of Operator.

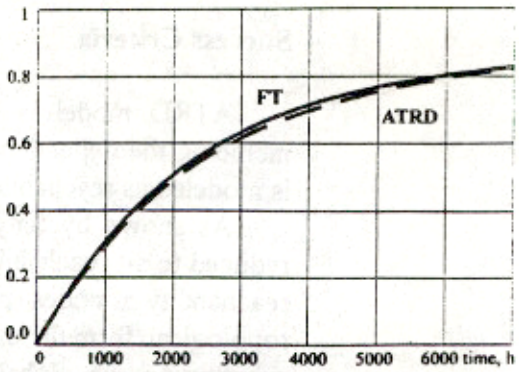


Figure 2. Average probability of failure of at least 1 of 4 RCPs (FT and ATRD methods).

Comparing FT and ATRD methods

We use the results of the comparative research presented in Manchev et al.[9]

FT model consists of 163 components only (in operational mode: four succeeding RCPs of four in total). Fault trees are calculated by IRRAS 2.5.

ATRD confirmed the contributions of various minimal cut sets obtained by FT to system reliability. The contributions of identical components obtained by FT are equivalent and these obtained by ATRD are not. It is due to the fact that ATRD takes into account more structural connections than FT.

Figure 2 shows the results obtained by the two methods. They are very close (deviation less than 1 percent). It is due to the fact that ATRD uses exact reliability algorithm and minimal cut set used in FT increases unavailability.

Analysis of operator and automatic actions in emergency situations.

Figure 3 presents RCP system behaviour in emergency situation "Spurious closing of pneumatic valves." Figure 3 gives instantaneous availability of the main components of RCP3, instantaneous availability of any RCP, as well as the moments of automatic and operator's interventions.

RCP model constructed with the aid of ATRD allows tracing the availability of all components and subsystems described in controled by the operator parameters. They can be traced from the lowest to the highest hierarchical level in real-time (calculation time is less than 1s with IBM/PC 386DX/40). The model enables the operator to receive information about critical system components (Figure 3) and proper automatic action, to develop the strategy of his interaction and to correct the algorithm of his actions.

The operator's aim in the described emergency situation is to turn on at least one RCP. Figures 3a and 3e-h present the availability diagrams of the RCPs, including the moments of operator's and automatic actions. This information makes it possible:

- to check up the correctness of the automatic action;
- to define the suitability of the operator action for the set purpose;
- to specify the optimal actions. For example, operator actions applied to RCP3 components and subsystems (average availability for 152s is 0.485) are considered to be suboptimal with respect to RCP1 - 0.483, RCP2 - 0.337 and RCP4 - 0.333;
- to obtain a sufficient sampling of operator actions in RCP control. It permits defining the probability of operator error. These data can also be used for supplementing and expanding the fuzzy rules implied in FLS module (Figure 1).

Legend. Actions: ● Operator ; ▼ RPC 3 Automatic Control.

Operational Modes: ——— Success: - - - - Standby; . . . . Failure.

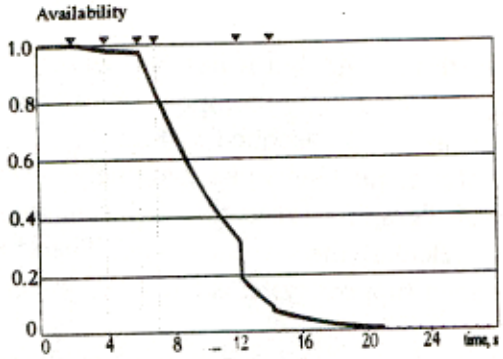


Figure 3a. RCP 3 (until 30s).

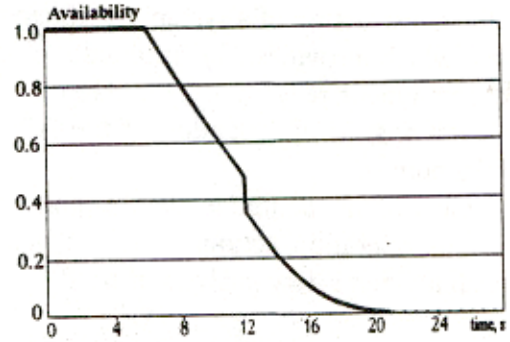


Figure 3b. Motor of RCP 3.

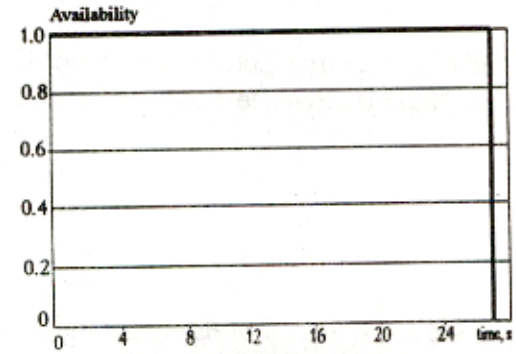


Figure 3c. Control System of RCP 3.

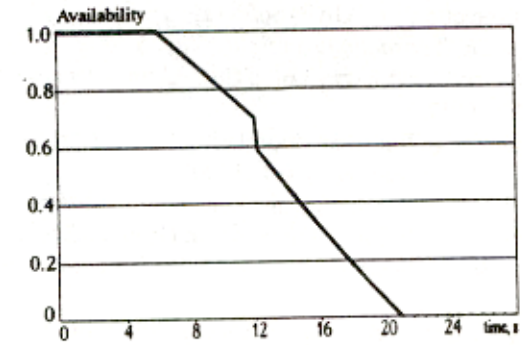


Figure 3d. Main Radial Bearing of RCP 3.

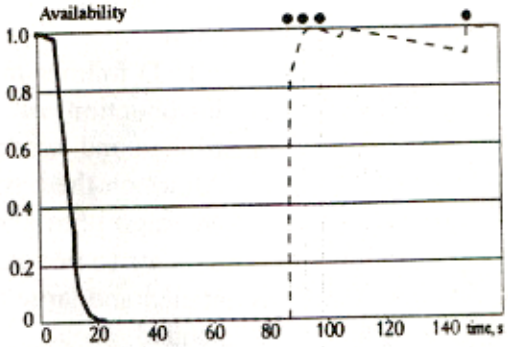


Figure 3e. RCP1.

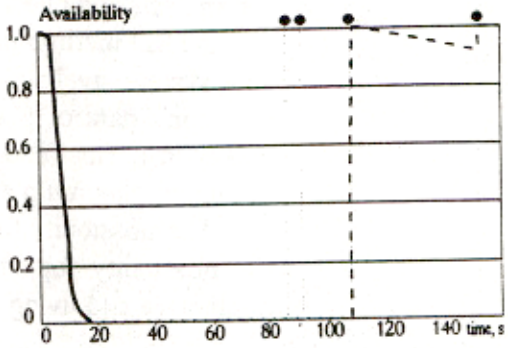


Figure 3f. RCP 2.

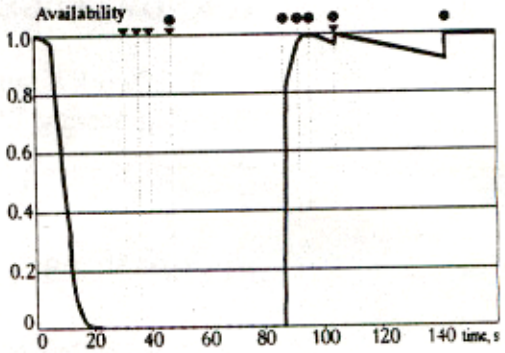


Figure 3g. RCP 3.

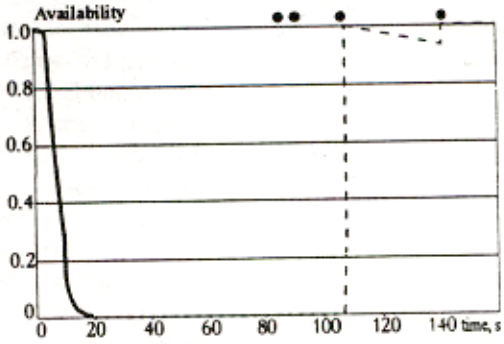


Figure 3h. RCP 4.

Figure 3. Emergency situation "Spurious closing of pneumatic valves".

CONCLUSIONS

Fault tree can be processed trough the ATRD codes but ATRD digraphs cannot be processed trough FT analysis codes without breaking the cycles and using the time transitions.

ATRD follows many ideas set forth in DMA but it has two advantages: first, through the introduction of PN elements and possibility components a dynamical model is constructed and, second, operator's behaviour is described by FLS.

Although the physical and control systems tend to be extremely cyclic[3], the capacities of S&P algorithm allow a conditional digraph representing a system of several thousand components to be easily processed to calculate the s-t reachibility. Therefore models can be so detailed and large that fully developed support systems and common cause initiators can be included.

S&P algorithm does not use truncation probability and minimal cut set. It can be used for analysis and check up of any cut set order, as well as for analysis of sensitivity.

ATRD method makes possible the construction of a system for tracing NPP component and system availability in real time which provides: 1) automating of the system for collecting data of plant system and component reliability; 2) efficient help to the decision maker in normal and "brainstorm" situations; 3) optimization of the NPP management for obtaining maximum efficiency and minimum risk.

The possibility for obtaining reliability of any component and support system, as well as the possibility for simulation of various operation actions provides better conditions for qualitative and living quantitative reliability and safety analysis of NPP.

ACKNOWLEDGEMENTS

This work is supported by Foundation "George Zolotovich" under Grant No. NS-1/92, Risk Engineering Ltd. and Bulgarian National Science Foundation under Grant No. TH-203/92.

REFERENCES

1. G.I.Petkov, "Development of Techniques and Algorithms for Modeling and Analysis of NPP System Reliability", PhD Dissertation, Moscow Power Institute, Moscow (1992).
2. G.I.Petkov, Modeling of reliability and risk of NPP using Petri-like digraphs, in: "Mathematical models in nuclear safety and radiological protection", CPUAE, Sofia (1993).
3. I.J.Sacks, Digraph Matrix Analysis, *IEEE Transactions on Reliability.* 5:437 (1985).
4. C.T.Lin and C.S.George, Neural-Network-Based Fuzzy Logic Control and Decision System, *IEEE Transactions on Computers.* 40:1321 (1992).
5. S.M.Chen, J.S.Ke and J.F.Chang, Knowledge Representation Using Fuzzy Petri Nets, *IEEE Transactions on Knowledge and Data Engineering.* 2:311 (1990).
6. G.R.Sotirov,S.H.Doichinov and D.T.Stefanov, Modelling and control of manufacturing system using fuzzy Petri nets, in:"Proceedings of the 1991 IFAC Workshop on Discrete Event System Theory and Applications in Manufacturing and Social Phenomena, June 25-27, 1991, Shenyang, China", IAP, Beijing (1991).
7. A.Satyanarayana, A Unified Formula for Analysis of Some Network Reliability Problems, *IEEE Transactions on Reliability.* 1:23 (1982).
8. A.Satyanarayana and A.Prabhakar, New Topological Formula for Rapid Algorithm for Reliability Analysis of Complex Networks, *IEEE Transactions on Reliability.* 2:82 (1978).
9. B.L.Manchev, N.N.Hristov, G.I.Petkov, S.H.Dojtchinov and G.P.Halev, Reliability Analysis and Assessment of Systems YD10-40D01 and YD50,60 in Power Unit WWER-1000, BAS-CLSC (1993).

K-Reactor Restart Configuration Level 1 Internal Events PRA Results

S. P. Tinnes, D. S. Cramer, V. E. Logan, S. V. Topp, J. A. Smith, H. A. Ford, R. T. Bailey, M. D. Brandyberry, and B. G. Kingery

Westinghouse Savannah River Company
Savannah River Site
Aiken, SC 29808
(803) 644-5444

INTRODUCTION

A full-scope probabilistic risk assessment (PRA) has been performed for the Savannah River Site (SRS) K-Reactor restart configuration prior to the initiation of lay-up activities in 1993. The Level 1 PRA includes the assessment of reactor systems response to accidents and estimates of core damage. The internal events spectrum includes those events related directly to plant systems and safety functions for which transients or failures may initiate an accident.

The PRA applies to the tritium-producing core design in the K Reactor with the physical layout that existed in 1992-1993. The PRA updates a previous analysis performed for K Reactor that modeled the 1987 configuration. Since 1987, significant hardware changes have been made to K Reactor, and key operating procedures have been revised to improve reactor safety. K Reactor restarted in June 1992 and successfully completed a three-month test and demonstration program, operating at low power. The reactor was then shut down to tie in a new natural draft cooling tower when a decision was made by DOE in April 1993 to place the reactor in cold standby.

The PRA models three different restart configurations. The first case models reactor operation with the June 1992 restart configuration (without the cooling tower). The next two cases model reactor operation with the cooling tower, but with significantly different river water distribution system configurations. The cooling tower configuration with the lowest risk has been chosen as the K-Reactor configuration if restart is authorized.

REACTOR DESCRIPTION

The SRS is located in South Carolina approximately 25 miles southeast of Augusta, Georgia. It is situated in portions of Aiken, Allendale, and Barnwell counties on an area of about 300 square miles. The site, which is owned by the U. S. Government, is set aside as a controlled area for the production of special materials for national defense. The site produces nuclear materials, primarily plutonium and tritium, for the Department of Energy (DOE).

The SRS facilities include one operating reactor (K), which is now in cold standby, and four non-operating reactors (P, C, L, and R) that are almost identical to each other in design and administrative controls. The reactors are sited a minimum of 2.5 miles apart and a

minimum of 4.5 miles from the site boundary. The SRS reactors began operation in 1953 with the primary purpose of producing plutonium and tritium for nuclear weapons. K Reactor has recently undergone an extensive program to upgrade seismic resistance, reactor systems, reactor systems control, and administrative controls to become more nearly equivalent (in risk terms) to those used in the U. S. nuclear utility industry. At present, the reactor is limited to operating at 30% power (30% of maximum historical power). The reactor was successfully restarted in June 1992 and operated at 30 per cent power for about three months before shutting down to tie in a new natural draft cooling tower. Restart of the reactor for a demonstration run with the new cooling tower had been planned for June 1993. However, a decision was made by DOE in April 1993 to place the reactor in cold standby. Prior to the April decision, extensive testing had been performed with the new cooling tower system.

The PRA applies to a tritium-producing core design operating at 30% historical power. The tritium-producing charge uses relatively lightweight highly-enriched uranium-aluminum alloy tubular fuel containing tubular lithium targets, for the purpose of tritium production. The core is moderated by heavy water (D_2O), and the primary coolant is also D_2O. The reactor is cooled by six primary loops, with redundancies in pump motors for these loops and the electric power supplies. The six primary loops are cooled by twelve heat exchangers, which are supplied by water from the Savannah River via a large basin.

Normal operation with the new natural draft cooling tower (NDCT) consists of routing effluent cooling water from the reactor to the cooling tower. Once cooled, the water would be recirculated to the K-Reactor inlet basin. Makeup water to the closed-loop system would be routed to the inlet basin from the river water distribution system. A small blowdown from the system would be maintained. Fresh river water would be blended with the blowdown to maintain a constant rate to the plant effluent.

It is useful in understanding this PRA to note some of the major differences between the SRS reactors and the light water cooled reactors used for commercial production of electricity (LWRs). Since the SRS reactors are not required to produce steam, they operate at low temperature (maximum about 90 degrees C) and low pressure (maximum about 200 psi). There are no concerns with steam blowdown, turbine trip, or other scenarios related to the high stored energy and electricity generation aspects of an LWR. On the other hand, uranium-aluminum alloy fuel clad with aluminum for the SRS reactors melts at a much lower temperature than the uranium oxide, zirconium-clad fuel for LWRs and also has lower heat capacity. The SRS reactors therefore require much faster action to maintain adequate core cooling under accident scenarios.

LEVEL 1 INTERNAL EVENTS METHODOLOGY

Due to the major differences between SRS reactors and commercial power reactors, which affect accident-initiating events, mitigating system designs and the spectrum of possible damage, it is inappropriate to treat this analysis as a perturbation on the PRAs for power reactors. All phases of the analysis are treated as unique to SRS. The duration of all accidents is assumed, by convention, to be 24 hours.

The SRS Level 1 PRA uses the fault-tree linking methodology, which is a well-established technical approach used in many other PRAs. The detailed technical efforts are divided into seven principal task areas:

1. Initiating Event Identification and Analysis
2. Event Tree Development
3. System Fault Tree Development
4. Electrical Power Model Development and Analysis
5. Component and Human Reliability Database Development
6. Sequence Analysis and Compilation of Results
7. Uncertainty Analysis

The task efforts define the expected progression of a potential accident scenario and develop the associated SRS-specific models to represent plant response or to incorporate plant operational experience. The SRS reactors are unique in that initiating events discovered

in analyses associated with other reactor types generally do not apply. Eight different classes of accidents are identified that might yield reactor severe core damage scenarios. Partial and total "Loss of Cooling Tower" have been added as new initiators.

- Transient: An upset of the reactor power-to-flow ratio.
- Primary-Loss-of-Coolant Accident (LOCA): A leak in the primary (D_2O) cooling system.
- Secondary-Loss-of-Coolant Accident: A leak in the light water secondary cooling system that leads to a Loss of Pumping Accident.
- Loss-of-Heat-Sink Initiator: Failure of heat transfer between the primary and secondary cooling systems, requiring emergency cooling.
- Loss-of-River-Water Accident: Failure of the river water supply to the K-Reactor inlet basin, requiring conservation of the water on hand.
- Loss-of-Normal-Power Initiator (LONP): Failure of the normal power supply to K Reactor requiring primary cooling system pumps to be powered from online DC diesel generators and secondary cooling to be provided by gravity flow. A LONP will also shut down the cooling tower system pumps, requiring conservation of the water on hand.
- Loss-of-Cooling-Tower Accident: Failure of the closed-loop recirculating system from causes other than LONP, requiring conservation of the water on hand.
- Partial-Loss-of-Cooling-Tower Accident: A partial failure of the closed-loop recirculating system (reduction in flow), requiring conservation of the water on hand.

For each of these accident classes, the potential accident progression scenarios are developed and modeled as event trees. For the branchpoints, the related plant system responses are identified and system fault trees are developed. Since the original PRA, detailed fault tree models have been developed to replace simplified models used for the Shutdown Systems, Emergency Cooling Activation Systems, and different plant support systems.

The K-Reactor electrical system is analyzed using a Markov model and also by using detailed fault trees. The system fault trees trace the supply of electrical power back to key buses. For the Markov model analysis, the availability and reliability of electrical power at buses is represented as a series of basic events in the fault trees. The Markov model then considers the frequencies of losing normal power, the probabilities of failure of emergency power, and the mean times to repair parts of the electrical power supply for 32 possible configurations. The theoretical model calculates the probability of finding the system in any particular configuration (i.e., combination of buses On or OFF), given some initial condition. Unavailability is calculated by admitting all possible transitions among configurations, both those caused by failures and those caused by recovery steps. Unreliability is calculated by admitting only failure transitions.

Throughout the development of the PRA models, SRS-specific design and operational information are used. Plant design features and response strategies, including operator actions as specified by SRS procedures, are incorporated directly into the models. Actual plant experience, as obtained from incident reports and operator logs, is used to compute SRS-specific component reliability data. The SRS experience-base of 110 reactor-years of operation is available for these computations and is supplemented by generic industry data only when necessary.

By linking the system fault tree models together in the manner indicated by the event trees to represent the accident sequence of interest, and by using the plant-specific data to estimate initiator frequencies and component failure rates, plus estimation of the human error rates, the accident sequence frequencies are quantified. Contributing to the result are over 300 different sequences from the different initiating event classes. The CAFTA code is used to solve the fault trees for their minimal cut sets and to perform the sequence analysis.

Uncertainty estimates are made for the total severe core melt frequency (SCMF) by assigning probability distributions to the basic events and propagating them through a simplified model of the SCMF cut set results. Data for the basic events are derived from SRS-empirical or generic data, and uncertainties in the events are taken to be described by log-normal distributions. Fifth and ninety-fifth percentiles of these distributions are derived from chi-squared confidence interval tests for events where SRS data are available, from error factors quoted for generic data, or from judgment and industry practices for human errors. The simplified SCMF model includes the dominant cut sets from all eight contributing classes of accidents. The basic event distributions are propagated through this simplified

model with either the CAFTA computer code using Monte Carlo Sampling or the TEMAC computer code using Latin Hypercube Sampling to assess the distribution of the SCMF.

COOLING TOWER IMPACT

The new natural draft cooling tower increases the core damage frequency for the reactor, because additional manual actions are required to maintain cooling water and/or Emergency Core Cooling System (ECCS) flow to the reactor during most reactor accidents. These manual actions are to open river water valves at the reactor inlet basin and to start river water pumps at the river water pumphouses.

The original cooling tower and river water distribution system configuration specified that only the minimum number of river water pumps (two pumps) be maintained continuously online to provide makeup flow to the K-Reactor inlet basin. Additional river water pumps would have to be started for almost all accident initiating events (such as a LOCA or a Loss-of-Cooling-Tower) to prevent depleting the reactor inlet basin inventory. Insights from the PRA showed that risk (core melt frequency) could be decreased by maintaining additional river water pumps online.

Extensive cooling tower and river water distribution system flow tests were then performed to determine the optimum flow configuration and the number of online river water pumps required to minimize risk. The tests showed that the optimum configuration is to maintain seven river water pumps continuously online, supplying river water to L, C, and K Areas. With this configuration, additional river water pumps are not required to be started to provide full cooling water flow to K Area. This is the planned cooling tower and river-water distribution system configuration for K-Reactor operation if restart is authorized.

RESULTS OF THE PRA - SEVERE CORE DAMAGE

The SCMF (point estimate) for the final restart configuration at 30% power with the cooling tower is 1.8E-5 per reactor-year from internal initiators. A sufficient number of river water pumps will be maintained online (seven pumps) to provide full cooling water flow to the reactor in the event the cooling tower system becomes disabled. This is compared to a SCMF of 1.3E-5 per reactor-year for the restart configuration without the cooling tower (the June 1992 restart configuration) and 3.9E-5 per reactor-year for the initial cooling tower restart configuration (i.e., with two river water pumps online). The SCMF for the 1987 reactor configuration operating at 100% power was 2.1E-4 per reactor-year. The results lie within the range of values calculated for currently-operating nuclear power facilities using similar techniques.

Contributing to the results are over 300 different sequences from the different initiating event classes. The distribution of the total SCMF among the contributing initiating event classes for the different restart configurations is tabulated in Table 1. Also shown are the mean values and the 5% and 95% confidence values.

Since 1987, significant hardware changes have been made to K Reactor and key operating procedures have been revised to improve reactor safety. Also, better defined Emergency Core Cooling System (ECCS) and shutdown system success criteria based upon current state-of-the-art technology have been developed.

Hardware improvements include a new safety system to cope with small primary LOCAs (the Moderator Recovery System), a new safety system to cope with large secondary LOCAs (the Automatic CW Pump Trip System), and new dedicated diesel generators to supply emergency power to the cooling water recirculation pumps.

Improvements have been made to emergency operating procedures specifying ECCS activation and subsequent ECCS throttling, leak isolation, and actions to cope with the loss-of-river-water incident. These improvements have been coupled with improved reactor operator training, which now includes reactor simulator training. All key procedures are now tested on the reactor simulator. In addition, different accident scenarios are programmed on

Table 1. Level 1 PRA Internal Events Severe Core Melt Frequency Distribution (Restart Configurations)

Class of Initiating Event	1992 K Reactor at 30% Power (without NDCT)	1992 K Reactor at 30% Power with NDCT & 2 RW Pumps (Initial)	1993 K Reactor at 30% Power with NDCT & 7 RW Pumps (Final)
Primary-Loss-of-Coolant (LOCA)	42%	11%	20%
Secondary LOCA (Loss of Pumping)	27%	49%	25%
Transients	8%	3%	6%
Loss-of-Heat-Sink	8%	3%	7%
Loss-of-River-Water	7%	3%	8%
Loss-of-Normal-Power	8%	15%	6%
Loss-of-Cooling-Tower	-	3%	5%
Partial-Loss-of-Cooling-Tower	-	13%	23%
Total SCMF (Per Rx-yr) Point Estimate	1.34E-5	3.90E-5	1.75E-5
Total SCMF (Per Rx-yr) Mean Value	1.26E-5	3.70E-5	1.68E-5
5% Confidence Value	4.07E-6	1.02E-5	4.87E-6
95% Confidence Value	3.17E-5	9.65E-5	4.30E-5

the simulator, and operators are trained to cope with these emergencies using the emergency operating procedures.

Reactor ECCS success criteria have changed significantly from the 1987 100% reactor power case to the 1992-1993 30% reactor power case. New tools (latest revisions of the RELAP and TRAC computer codes) have been used to derive the "best estimate" ECCS success criteria. The 30% reactor power calculations show that fewer ECCS injection paths are now required for success during a primary or secondary LOCA. In addition, Manual Incident Action (MIA) is not required for loss-of-pumping accidents [LOPAs] (to prevent core damage) until well after ten minutes from the start of the incident.

The PRA models have identified several factors that suggest greater attention is warranted. If K Reactor is again restarted, these insights should be considered before returning the plant to an operational status. With the cooling tower installation, secondary LOCAs (LOPAs) contribute to almost one-quarter of the total core damage. The ability to restore river water flow to the cooling water basin is vital, especially during large secondary LOCAs when the cooling water inventory is being depleted from the leak, as well as from activation of the ECCS. The accident is compounded by additional requirements for manual operator actions at the basin. Also, partial and total loss-of-cooling-tower (LOCT) contributes about 28% to the total core damage. In the LOCT case, the cooling water basin inventory is being depleted by routing water to the plant outfall. After reactor shutdown, cooling water conservation steps must be implemented or river water flow to the basin must be increased.

The PRA has identified equipment and human actions, as well as procedures and systems, that dominate the total severe core melt frequency. Attention should be given to these items to obtain the greatest benefit in risk reduction. Ultimately hardware or procedural retrofits, increased operator training, more frequent testing, and increased maintenance activities must be weighed in a cost/benefit context and against future operating plans for K Reactor.

Pipe breaks are a large contributor to the total core damage. The combination of primary and secondary LOCAs cover 45% of the SCMF.

The contribution of sequences associated with emergency cooling cover 59% of the SCMF. These include primary and secondary LOCAs, loss-of-heat-sink initiators, and loss-of-normal-power initiators.

The most dominant sequences, accounting for about 75% of the total SCMF, are as follows:

- A partial or total loss of the cooling tower or a loss of river water and failure to manually shut down the reactor. Note there is no automatic scram available for these accidents.

- A large secondary LOCA pipe break (H_2O leak), failure to isolate the leak, and failure to inject emergency coolant following flooding.
- A primary LOCA bellows break (D_2O leak), failure to isolate the leak (which includes failure to shut down the primary cooling system (PCS) pump AC motors and to activate the Moderator Recovery System), and failure to inject emergency coolant.
- A transient (including loss of normal power) and failure to shut down the reactor.
- A large unisolated secondary LOCA, successful injection of emergency cooling, but failure to increase river water flow to the reactor inlet basin.

Human error dominates the basic event Importance rankings. The human error basic events that rank high in Importance are listed below. Special attention should be given in training operators to cope with these emergencies.

- Operator fails to recognize and initiate a required manual scram when no scram annunciator plates are illuminated.
- Operator fails to activate Manual Incident Action.
- Operator fails to initiate water conservation procedures during a loss-of-cooling-tower accident or loss-of- river-water accident.
- Operator fails to open river water valves at the reactor inlet basin.

APPLICATIONS OF THE PRA

Improvement in understanding the issues involved in SRS reactor safety has been accomplished through analysis of the mechanisms encountered. Insights from the PRA have been applied to reactor safety decision-making in the K-Reactor restart effort. PRA methods and results are included among the bases for evaluating reactor restart issues and for assigning priorities to projects in the Reactor Safety Improvement Program. The use of the PRA and PRA methodology has supported different analyses affecting

- Implementation of "smart" maintenance strategies
- Training for accident and emergency preparedness
- Perspective on equipment unavailabilities
- Awareness of the source and impact of common cause
- Failure rates for piping system materials
- Graded approach to address aging
- Procedure upgrades
- Risk perspectives for radiological releases and Technical Specifications changes
- Means to rank cost effectiveness alternatives
- Project scheduling and prioritization

ACKNOWLEDGMENTS

The information contained in this article was developed during the course of work under Contract No. DE-AC09-89SR18035 with the U. S. Department of Energy.

This paper was prepared in connection with work done under contract DE-AC09-89SR18035 with the U. S. Department of Energy.

PREDICTABILITY VERSUS AVAILABILITY

HIGH FLUX ISOTOPE REACTOR

Larry Merryman

Maintenance Manager
Research Reactors Division
Oak Ridge National Laboratory
Oak Ridge, Tennessee 37831

Eric Ballon and Bob Christie

Reliability Consultants
Reliability And Performance Associates (RAPA)
P.O. Box 53102
Knoxville, Tennessee 37950-3102

ABSTRACT

An analysis to compare the "predictability" versus the "availability" of the High Flux Isotope Reactor (HFIR) at the Oak Ridge National Laboratory was conducted in order to provide input into the design of the Advanced Neutron Source (ANS) Reactor. The analysis covers the period of time from January 1992 to April 1993 since the High Flux Isotope Reactor has kept three-month schedules starting with January 1992.

Predictability is a measure of the percentage of time that a reactor is operating on the days when the advance schedule says the reactor should be operating. The mathematical definition of predictability is discussed in detail in the paper. Availability is defined in the traditional manner.

There were two major conclusions from the HFIR analysis:

- For long-term forecasts without updates, the predictability and the availability of the reactor are basically the same.
- The more often the schedule is updated, the higher the predictability compared to the availability.

Based on these major conclusions, a recommendation was made that the effort to calculate the predictability of the ANS Reactor be redirected toward calculation of the availability of the ANS Reactor. Availability models are much easier to calculate (no explicit time dependency) and are more useful in the design, operation, and maintenance of the reactor. After the ANS Reactor goes into operation, predictability models might be useful for establishing an update frequency for the ANS Reactor schedule and in providing an indication of the probability of having neutrons generated during a specific period of time.

I. INTRODUCTION AND DEFINITIONS

A. Background

If you set a schedule in advance for the time you expect to be at power, you can have four possible outcomes:

1	Said you would be at power	Were at power
2	Said you would be at power	Were not at power
3	Said you would not be at power	Were at power
4	Said you would not be at power	Were not at power

B. Availability

Availability is defined as the ratio of the time you were at power to the total time you want to be at power. With respect to the four possible outcomes listed above, availability is the ratio of the time spent in States 1 and 3 to the time spent in States 1, 2, 3, and 4 since you would like the reactor to run all the time. All the states listed above are applicable to the availability index.

C. Predictability

Predictability can be defined as the ratio of the time you were at power when you said you were to be at power to the total time you said you would be at power. With respect to the four possible outcomes listed above, predictability is the ratio of the time in State 1 to the time in States 1 and 2. State 1 can be considered a success; State 2 can be considered a failure. States 3 and 4 are not applicable to the predictability index.

D. Time Periods

Predictability is calculated over some period of time. In order to see the trend in predictability, it is advantageous to use a sliding value over some time period.

To use a 30-day (calendar) sliding value, take the last 30 calendar days, count up the number days you were at power and you said you would be at power (State 1 above) and the number of days you said you would be at power (states 1 and 2 above). Predictability will be the ratio of the two. For a 90-day (calendar) sliding value, substitute 90 days for 30 days.

II. HFIR SCHEDULES

Schedules for HFIR have been generated since January 1992. The schedules have generally been published for a three-month period.

A. Theoretical 12-Month Forecast

All the schedules that were published since January 1992 were examined. Two places were identified where the End of Cycle outages were predicted in advance to be longer than usual: End of Cycle 305 predicted a 24-day outage for Hydro Cooling Tower work; End of Cycle 309 predicted an eight-day outage to change control plates.

A theoretical 12-month forecast for 1992 was calculated based on a 21- to 22-day power run and a 5- to 6-day outage for all cycles except 305 and 309. If this theoretical forecast had been followed, HFIR would have gone through cycle 316 during the year. HFIR actually got to cycle 314.

B. Three-Month Forecast

A three-month theoretical forecast was made based on the first time anything was scheduled for that day. Once something was scheduled for a given day, it stayed fixed no matter how many updates were made.

C. Periodically Updated Forecast

The forecast was changed to include the latest information for every update that was made.

III. RESULTS

Each forecast was analyzed for two cases of predictability: 30-day (calendar) sliding value and 90-day (calendar) sliding value

HFIR availability was also calculated for 30-day sliding values and 90-day sliding values. This was done to compare the predictability versus the availability for the various forecasts and cases.

A. Predictability

The predictability of HFIR for the various forecasts are shown in Figures 1 through 3:

Figure 1, Theoretical 12-Month Forecast (30- and 90-day sliding values),
Figure 2, Three-Month Forecast (30- and 90-day sliding values),
Figure 3, Periodically Updated Forecast (30- and 90-day sliding values).

HFIR PREDICTABILITY				
Forecast	Period	Range, %, 30 Day	Range, %, 90 Day	Eyeball Average %
12 Month	Calendar	0 - 94	50 - 81	62
3 Month	Calendar	0 - 100	55 - 86	69
Periodic	Calendar	0 - 100	55 - 93	78

B. Availability versus Predictability

The availability versus predictability of HFIR for the various schedules are shown in Figures 5 through 10:

Figure 4, Theoretical 12-Month Forecast (90-day sliding value),
Figure 5, Three-Month Forecast (90-day sliding value),
Figure 6, Periodically Updated Forecast (90-day sliding value),
Figure 7, Theoretical 12-Month Forecast (30-day sliding value),
Figure 8, Three-Month Forecast (30-day sliding value),
Figure 9, Periodically Updated Forecast (30-day sliding value).

C. Conclusions

As seen in Figures 1, 2, and 3, predictability goes up the more the schedules are updated. The Theoretical 12-Month Forecast Predictability has an average of about 62% while the Periodically Updated Forecast Predictability has an average of about 78%.

As seen in Figure 4 and Figure 7, for long-term forecasts without updates, the availability and predictability are basically the same.

As seen in Figure 6 and Figure 9, the predictability can be as much as 20% above the availability when numerous updates are made to the schedules.

IV. RECOMMENDATIONS

A recommendation has been made that the effort to calculate the predictability of the ANS Reactor be redirected toward calculation of the availability of the ANS Reactor. This recommendation was made because it is believed to be much easier to calculate availability than predictability. Availability models do not require the explicit time dependencies that appear to be required for predictability models.

Availability models are also generally understood by a larger portion of design engineers and are believed to be more useful at the design stage. After the ANS Reactor goes into operation, predictability models might be useful for establishing an update frequency for the ANS Reactor schedule and in providing an indication of what would be the probability of having neutrons generated during a specific period of time.

HIGH FLUX ISOTOPE REACTOR
Predictability of a Theoretical 12 Month Forecast

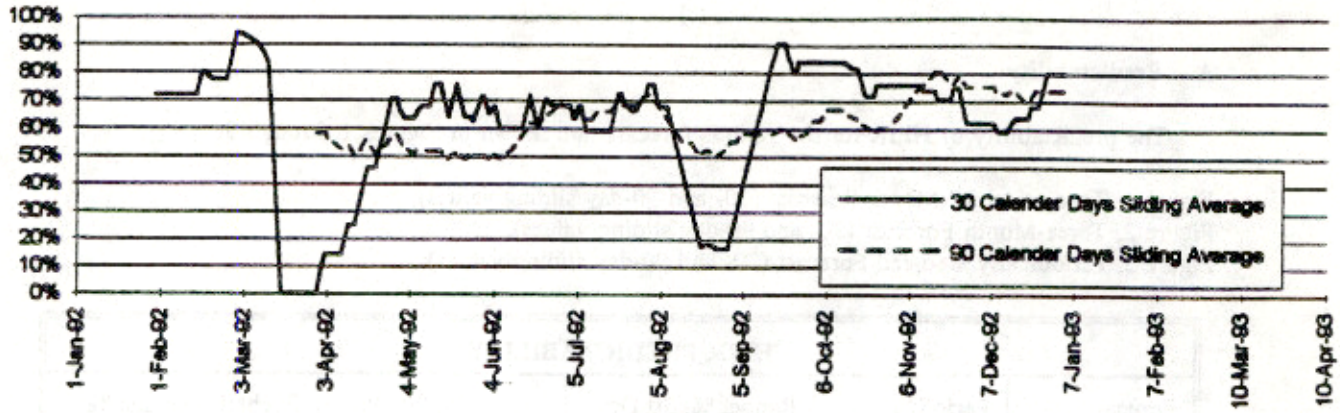


Figure 1

HIGH FLUX ISOTOPE REACTOR
Predictability of a 3-Month Forecast

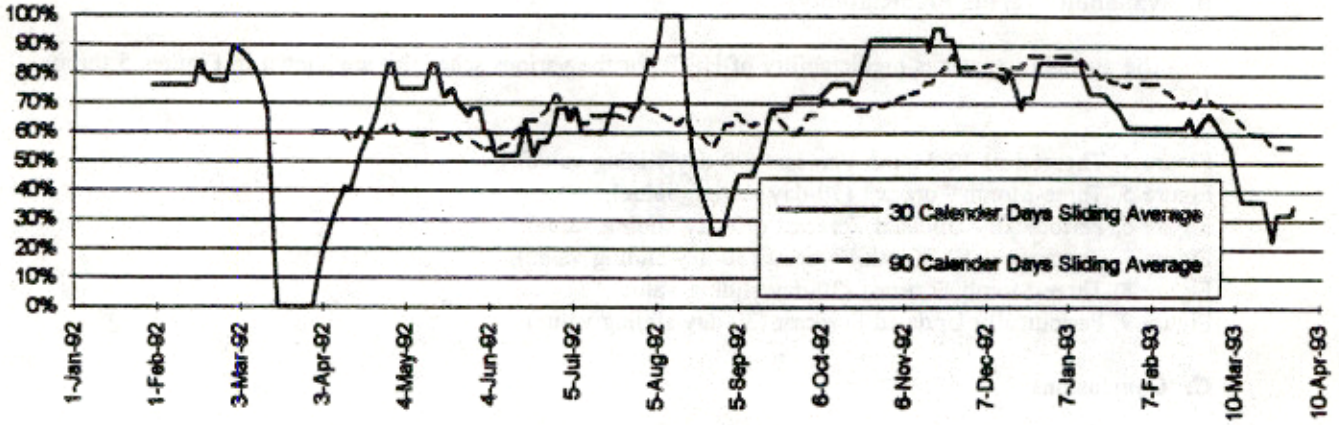


Figure 2

HIGH FLUX ISOTOPE REACTOR
Predictability of a Periodically Updated Forecast

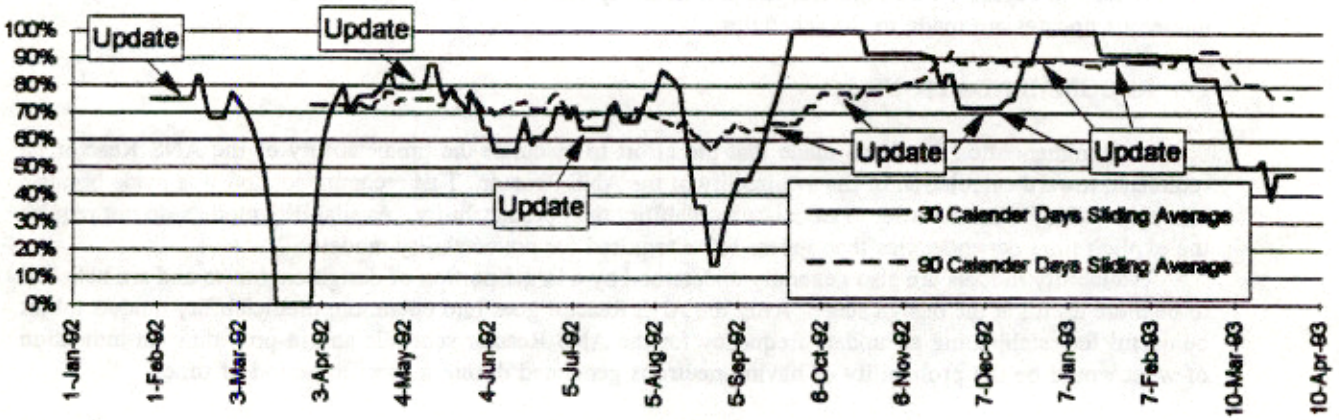


Figure 3

HIGH FLUX ISOTOPE REACTOR
Predictability vs. Availability of a Theoretical 12 Month Forecast

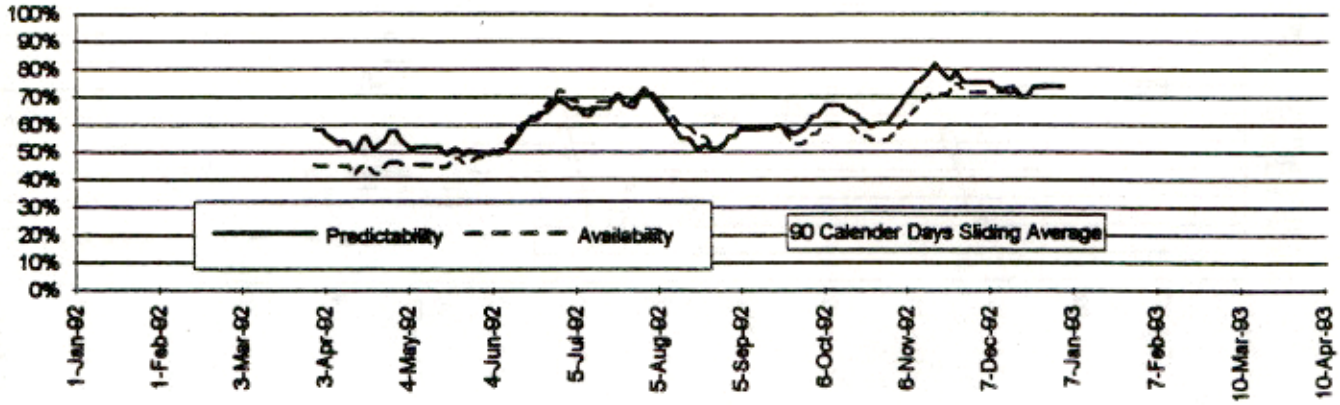


Figure 4

HIGH FLUX ISOTOPE REACTOR
Predictability vs. Availability of a 3-month Forecast

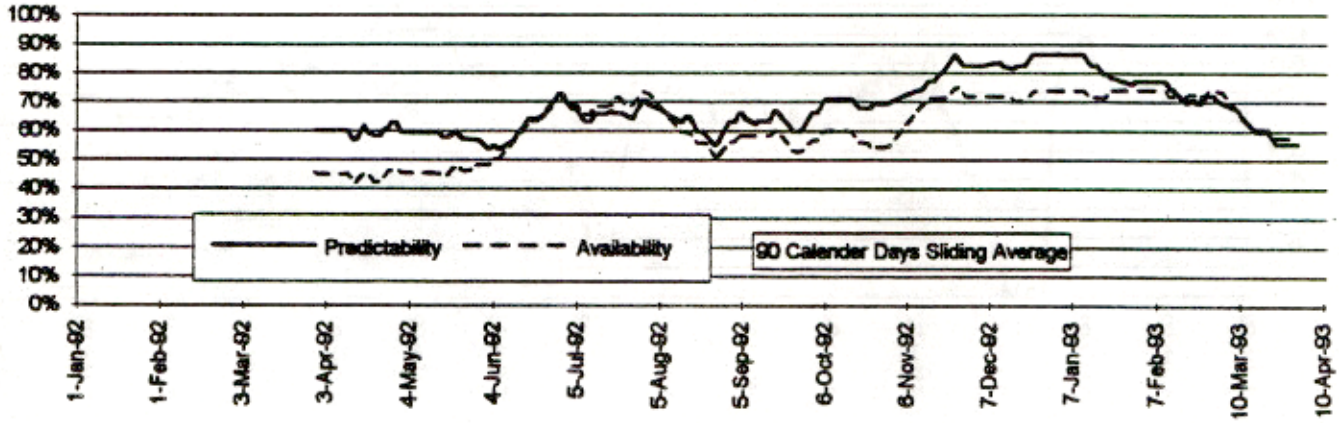


Figure 5

HIGH FLUX ISOTOPE REACTOR
Predictability vs. Availability of a Periodically Updated Forecast

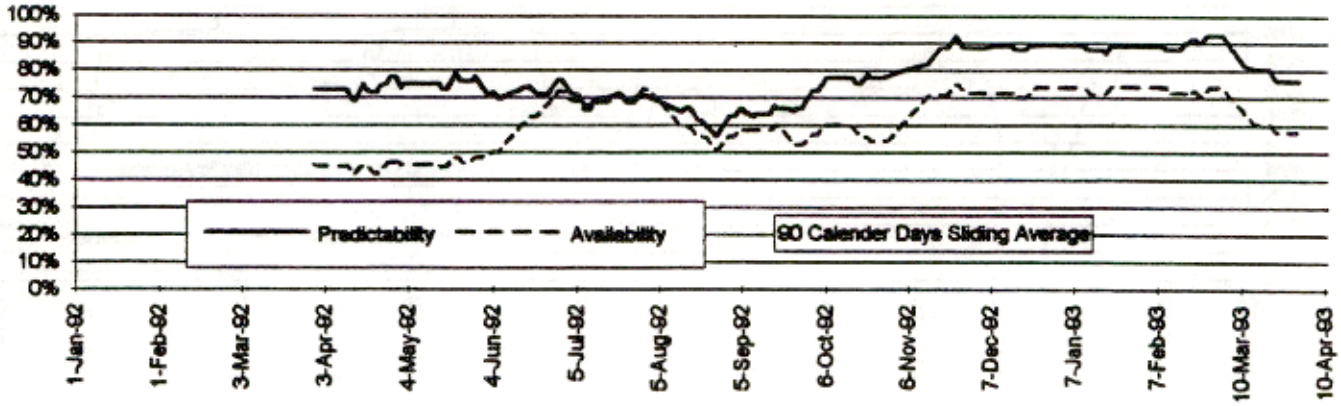


Figure 6

HIGH FLUX ISOTOPE REACTOR
Predictability vs. Availability of a Theoretical 12 Month Forecast

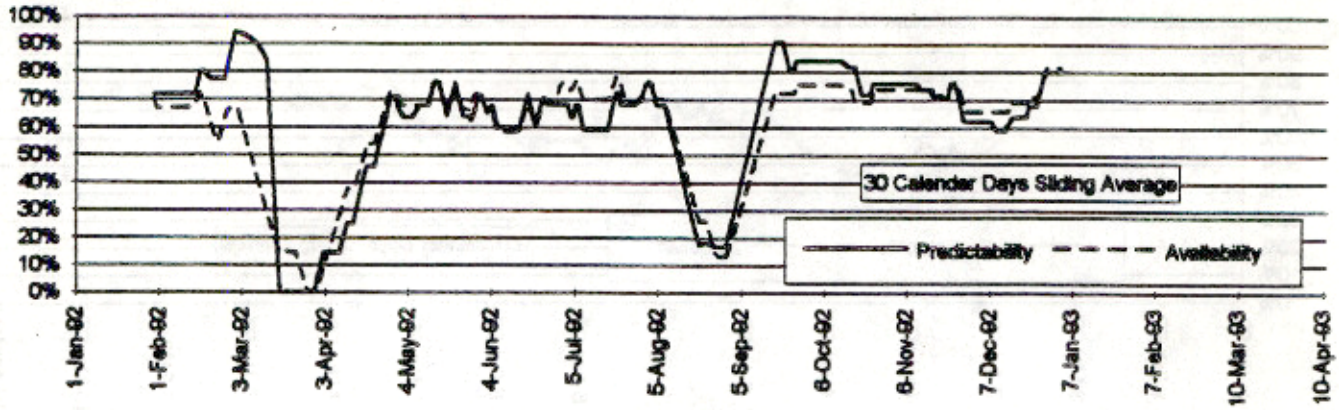


Figure 7

HIGH FLUX ISOTOPE REACTOR
Predictability vs. Availability of a 3-month Forecast

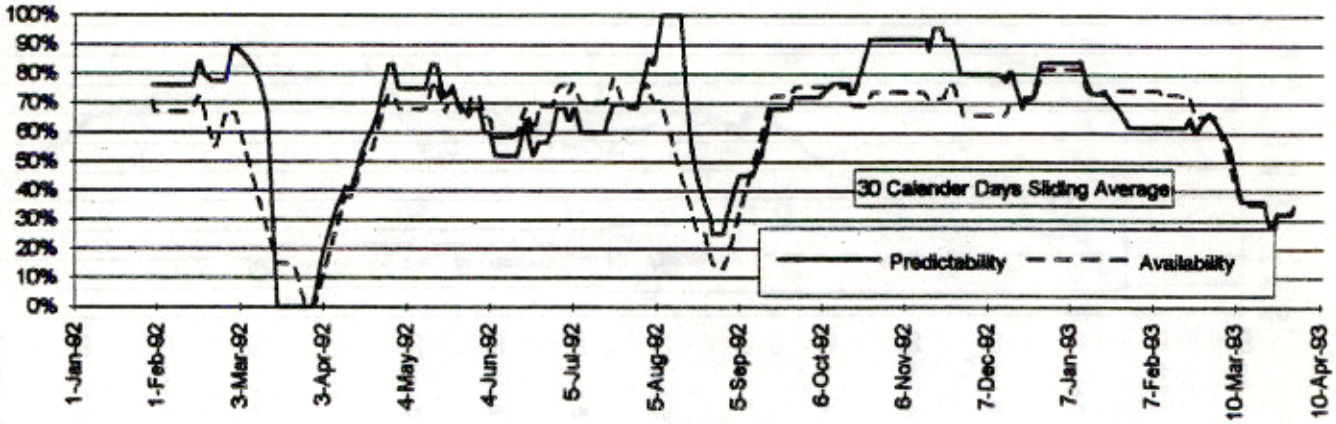


Figure 8

HIGH FLUX ISOTOPE REACTOR
Predictability vs. Availability of a Periodically Updated Forecast

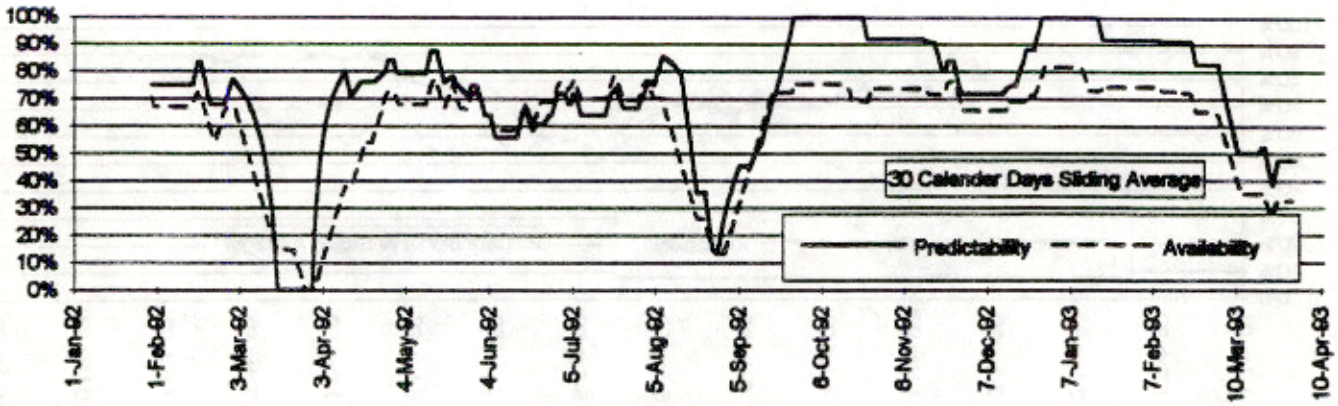


Figure 9

014 PRA Methodology

Chair: J-P. Sursock, EPRI

How Uncertain We Should be About the Outputs of a PSA: the HMIP Procedure
P. Grindrod, (INTERA); S. Watson (Cambridge Decision Analysts)

Benchmark Exercises on PWR Level-1 PSA
Y. Niwa (Inst. of Nucl. Safety System), H. Takahashi (Mitsubishi Res. Inst.)

Development of a Level 2 PSA Approach to Support Regulatory Evaluation of Severe Accident Management (SAM) Strategies
T. Okkonen, I.M. Niemela, J. Sandberg, R.K. Virolainen (STUK, Finland)

HOW UNCERTAIN WE SHOULD BE ABOUT THE OUTPUTS OF A PSA : THE HMIP PROCEDURE

Peter Grindrod[1] and Stephen Watson[2]

[1] **Intera Information Technologies Ltd, UK.**
[2] **Cambridge Decision Analysts Ltd, UK.**

INTRODUCTION

Since 1982 HMIP (Her Majesty's Inspectorate of Pollution, part of the United Kingdom Government Department of the Environment) has funded the development of a methodology for carrying out a probabilistic system assessment (PSA) of radiological safety during the long term post closure period for any proposed deep geological disposal of radioactive waste (Thompson 1987 and Thompson and Sagar, 1993). Rather than employing a scenario methodology, within which key events are selected and are assumed to dominate and determine the future behaviour of the key performance variables (thus enabling a reduced system to be modelled), HMIP has adopted a system simulation methodology, within which much of the full process system is represented, and forced by simulating external events (climate, geophysical or human effects), see figure 2. This reduces the reliance upon *a priori* expert elicitation of scenarios, yet makes the specification of the model system critical. Thus the rôle of experts in defining those internal and external processes and couplings to be incorporated, in selecting requisite mathematical model terms and solution methods (based on site data, expertise, underlying research or simply pragmatic constraints), and in defining input data and parameters, must be examined and carefully documented.

The resulting system, initially developed and iteratively refined, is used to simulate an ensemble of possible futures. This set of futures, generated by the model, represents a discrete sampling of the envelope of all possible futures of the repository system : at least in so far as the system model permits this. Within the model, input data and parameters can be distributed probabilistically using Monte Carlo simulation resulting in an inferred distribution of probabilities over the output variables. The most important output variable is annual individual risk of a serious deleterious health effect arising from radiation exposure of an average member of a critical group.

The methodology of PSA, using a Monte Carlo technique, is not the issue addressed here. Rather we focus on the more fundamental uncertainties which arise in specifying the system model. There the omission or misrepresentation of key processes or couplings can lead to misrepresentation of the spectrum of possible futures of the repository. Alternative representations, based upon the same site specific data, may legitimately yield different distributions of performance measures, see figure 1. Such divergencies are termed as "biases".

The development of the methodology has incorporated detailed considerations of a number of distinct fields in order to address the issue of expert elicitation, and the sources and propagation of uncertainties, and biases, throughout the system model. Work on input parameter value elicitation (see Dalrymple 1988), model structure elicitation (see Thorne 1993), and methods of combining various alternative models and their possible biases (Thorne and Laurens 1990) has been carried out.

In a previous programme (Summerling 1992) HMIP's methodology was applied to a trial assessment of a hypothetical repository. As noted in (Zimmerman et al. 1992), the part of the approach designed to elicit, examine and assess the impact of modelling decisions representing possible sources of bias to results of the PSA was not carried through for the reference assessment. Rather, the main focus of such work there was on the discussion of elicitation practices within expert groups, and possible techniques for propagating biases through the structure of an assessment, independent of the information arising within the trial assessment (see also Thorne and Laurens 1990).

During 1992-1993 HMIP's methodology has been applied within the first phase of HMIP's assessment of the UK Nirex proposals for disposal at the Sellafield site. This included the utilisation of an uncertainty and bias audit (UBA), designed to identify sources of bias and uncertainty within the specification of the system assessment modelling and calculations, which was fully integrated into the structure of the scientific and technical work programme. This is described in the next section.

THE UNCERTAINTY AND BIAS AUDIT

The need for an audit of the PSA modelling process arises from the wide range of decisions that must be made in specifying the system models and inputs. The uncertainties which derive from not knowing how the outputs of the PSA might differ if parts of the system were modelled differently, are not accounted for in the ensemble probabilistic assessment calculations. Hence, given the large number of alternative calculations which might be made for an assessment, it is essential to have some estimate as to where and how conceptual decisions may have biased assessment results. This is particularly relevant when alternative assessments are to be compared.

Assumptions and models may evolve or develop over the course of an assessment. Thus it is important to keep a record of all individual cross references and dependencies, so that the effect of (sub)models and corresponding calculations may be assessed in the future. More generally, within the documentation of an assessment, there are always a large number of decisions concerning the inclusion or exclusion of processes, model choices, simplifying assumptions and suitable input data. These are supported by detailed sub-tasks within the HMIP's Performance Assessment programme, by relevant expertise, or by more wide ranging research and development. Nevertheless, they remain embedded within the relevant chapters or sections of the documentation and are often not labelled explicitly, or made available for independent examination. Consequently there is a need to make unequivocal statements of all such decisions. For these reasons the **traceability, consistency** and **completeness** of the lists of decisions and assumptions adopted within the assessment constitutes the heart of the UBA methodology, as used by HMIP.

The overall objective of the UBA is to identify those issues and decisions which have the potential to change the results of the system calculations significantly. This will be achieved by:

- making explicit all decisions arising in the definition of the system models;
- documenting the reasons why particular decisions were made;
- documenting alternatives which were considered and set aside;
- documenting the sources of supporting evidence for each decision;
- investigating some key decision alternatives in order to qualify the extent of possible variations in the output variables in these cases.

The primary objective for this assessment has been to obtain all decisions in a structured form, together with relevant supporting information from the expert groups.

In addressing this task, it was the aim to record and account for all decisions which were made by the Working Groups of experts gathered together for the purpose of defining (and selecting) suitable conceptual models. In effect these conceptual models are simply lists of assumptions and decisions that must be made in order to specify how various processes will be represented (or not) within the system, and enabling their mathematical

formulation and (sub) system solution.

The format for the specification of the decisions was designed to allow for both a short formal statement of the decision, its support, and its possible alternatives, and a more wide ranging discussion. References to existing literature were encouraged.

It should be pointed out that there were some significant bonuses in adopting this formality within the Working Groups. Since it was clear what was required of the groups, they could revisit issues (or not) depending on the completion of the relevant decisions; and it was clear when their consideration of each topic was complete. It also provided a focus on those decisions which are contentious, or where few experts had much confidence in the models to be employed; this allowed for the specification of more realistic models in the future.

The Working Groups themselves were composed of relevant experts, and their expertise in specifying models was also relevant to the criticism of such models. Their guiding experience, or best guesses, were clearly relevant to issues where no more formal sources of information (literature, experiments, previous assessments, analogous) were available. Hence, at worst, the information supplied at sessions of the Working Groups was a subjective assessment by the individual experts involved, whilst at best it was based on traceable sources.

Detailed advice was sent to all Working Groups in order to minimise the burden of contributing to the UBA. It was stressed that Working Groups were to base their discussions around the production of sufficient decisions to justify the models selected. In most cases, there was a limited range of options available. Since the members of the Working Groups were able to discuss these models, without necessarily asserting that they were the "best", or most suitable, available, the process was valuable on three counts:

- Working Group members were able to discuss issues with reference to the models selected, rather than in complete generality;
- Working Groups were able to identify alternative decisions, which they would have preferred ;
- Working Groups were able to criticize the way in which concepts were represented, or managed, within the selected mathematical models.

Thus the UBA offered a formal way in which dissention (and disagreement) within groups could be incorporated, whilst still allowing the model specification to proceed.

There were five Working Groups: the Surface Environment Working Group, the Geochemical Transport Working Group, the Near-Field Working Group, the Hydrogeology Working Group and the Environmental Futures Working Group. Early in the work a description of the UBA and guidance notes were circulated to Working Group Leaders, to be passed onto Working Group Members. It was stressed that explicit decisions were to be elicited in the format provided and that experts were to take a subsystem perspective, and not prejudge the possible response in total-system performance resulting from their decisions.

All Groups completed their decision lists: there were 65 decisions in all.

Note that there are a number of other possible sources of bias within the main line assessment, which were not covered by the application of UBA to the work of the five Working Groups. These include

- detailed mathematical model specification;
- the choice of solution techniques;
- the adequacy and precision of the computational systems (verification issues);
- the elicitation of input data sets, including probability distributions for PRA;
- statistical interpretation of PRA results.

At this stage in HMIP's analysis no information has been elicited regarding the above issues, although decisions concerning them must have been made either on the basis of standard practice, or in response to events. It is intended to address them in subsequent work, however.

DEVELOPMENT OF THE UBA

As a result of experience with the work carried out during 1992 the methodology of UBA will be further developed, as we now go on to describe.

By the nature of the PSA methodology, experts are obliged to specify a system simulation model, albeit with caveats and reservations. The objective of the UBA is to document, structure and audit this process, and to assess the possible ramifications that decisions taken within the process may have for the calculated envelope of possible results obtained by the PSA. There would seem to be four possible stages within this task:

Stage 1 :

The documentation of all component decisions and assumptions which form the basis for the system assessment model is the crucial first stage. The **traceability** of decisions and the documentation of the **justification** available are essential. For this reason in the work so far achieved, Working Groups specified their own decisions, logically breaking their field down as they saw fit. The emphasis was on completeness, allowing experts an opportunity to discuss the implications of issues ruled out of the system model and consequently unaddressed (and implicitly ignored) elsewhere within the Assessment. The compilation of a complete list of modelling decisions from all groups was a major achievement.

Stage 2 :

Alternative decisions or submodels suggested by the Working Groups should be examined. This involves identifying those issues of most importance. The objective here is to gain some insight as to how biased the results of the PSA may be as a result of the option adopted. This should not result in full alternatives to the system PSA, but should lead to some quantitative estimates of how the outputs of the PSA might change.

As a first step a limited set of alternative submodels will be identified for a key process, and full analyses will be run, employing each. The resulting divergence of the output probability distributions will represent the possible range of representations of uncertainty induced by the modelling options for that particular process, and provides a qualitative way of comparing such uncertainty with that induced by the parametric and input data uncertainties accounted for explicitly within the separate submodels.

In figure 1 we show schematically how the output distributions of the PSA may depend upon a single modelling decision adopted and an available alternative decision (for example, by using an alternative conceptual submodel for some part of the system).

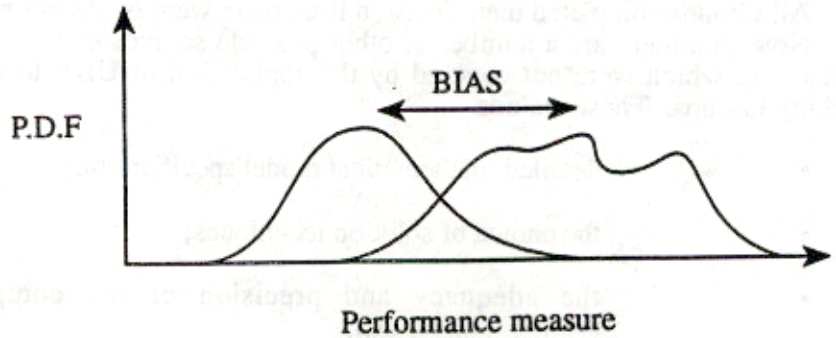


Figure 1.

The divergence between the results represents the impact of this conceptual uncertainty as a bias upon the PSA results. Are these large or small compared to the range of the distribution arrived at through parameter uncertainty ? A few key decisions will be tested in this manner.

Stage 3 :

A further possibility would be to carry out the full PSA using many different combinations of different modelling options. In the light of the output we could assess which were the key decisions which seemed to affect the PSA calculations. This would lead to a focusing of research effort on investigating which modelling alternative was the more plausible representation of the likely behaviour of that part of the physical system. This stage amounts to a sensitivity analysis of the PSA with respect to modelling options.

Stage 4 :

A further modification might be to make calculations with alternative model systems, and fold everything together into one envelope of results by associating a probability for each model alternative. The alternatives to the system PSA need not be full PSAs but could result from bias correcting shifts applied to the system simulation results as a consequence of changing one or more of the modelling decisions. This last alternative is the most obvious at first sight, but also itself introduces conceptual uncertainty. It is recognised though that if results are to be folded in together, the probabilistic nature of PSA would demand that probabilities be attached to both the mainline and perturbed results. This runs into severe technical issues since the results are not independent. It also leads to difficulties of meaning. Our intuition is that, faced with several modelling choices, one of them must be true, so that we can ask what the chance is that a particular modelling choice is the true one. Unfortunately, we know that *none* of them is, in any detailed sense, a representation of the truth.

Given the difficulties outlined above it is evident that Stage 1 is achievable (the traceability and completeness being demonstrable by the UBA database compiled during our work so far). Stage 2 is desirable. Stage 3 might be possible, but would entail a great deal of (possibly costly) simulations. **Stage 4 is probably not defensible.** In our future work effort will be focused upon obtaining better information from the expert groups in order to identify those decisions most likely to have biased the ensemble system calculations. We plan to achieve at least stage 2 in the next part of our program.

Within stage 2 it is clear that the UBA can take advantage of the sequential structure of the system model. This is represented in Figure 2. Each group considers a subset of the processes, with well defined start and end points.

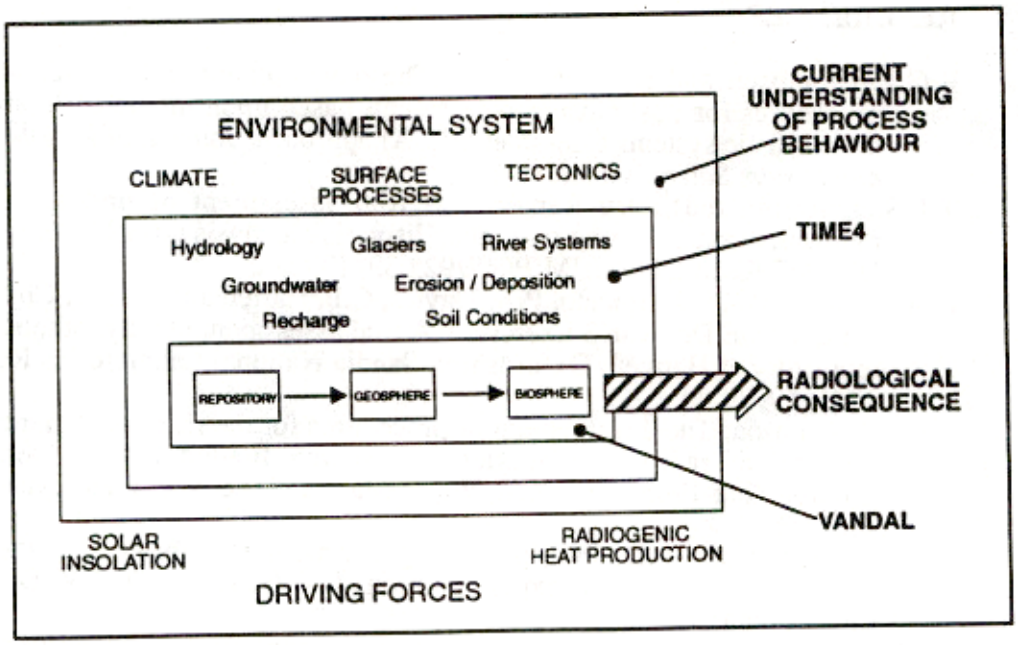


Figure 2: Environmental System.

For this reason it is proposed to proceed as follows. Each Group should make an explicit list of the inputs and outputs to be calculated by whatever subsystem model is

arrived at as a result of their deliberation. For example: the Geochemical Transport Group has input variables: the hydrology model, fluxes, heads; the nuclide fluxes released from the near field (as functions of time); the location of the geosphere biosphere interface. The Group's task is to specify and support a model producing output variables, in the case of the Geochemical Transport Group these are: radionuclide fluxes released from the geosphere (as functions of time). For each decision arrived at (whether in pragmatic support of existing models, or as a result of novel considerations), the group should estimate the impact arising from the adoption of possible alternatives by giving an estimated bound or percentage change on the increase or decrease to the output variables. For example, the Transport Group might state that alternatives to a particular decision could give rise to an order of magnitude increase on nuclide fluxes from the geosphere.

The strength of this is that individuals must focus upon the variables to be computed by the models rather than some nebulous general sense of model accuracy. Thus the decisions produced by each group will be associated with specific estimates of changes in output variables, and these will be used to assess which (if any) should be perturbed in order to investigate alternatively biased PSA results.

SUMMARY

Within HMIP's assessment methodology, an uncertainty and bias audit is employed in order to account for those conceptual and modelling decisions which may have misrepresented key processes, and hence, distorted the output of the subsequent PSA.

All working groups charged with specifying the system assessment model conditioning, and input data are required to itemize their decisions. The emphasis is on the traceability and defensibility of such information. In future work, the scope of the UBA will be widened, and some parallel PSAs will be run in order to qualify the impact of key decisions upon distributions for performance measures.

Acknowledgement

The authors thank HMIP for permission to publish this paper. The work may be used for the formulation of UK Government policy but does not at this stage constitute UK Government policy.

REFERENCES

B.G.J. Thompson and B. Sagar, 1993, The development and application of integrated procedures for post-closure assessment, based upon monte carlo simulation : The probabilistic systems assessment (PSA) approach, *Journal of Reliability Engineering and System Safety (submitted)*.

T.J Summerling (ed), Dry Run 3 : A trial assessment of underground disposal of radioactive wastes based on probabilistic risk analysis : (in 11 volumes) : Overview, UK DoE Report, DoE/HMIP/RR/92.039, 1992.

D.A. Zimmerman, E.J. Bonano, P.A. Davies, C.P. Harlen and M.S.Y. Chu, Peer review of the UK DoE Dry Run 3 Exercise : A trial assessment of a hypothetical nuclear waste repository at Harwell, Oxfordshire, Sandia National Laboratories Report SAND 92-1945, 1992.

B.G.J. Thompson, The development of procedures for the risk assessment of underground disposal of radioactive wastes : research funded by the Department of the Environment 1982-1987. Rad, Waste Man. and the Nuc. Fuel Cycle, 99, (1987), pp 215-256.

G.J. Dalrymple and L.D. Phillips, Using a structured approach to the acquisition of probabilistic data from expert opinion, DoE/RW/88.007, UK Department of the Environment, London, 1988.

M.C. Thorne and J-M. Laurens, The development of overall assessment procedure incorporating an uncertainty and bias audit. In NEA/IAEA/ CEC, Paris 1990, pp 673-681.

M.C. Thorne, The use of expert opinion in formulating conceptual models of underground disposal systems and the treatment of associated bias, *Journal of Reliability Engineering and System Safety (submitted)*.

BENCHMARK EXERCISES ON PWR LEVEL-1 PSA.

Y.NIWA
Department of Engineering System Research,
Institute of Nuclear Safety System, Inc.
H.TAKAHASHI
Safety Engineering Department,
Mitsubishi Research Institute, Inc.

ABSTRACT

The results of sensitivity analysis of benchmark problems are described. These benchmark problems have been set up for Japanese 3-loop PWR plant to investigate uncertainties which however have not been discussed specifically through the uncertainty analysis.

The effects of differences in component failure data bases applied to several preceding PSAs, differences in treatments and data on common cause failures, differences in human reliability evaluation procedures, and differences in treatments of dependencies on a series of human errors are described in this paper.

1. INTRODUCTION

On various stages in performing level-1 PSAs, many assumptions based on engineering judgment are adopted. Various premises and assumptions generate uncertainties in the results in addition to the uncertainties caused by statistical dispersions of component failure rates. In order to comprehend the results of PSA, it is necessary to understand the essential factors which increase the uncertainties and to know their effects on the results quantitatively.

Commission of European Communities-Joint Research Centre (CEC-JRC) has performed several international benchmark exercises[1]. However the design of objective system is q u i t e different from that of the PWRs' in Japan. Also there are some differences in emergency response. The exercises by CEC-JRC assessed a degree of consistency among the results obtained from different analysis teams. Their results spread in a wide range and there are variety of causes, so it is difficult to comprehend the differences and to apply the knowledge obtained by those exercises directly to PSAs in Japanese PWRs.

In our study, it is aimed to understand generally the quantitative effects of premises and assumptions through the analysis of benchmark problems set up by reflecting the realistic design and operating procedures of Japanese plants. For this purpose, one team performed modeling and analysis by changing some assumptions. It is discussed how the results of sensitivity analysis should be described in PSA report.

2. CRITERIA FOR BENCHMARK PROBLEM

PSA is a technology based on various premises and assumptions. So far many PSAs for NPPs worldwide have been completed. Differences are seen in terms of the following items.

(1) Procedure to construct Fault Trees
  (a) System boundaries
  (b) Component failure modes
  (c) Structure of Fault Trees
(2) Source of component failure data
  (a) Component failure rates
  (b) Out of service time
(3) Common cause failure
  (a) Components and failure modes for which CCF is considered
  (b) CCF model and data
(4) Operator action, and HRA methodology
  (a) Human errors in test and maintenance
  (b) Human errors in post accident diagnosis and action
  (c) Human errors in recovery action (Accident Management)
  (d) Technique of Human Reliability Analysis
(5) Success Criteria
  (a) System success criteria and mission time
  (b) Requirements of cooling system and ventilation system
(6) Analysis methodology
  (a) Treatment of support system interactions

The above differences affect the analytical results even though the objective plant is the same. The following 6 criteria were established to investigate the fluctuation of analytical results and to understand the causes quantitatively.

(1) The benchmark problem should include analysis of safety system which plays important role to decrease the core damage frequency
(2) The system should have a design where common cause failures have an important role
(3) The system should have interactions with several support systems
(4) The benchmark problem should include human errors in test & maintenance and in emergency operation
(5) Recovery action should be examined
(6) Accident sequence which includes several front line systems requiring common support systems should be examined

Taking these criteria into account, the following 3 benchmark problems for SGTR accident on Japanese standardized 3-loop PWR plant are studied.

A. Failure of Auxiliary Feedwater System(AFWS) including support system failures.
B. Accident sequence consisting of multiple human errors.
C. Accident sequence consisting of multiple system failures.

Figure 1 shows these sequences in general SGTR event tree.

3. MODELING AND ANALYSIS

3.1 PROBLEM A (SYSTEM ANALYSIS)

Problem A is to analyze a failure of AFWS which is included in a heading "secondary cooling" in SGTR event tree. Safety injection(SI) signal is generated on coincidental occasion of low pressurizer level and low reactor pressure signal. Power of non-essential electric bus is lost, then after 10 seconds, the Emergency Diesel Generators start. Following the SI sequence, auxiliary feedwater pumps start and supply feedwater to steam generators(SGs). The SG where tube rupture occurs is assumed to be the one which supplies steam to the turbine-driven auxiliary feedwater pump. The top event is "a failure to supply auxiliary feedwater to at least one out of two intact SGs".

This problem was set up to discuss the items (1) through (3) and (4)-(a) described in the previous chapter.

Fault trees(FTs) were constructed using Automated Fault Tree Generating System (AFTG)[2] to standardizes the process of constructing FTs and the logical structure of FTs. It was expected to eliminate some discrepancies among the analyst and modeling uncertainties. Also clear identification of the assumptions and premises were expected.

Figure 2 shows the relationship among the systems included in the model. Figure 3 is a simplified system diagram which shows modeling boundary of the AFWS. The following analysis were performed and effects of human errors in test and maintenance were also investigated.

(1) Case studies to investigate the effects of component failure data
- Case 1.; Generic data[3]
- Case 2.; NUREG/CR-4550 Surry data[4]
- Case 4.; Surry IPE data[5]
- Case 5.; NUREG/CR-4550 Sequoyah data[6]
- Case 6.; Sequoyah IPE data[7]
- Case 7.; Millstone-3 PSA data[8]
- Case 8.; LER data[9]
- Case 9.; The same as Case 8 except that DG data is replaced by the data of Millstone-3

(2) Case study to investigate the effects of the details of system model
- Case 3.; Develop signal system model for case 2 using generic data

(3) Case studies in terms of Common Cause Failure(CCF)
- Case A. Apply beta factor and data in NUREG/CR-4550[4]
- Case B. Apply beta factor and data in Surry IPE[4]
- Case C. Apply BFR and data in Millstone-3 PSA[8]
- Case D. Apply MGL and data in Sequoyah IPE[7]
- Case E. Apply MGL and data of PLG[10]
- Case F. Apply MGL and data of FRG[10]

(Except case A, two cases with differences in the treatment of passive failure mode are analyzed.)

Time data such as test interval and mission time, and

treatment of test lines are commonly applied in all of the above cases. Also, boundaries of component failures are unified.

3.2 PROBLEM B (HUMAN RELIABILITY ANALYSIS).

Human reliability analysis were performed using Human Reliability Analysis Support System which supports THERP oriented detailed HRA. This support system generates potential errors according to the objective tasks, assign human error probability according to the situation of PSFs, and construct and analyze HRA event tree. It was expected to standardize the process of HRA and to eliminate discrepancies caused by the differences in expertise of the analyst. Also transparency of the modeling assumptions were expected. Operating manual and maintenance manual were investigated precisely and task analysis were performed by examining a realistic operator action.

This problem was set up to discuss the items (4)-(b) through (d) described in the previous chapter.

Detailed OAT(Operator Action Tree) was developed to examine the S/G isolation and Feed & Bleed sequence. Figure 4 is the OAT which was constructed considering a case where the operating crew is required to realize the situation that they failed to isolate suitable S/G. In this case, human cognitive process is expected to be complicated compared to the other accidental situations.

4. SUMMARY OF THE RESULTS

4.1 PROBLEM A (SYSTEM ANALYSIS)

Figure 5 shows the results obtained from analytical case 1 through 9. In these cases, only independent component failures are treated. Figure 6 shows the weight of Fussell-Vesely importance measure in terms of component groups. Figure 7 shows the results of the analysis which consider CCFs. Figure 7-a and figure 7-b show the results where CCF is applied to case 3 and case 7 respectively. The results indicate relative value to the base case which neglects CCF. The dashed cases treat CCFs for some specific failure modes(e.g. plugging of MOVs, failure to open check valve, etc.) which are considered specifically in the reference PSAs.

A knowledge obtained is summarized as follows.

(1) Importance of numerical data

As the preceding benchmark exercises pointed out, problem A emphasizes the importance of basic numerical data such as component failure rates, out of service, mission time, and test period. Even if the unavailabilities of AFWS are similar, profile of component importance measure are different.

(2) Effects of the dependencies between systems

Case 2 and 3 differs in the treatment of instrumentation system. Case 2 treats the failure of SI signal as a basic event. Case 3 developed FT which precisely treats the dependency between instrumentation system and electrical power system(vital AC power). The results spread within the difference of about 20%. Even if the difference is small, it should be noted that there appears cut sets which include component failures in vital power system in case 3.

These failures cause loss of SI signal. It is important to identify the detailed cut sets when the purpose of the analysis is to survey weakness of the system. In NUREG/CR-4550, FTs for instrumentation systems are not developed. Instead, dependencies between instrumentation systems and electric power systems are treated by boolean equation.

(3) Effects of the usage of plant specific data

Differences in case 3 and 4, and case 5 and 6 arise from component failure rate data which are used in NUREG/CR-4550 and IPE. There appears differences up to 1 order of magnitude.

(4) Effects of single component

The difference in the results between case 8 and 9 arises from failure rate of DG. It should be noted that data on single type of component can affect the results drastically. In this case where the failure rate of DG is changed from LER data to Millstone data, the analytical result decreased for 3 orders of magnitude. This emphasizes that the attention is required when data from different sources or backgrounds are used for important components such as DGs, pumps, and valves.

(5) Effects of common cause failures

Degree of the effect of CCF relates to independent component failure rates. In case 7, failure rates for some components(ex. DG,invertor) are smaller for about 1 order of magnitude than the one in case 3. These differences in component failure rates affect the analytical results drastically.

(6) Effects of human errors in test and maintenance

The effects of human errors in pump test and instrumentation calibration are negligible, because the human error probabilities are reduced by multiple administrative factors and become relatively small compared to hardware failures.

4.2 PROBLEM B (HUMAN RELIABILITY ANALYSIS)

The results will be presented at the conference.

5. CONCLUSION

The analysis of benchmark problem A shows the necessity of clarification of the assumptions and its effect on the analytical results. Especially sensitivity to component failure rates should be examined carefully. Data tables which include list of considered failure modes and failure rates, their data source, and values of time parameters should be attached in the report.

The knowledge obtained through benchmark problem B will be presented at the conference. Further, benchmark problem C will be analyzed in the future, and the results will be synthesized.

Because uncertainties from various causes exist, it should be assessed synthetically and indicated intelligibly. Traditional uncertainty analysis assesses only statistical dispersions which originate the dispersions of component failure rates. Development of a methodology to display overall uncertainties and also contributions from various sources are required.

Reference

1) A.Amendra et.al., "PSA Models for System and Human Reliability: Results of benchmark Exercises and Needs" IAEA-CN-48/161
2) Y.Kitamura and H.Takahashi, "Support Tools for Fault Tree Generation and Modeling Information Management".
3) S.A.Eida and M.B.Cally, "Generic Component Failure Data Base" PSA'93 (1993)
4) R.C.Bertucio and J.A.julius, "Analysis of Core Damage Frequency: Surry, Unit 1 Internal Events" NUREG/CR-4550 Vol.3, Rev.1, Part 1 (1990)
5) Virginia Electric and Power Company, "Probabilistic Risk Assessment for the Individual Plant Examination Final Report Surry Unit 1 and 2" (1991)
6) R.C.Bertucio and S.R.Brown, "Analysis of Core Damage Frequency: Sequoyah, Unit 1 Internal Events" NUREG/CR-4550 Vol.5, Rev.1, Part 1 (1990)
7) TVA, "Sequoyah Nuclear Plant Unit 1 Probabilistic Risk Assessment Individual Plant Examination" (1992)
8) Northeast Nuclear Energy Company, "Millstone Unit 3 Probabilistic Safety Study" (1983)
9) Data Summaries of Licensee Event Reports at U.S. Commercial Nuclear Power Plants.
    1. Diesel Generators ; NUREG/CR-1362
    2. Pumps ; NUREG/CR-1205
    3. Valves ; NUREG/CR-1363
    4. Selected Instrumentation and Control Components ; NUREG/CR-1740
10) A.Poucet et. al., "Common Cause Failure Reliability Benchmark Exercise, Final Report" EUR-11054 EN, CEC-JRC, Ispra (1987)

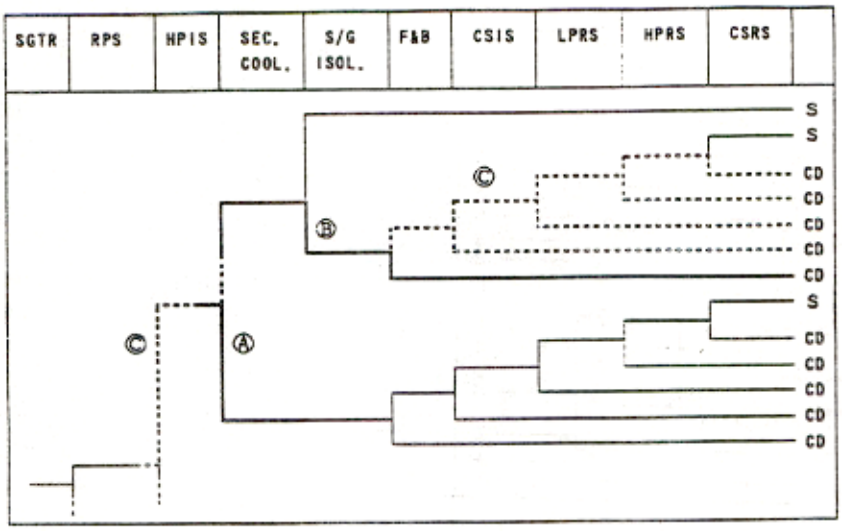


Figure 1 SGTR Event Tree

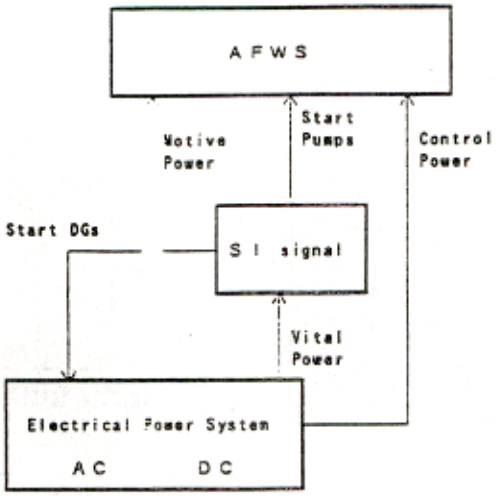


Figure 2 System Interaction Diagram

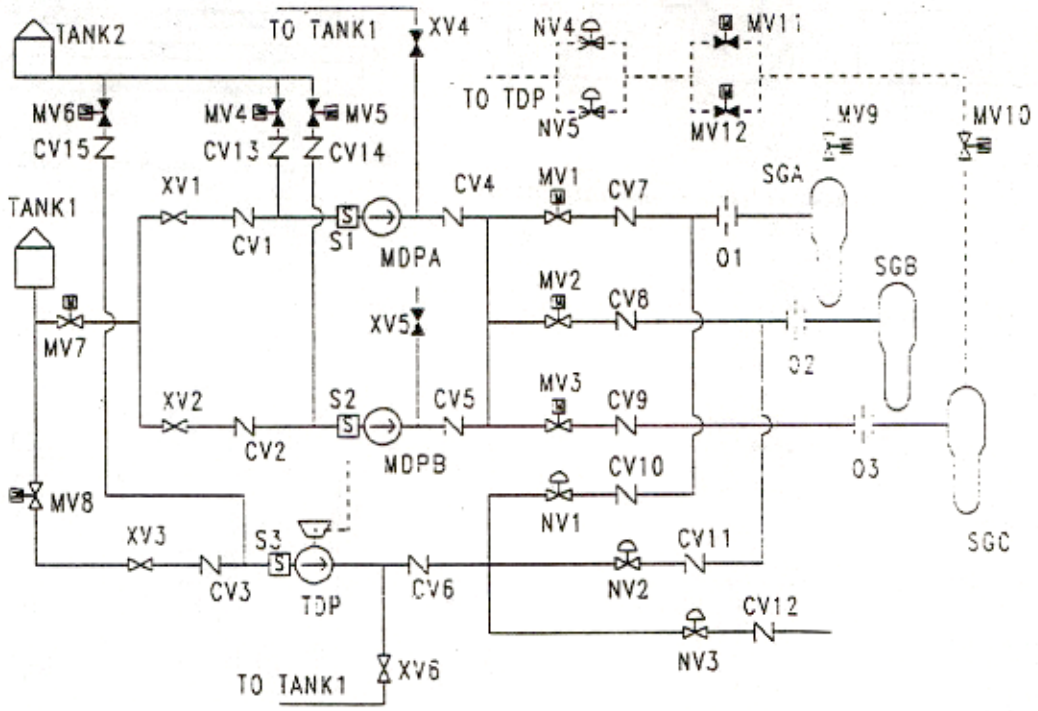


Figure 3 Simplified Diagram of AFWS

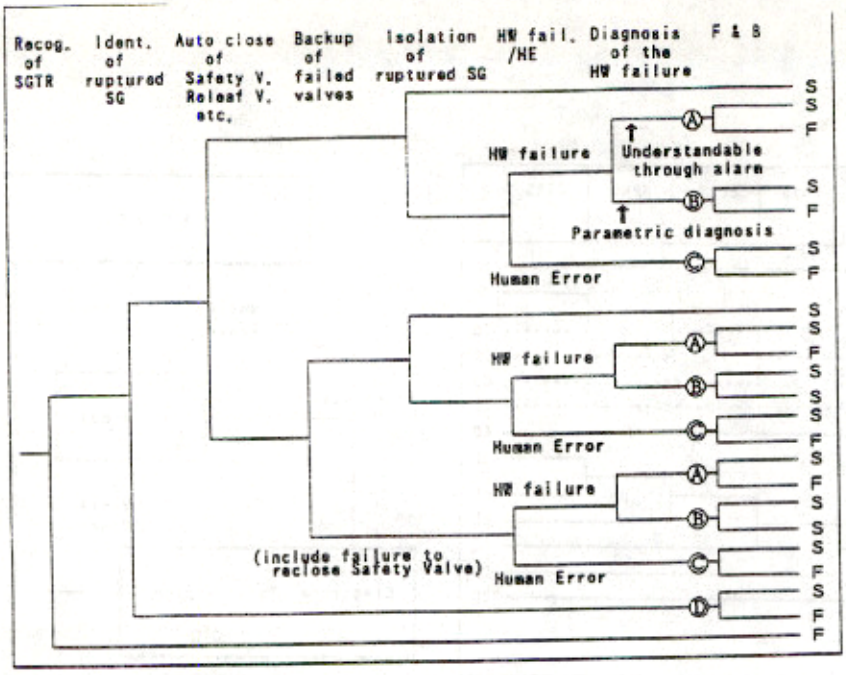


Figure 4 OAT of S/G Isolation and F&B

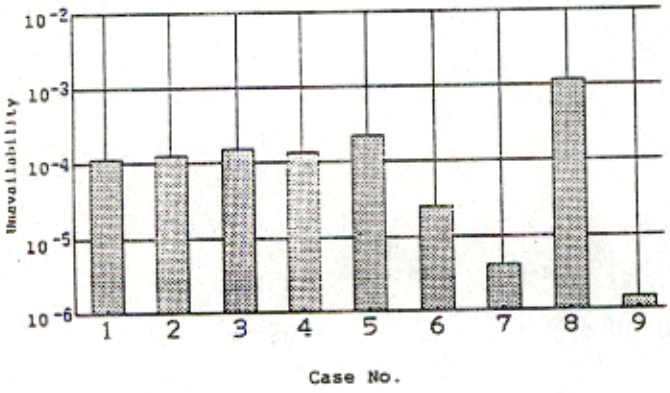


Figure 5 Analytical Results (system unavailability)

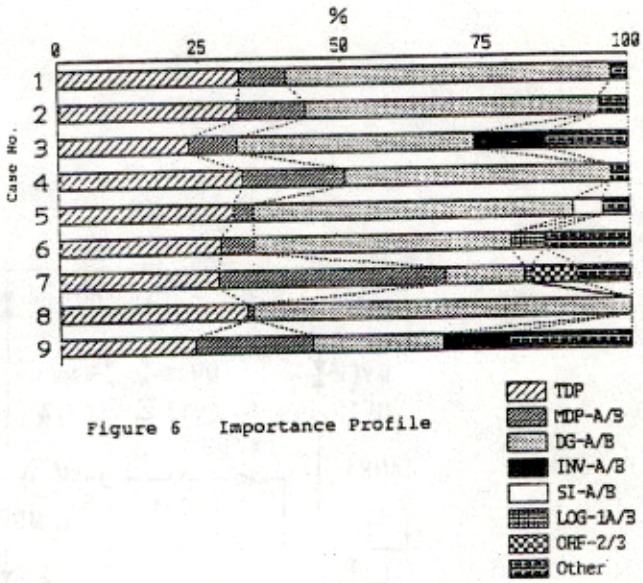
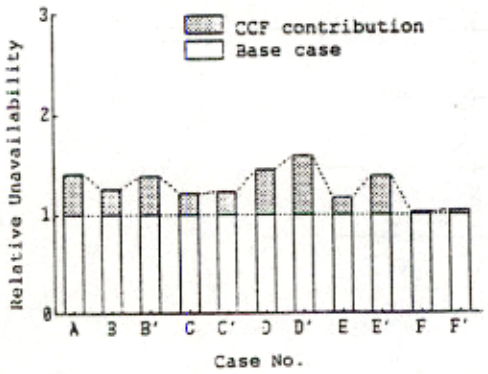
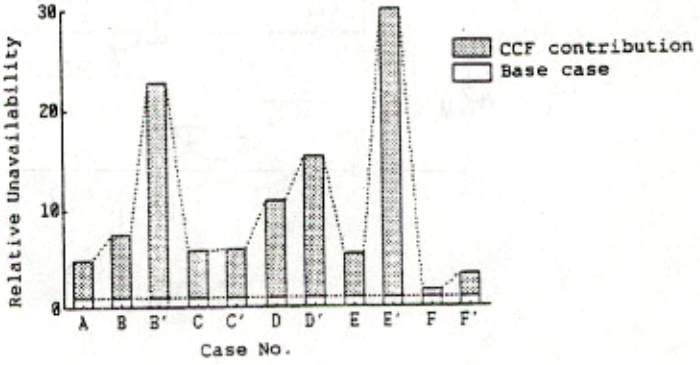


Figure 6 Importance Profile



7-a for Case 3



7-b for Case 7

Figure 7 Contribution of CCFs

DEVELOPMENT OF A LEVEL 2 PSA APPROACH TO SUPPORT REGULATORY EVALUATION OF SEVERE ACCIDENT MANAGEMENT (SAM) STRATEGIES

T. Okkonen[1], I.M. Niemelä[2], J. Sandberg, R.K. Virolainen

Finnish Centre for Radiation and Nuclear Safety (STUK)
P.O. Box 268, FIN–00101 HELSINKI, Finland.

[1] Currently at Royal Institute of Technology (KTH), Sweden.
[2] Currently at Swiss Federal Nuclear Safety Inspectorate (HSK), Switzerland.

INTRODUCTION

A goal–oriented approach to Severe Accident Management (SAM) has been adopted by the Finnish nuclear regulatory body (STUK). The goal is to prevent containment failure and severe environmental consequences in case of a severe accident (core meltdown accident), by introducing plant modifications, if necessary. The goal–oriented approach is particularly feasible if the benefits of the designed SAM measures are obvious and outweigh any associated concerns. Consequently, the implementation of the SAM systems has been completed for the TVO plants, and the SAM strategy of the Loviisa plants is under development and related plant modifications are aimed at in near future.

Probabilistic Safety Assessments (PSAs) have to be performed for the Finnish plants. For the TVO and Loviisa plants, Level 1 PSA studies for internal and external events have been mainly completed, yielding several modifications in plant systems and operating procedures; studies for low–power/shutdown conditions and reactivity initiated accidents are underway. Following the SAM development, Level 2 PSA studies can provide a systematic evaluation of the safety level reached with the mitigative SAM measures. The Level 2 PSA work has been initiated at TVO, and the Level 2 PSA studies of Loviisa will benefit from the research that is being carried out for the SAM development.

In this paper, the Finnish regulatory requirements related to severe accidents are first presented, and then the SAM strategies of TVO and Loviisa are described. Regulatory aspects of using PSA in studying the efficacy of the plant–specific SAM strategies are discussed, and an alternative Level 2 PSA methodology, under development at STUK, is introduced. Finally, conclusions on the objectives of the Level 2 development efforts of STUK, and the experience gained so far with the Living PSA code SPSA, are given.

While this paper focuses primarily on severe accident mitigation, it is emphasized that the preventive, high-quality plant operation and safe plant features have to be maintained and if not as safe as required, then modified. In this respect, a combination of design-level analyses and probabilistic studies, and evaluation of experiences, are necessary.

REGULATORY REQUIREMENTS

The Finnish regulations for the safety of nuclear power plants can be divided into two categories. The decisions of the Council of State constitute the mandatory requirements. Their fulfilment is controlled by STUK, which issues the detailed safety guidelines.

In 1982 STUK issued a revised guide concerning the design criteria for new nuclear power plants. Severe accidents shall be taken into consideration especially for the containment heat removal and gas treatment, and the protection of containment integrity.

In 1984 STUK required the utilities to perform Level 1 and Level 2 PSA studies. After the Chernobyl accident in 1986, the design and implementation of additional provisions to mitigate the consequences of a severe accident were required for all operating plants.

In 1987 STUK revised the guide on transient and accident analyses to include also severe accidents. In 1991 the severe accident criteria were confirmed by the Council of State in its decision on general regulations for the safety of nuclear power plants. When evaluating the adequacy of the plant safety systems, the abnormal events are divided into three categories: anticipated transients, postulated accidents and severe accidents. A severe accident shall not result in acute health effects in the plant vicinity or any long-term restrictions for the use of extensive land and water areas. For satisfying the long-term requirement, the limit for an atmospheric release of Cs-137 is 100 TBq, and other nuclides than caesium-isotopes shall not cause, starting three months from an accident, a hazard greater than the caesium release limit. The possibility that, as the result of a severe accident, these requirements are not met, shall be extremely small.

The current radioactive release limits and containment design requirements for severe accidents were not in force when the currently operating plants were licensed. However, the decision of the Council of State requires that for further safety enhancement, technically justifiable actions shall be taken.

The Finnish severe accident positions are discussed in detail in (Laaksonen, 1993).

SAM STRATEGIES IN FINLAND

The SAM systems and features of the TVO and Loviisa plants are shown in Figure 1.

TVO I/II

The SAM measures that were considered necessary due to the new severe accident safety requirements have been implemented at the TVO plants [two 2160 MW(t) ABB-ATOM BWRs with nitrogen-inerted containments, commercial operation started in 1978 and 1982]. The severe accident mitigation strategy of TVO is based on the following safety functions (Koski, 1988; Tuomisto et al., 1992): (1) Reactor Coolant System (RCS) depressurization by the relief valves, (2) core debris cooling by gravity-driven water flow from the suppression pool to the pedestal, (3) containment pressure control by the filtered venting system and (4) long-term plant stabilization by containment water-filling. An independent SAM instrumentation system has been installed. The containment over-pressure relief system would prevent a gross containment failure, and subsequent threats to core cooling, if the suppression pool were bypassed in a Loss Of Coolant Accident (LOCA).

Loviisa 1/2

The severe accident mitigation strategy of Loviisa [two 1375 MW(t) VVER–440 PWRs with ice–condenser containments, commercial operation started in 1977 and 1980] is planned to be based on the following safety functions (Tuomisto and Theofanous, 1991; Tuomisto et al., 1992): (1) RCS depressurization by primary relief valves (under design), (2) hydrogen management in the containment (further enhancement is under research and design), (3) core melt retention in the reactor vessel by external vessel cooling (additional provisions are under research and design), (4) long–term containment pressure control by the external spray system (installed in the secondary containment building). In addition, a protective shield has been constructed to prevent direct core melt attacks against the cavity air–lock, and the side–wells of the cavity have been filled with concrete to prevent a fast basemat penetration in case of a vessel failure. A filtered relief of slight containment over–pressures caused by non–condensable gases is to be considered, and an independent severe accident instrumentation system is being designed.

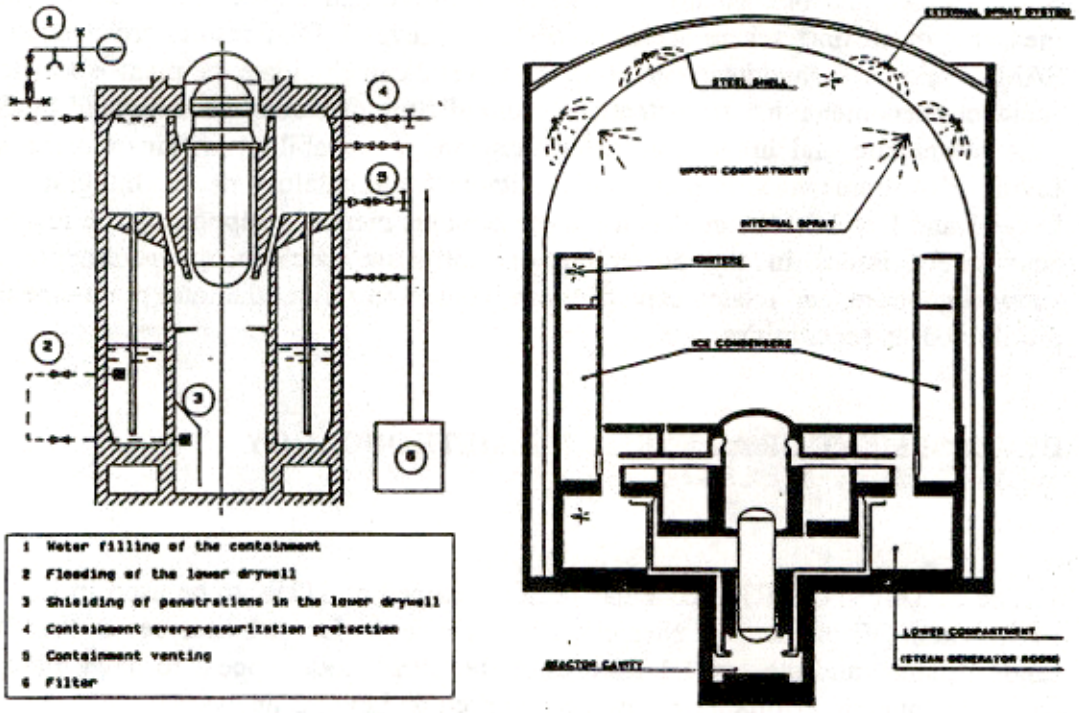


Figure 1. SAM systems and features of TVO (left) and Loviisa (right); not in scale with each other.

REGULATORY ASPECTS OF SAM AND PSA

The plausibility that the severe accident safety requirements have been met should be estimated and presented with plant–specific PSAs, and the rationale for this will follow.

Some severe accident types, such as severe reactivity initiated accidents, cannot be coped with, and thus the demonstration of a negligible probability requires Level 1 PSA studies. A low probability of severe core damages has to be demonstrated also for containment bypass sequences and refueling outages, during which the containment may lack its capability of retaining radioactive fission products. For all severe accident types, the reliability of the containment isolation deserves continuing attention.

In the goal–oriented development of the SAM strategies as described for TVO and

Loviisa, the challenges to containment integrity are mitigated by improved Emergency Operating Procedures (EOPs) and by specific SAM systems. Because there exists a wide spectrum of potential problems preceding a severe core damage, the credibility of the SAM strategy is increased by independence of the dedicated SAM systems. However, one usually needs to also credit systems or actions that are related both to the prevention and mitigation of severe accidents, most notably the intentional RCS depressurization. To estimate the independence of the SAM efficacy of other plant systems, Level 1 PSA studies are needed. The Level 2 PSA can be used to estimate and present the probability and consequences of a containment failure for accidents such as high-pressure scenarios, which may lie outside the scope of the SAM strategy.

During the SAM strategy development, the phenomena jeopardizing containment integrity, and the efficacy of the selected mitigative measures, are assessed for a range of severe accident initiators. With respect to some phenomena, a wide range of accidents may be covered by SAM measures or other plant features. For example, hydrogen combustions can be prevented by inerting the containment during normal operation. On the other hand, hydrogen mitigation in a non-inerted containment may be effective for only a limited range of accidents. In addition, some phenomena may require opposite SAM actions, and one should compare the positive and negative impacts of the SAM measures on distinct severe accident scenarios. Level 1 PSA results are needed for the SAM development, and its integration with Level 2 can elucidate the plant-specific severe accident phenomena that are potentially contradicting or cannot be mitigated by SAM.

A systematic and up-to-date safety assessment capability, within a plant-specific Living PSA framework, is particularly suitable for regulatory needs. Integration of the Level 1 and Level 2 PSA models has some obvious merits in supporting the resolution of new safety issues in the preventive or mitigative accident management. Such a knowledge-base, and related expertise, can be used to reflect the total plant-specific risk profile and its sensitivities.

DEVELOPMENT OF A LEVEL 2 PSA METHODOLOGY

Level 1

The SPSA (STUK PSA) code has been developed at STUK to be used in Living PSA environment (Virolainen and Niemelä, 1993). Since the Level 1 analyses of the TVO and Loviisa plants, and the Level 1 features of the SPSA code, appear to have matured, the code development efforts have now been shifted to Level 2 analyses.

Level 2

Many different methods are available for Level 2 PSA studies, and in principle the event tree approach has dominated (USNRC, 1989). In several Level 2 PSA studies, the number of Containment Event Tree (CET) questions have been reduced in order to make the CET characteristics more transparent and also to reduce calculational burdens (Galyean et al., 1990; Cazzoli et al., 1992). Deterministic codes have been used to study the uncertainties in severe accident progression (Khatib-Rahbar et al., 1989), and an organized treatment of phenomenological uncertainties has been introduced (Theofanous and Yan, 1991). In general, the biggest differences between various approaches result from the treatment of uncertainties and the level of detail with respect to severe accident progression, phenomena and SAM actions.

The Level 2 PSA methodology, under development at STUK, utilizes the event tree approach. As a unique feature, calculational models of accident progression and physical

processes can be programmed into a self-contained Level 1 and Level 2 PSA model. Since the methodology should be suitable for regulatory reviews of PSAs, such as (Schmocker et al., 1991), the overall development goal is to have a rather general Living PSA tool for Level 2. For the Level 2 code development efforts, the following objectives have been used: (1) Living PSA approach, (2) integration of Level 1 and Level 2, (3) transparency of models, (4) treatment of uncertainties and (5) computational efficiency.

Code Features

A Level 2 PSA model is being developed for the SPSA code. It is intended to be a flexible tool employing also parametric models that can be provided based on plant-specific considerations. For every branch of a CET, the plant state variables (pressures, temperatures, fission product inventories, etc.) can be manipulated at the CET question points, representing accident progression in time. When a single Monte Carlo simulation is performed for a CET, the parameters are sampled from their probability distributions and the variables along the branches change according to the rules and models programmed by the code user with the special SPSA-CET control language. The data from Level 1 cut sets, corresponding to the Level 1 events and failures that belong to the Plant Damage State (PDS) in question, can also be used in modelling accident progression and possible operator actions.

For every branch point in a CET, the frequencies and plant state variables, as well as their distributions, are available. Provided that fast enough parametric models can be developed for fission product behaviour, the environmental releases can be calculated for each simulation, based on branch-specific variables related to accident progression and plant status. In this case the frequency-release pairs can be calculated at the same time, and the frequency-release distributions of various release categories can be obtained straight-forwardly by adding each frequency-release sample to the corresponding release category (bin).

In case the releases were calculated separately from the frequency simulations, the treatment of the following correlations is provided: correlations between branch frequencies, between releases and frequencies, and between any two variables.

Development Status

For the treatment of uncertainties in the Level 2 model of the SPSA code, simple validation exercises were first conducted by comparing the results to those of hand calculations. The frequency distributions of the CET branches were calculated accurately enough by the code.

A test CET, including parametric modelling of the progression of a severe BWR accident, was constructed in order to gain a view of the code's capabilities and computational efficiency. They were proven reasonable also in the uncertainty analyses.

A more thorough review of the current development status of the Level 2 PSA methodology at STUK was carried out by Energy Research, Inc. (ERI). The frequency results of the SPSA's Level 2 model were compared to the results of the SNL's EVNTRE code. By programming parametric fission product models with the SPSA-CET control language, the results for environmental releases were compared qualitatively to the results of the ERI's ERPRA code, including also time-dependent release calculations. Several recommendations for future code development were made by ERI, and the preliminary conclusion was that the Level 2 methodology of the SPSA code is robust in representing severe accident progression and that the uncertainties are treated consistently.

CONCLUSIONS

The Level 2 PSA approach, under development at STUK, is aimed at identifying of critical severe accident sequences and SAM actions. The credibility of the dedicated SAM measures should be evaluated in a systematic way, and the severe accident sequences and phenomena that cannot be mitigated should be shown to be of a low likelihood. As a general PSA goal, the fulfilment of the severe accident safety requirements should be demonstrated plant-specifically with an integrated Level 1 and Level 2 model.

The Level 2 PSA methodology is being integrated into the Living PSA environment of the SPSA code. The experiences gained so far are encouraging with respect to the capabilities of a CET that uses parametric modelling of severe accident progression and phenomena. In Finland, parametric approaches are supported by the fact that during the development of the SAM strategies for the TVO and Loviisa plants, preceding the Level 2 PSAs, the range of manageable severe accident situations should be estimated. Using the SPSA code in integrating the knowledge and uncertainties of plant behaviour in severe accidents, a self-contained Level 1 and Level 2 PSA model can be constructed.

ACKNOWLEDGEMENTS

Special thanks are due to Dr. E.G. Cazzoli and Dr. M. Khatib-Rahbar of Energy Research, Inc., Rockville, Maryland, for their insights into the Level 2 PSA methodology.

REFERENCES

E.G. Cazzoli, et al., 1992, Quantification and Propagation of Uncertainties in Probabilistic Safety Assessments, Proceedings of Jahrestagung Kerntechnik '92, Karlsruhe, Germany, May 1992.

W.J. Galyean, et al., 1990, Simplified Containment Event Tree Analysis for the Seqoyah Ice Condenser Containment, NUREG/CR-5602, EGG-2606, December 1990.

M. Khatib-Rahbar, et al., 1989, A Probabilistic Approach to Quantifying Uncertainties in the Progression of Severe Accidents, Nuclear Science and Engineering: 102, 219-259 (1989).

S. Koski, 1988, Severe Accident Mitigation Programme for Finnish BWR Plants, Proceedings of an International Symposium on Severe Accidents in Nuclear Power Plants, Sorrento, Italy, March 21-25, 1988, IAEA-SM-296/10.

J. Laaksonen, 1993, Current Finnish Severe Accident and Source Term Positions and Practices, STUK, May 28, 1993, Finnish answer to the OECD/NEA/CSNI Questionnaire on Current National Severe Accident and Source Term Positions and Practices.

U. Schmocker, et al., 1991, Approach to Regulatory Review of Swiss Probabilistic Safety Assessments, Proceedings of an International Symposium on the Use of Probabilistic Safety Assessment for Operational Safety, PSA '91, Vienna, Austria, June 3-7, 1991, IAEA-SM-321/10.

T.G. Theofanous and H. Yan, 1991, ROAAM: A Risk-Oriented Accident Analysis Methodology, Proceedings of the International Conference on Probabilistic Safety Assessment and Management (PSAM), Beverly Hills, California, February 4-7, 1991.

H. Tuomisto and T.G. Theofanous, 1991, A Consistent Approach to Severe Accident Management, Proceedings of the OECD/NEA/CSNI Specialist Meeting on Severe Accident Management Programme Development, Rome, Italy, September 23-25, 1991.

H. Tuomisto, et al., 1992, Severe Accident Management Instrumentation in the Finnish NPP's, Proceedings of the OECD/NEA/CSNI Specialist Meeting on Instrumentation to Manage Severe Accidents, Cologne, Germany, March 16-17, 1992.

USNRC, 1989, Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, Summary Report, Second Draft for Peer Review, NUREG-1150, June 1989.

R.K. Virolainen and I.M. Niemelä, 1993, Implementation and Introduction of Living PSA in Co-operation with Finnish Utilities and Authorities, Proceedings of the International Topical Meeting on Probabilistic Safety Assessment, PSA '93, Clearwater Beach, Florida, January 26-29, 1993.

015 Decision Policy Management

Chair: R.S. Strait, LLNL

Risk Based Performance Goals and Probabilistic Source Term in Environmental Restoration and Waste Management Activities

D.A. Reny, T.E. Wierman (TENERA)

Managing Uncertainty in Risk Analysis Decisions

W.D. Rowe, K.J. Beierschmitt (Battelle Pantex)

PRA As A Management Tool: Improving the Safety of the Tiles of the Space Shuttle Orbiter

E. Paté-Cornell (Stanford U.); P. Fischbeck (Carnegie Mellon U.)

Reaching End of License - Big Rock Point

J.R. Schepers, G.C. Withrow (Consumers Pwr. Co.)

A Risk Assessment and Management Tool for the Chemistry and Metallurgy Research (CMR) Building

J.L. LaChance, A. Kolaczkowski, A. Crawford, J. Holderness, (SAIC); G. Medford (LANL)

RISK BASED PERFORMANCE GOALS AND PROBABILISTIC SOURCE TERM IN ENVIRONMENTAL RESTORATION AND WASTE MANAGEMENT ACTIVITIES

Daniel A. Reny and Thomas E. Wierman

TENERA, L.P.
477 Shoup Ave., Suite 201
Idaho Falls, ID 83402
Phone (208) 529-6691
Fax (208) 523-6946

INTRODUCTION

Environmental Restoration and Waste Management activities within the DOE Complex routinely encompass large quantities of nuclear materials dispersed randomly throughout stored or buried waste. When handling or processing this material, hazards analysis and/or accident analyses require an evaluation of the source term. Poor or non-existent data on waste radiological or hazardous contents are routinely encountered. Deterministic methods in cases like this can estimate the source term, but typically use highly conservative quantities that are highly unlikely to occur. These conservative deterministic methods may result in high consequences leading to unduly restrictive safety requirements. Many of the attempts to come up with a deterministic source term are also not defendable since they typically use gross assumptions.

This paper proposes an alternative approach that develops a probabilistic source term. The result is a risk (probability versus consequences) basis for determining safety requirements from hazard and accident analyses. The example in this paper illustrates how this alternative probabilistic approach has been used in an actual application. This paper provides a description of the processes and statistical methods used in developing and calculating the probabilistic source terms and how they were applied in the accident consequence analyses. These methods have many applications to large amounts of wastes previously generated and disposed with little or no records. The risk based approach provides a well documented and firm basis for applying cost effective safety design decisions.

The example application in this paper is a buried transuranic mixed waste remediation project. This is an environmental restoration activity where a buried waste pit will be excavated and contents retrieved. The contents of the pit mainly consists of waste generated from defense related production activities. The main radioactive source term consists of Plutonium (Pu) isotopes and Americium 241 (Am241) mixed in various forms and types of materials ranging from solids (wood, glass, metals, etc.) to solvents and oils absorbed in cement and other absorption materials. The radioactive content is the object of this example but some application to the non-radioactive hazardous constituents can also be found.

The retrieved contents will be processed to remove contaminants and package the recovered hazardous material for storage and disposal. The three main functions associated with this remediation are pit excavation, processing and packaging, and storage. The pit contents source term are defined to reside either in the pit excavation, in process, or in storage as a final packaged product. Based on available data, conservative assumptions were made defining the form of waste in all three areas. The types of potential accident events and form of the waste in the pit excavation and in process are relatively more vulnerable to release than the final packaged product in storage due to the assumed immobilization of the final product for disposal.

Contents were deposited in the pit in waste containers consisting mainly of 55 gallon metal drums and various size boxes. Records were kept on number of containers, type and weight of waste in each container, and approximate location where container was deposited in the pit. However, no records were kept indicating the amount of radionuclides in each container. Each drum or box was allowed, by administrative procedure control, to contain up to 200 grams of radionuclides per drum or 300 grams per box. However, it is known that the majority of the containers, with few exceptions, contain considerably smaller amounts of radionuclides. The problem that lies in the lack of data to verify the actual distribution of radionuclides amongst containers leads to deterministic bounding assumptions requiring the use of 200 or 300 gram source terms per container in hazard and accident consequence analyses without regard to likelihood whether a particular container may contain 200 or 300 grams. This results in severe consequences, especially if several or many containers are involved in any postulated accident release event. With no better representation or information about container contents, the 200 or 300 gram per container assumption leads to unrealistic (incredible) results.

OBJECTIVES

The main objectives of the use of a source term for this example application is to provide a basis for the hazard classification analysis and safety analysis. These analyses then provide the foundation of the safety design basis for the activity. Therefore, the source term used directly drives the results of the hazard classification and safety design basis of the activity. The hazard classification requires the use of a source term which represents the credible (greater than or equal to 10^{-6}) probability of a worst-case or bounding release occurring. The application takes the form of the probability of the release event occurring and the probability of the highest source term whose product probability is greater than or equal to 10^{-6}.

Without information relating the pit contamination concentrations to pit volumes, no

reasonably defensible assumptions could be made concerning how much of the pit source term could be contained in any given pit volume at risk to accidental release from any of the three functional areas in the activity. Furthermore, assuming the total volume of the pit source term is in each functional area at any given time is only valid for the storage functional area and is extremely conservative leading to excessive consequences for the excavation and processing functions. The objective here is to identify a reasonably defensible source term and pit volume for each of the three functional areas to be used in the hazard classification consequence analyses.

Safety design guidance allows for the use of a graded approach in accordance with the risks posed by the activity. For non-reactor nuclear facilities, safety design risk criteria can be found in Nonreactor Nuclear Facilities: Standards and Criteria Guide.[1] These guidelines allow higher consequences for lower probability events in accordance with accepted risk philosophy. In accordance with the approach for the hazard classification above, the probability of source term was used in conjunction with the probability of the accident release event to arrive at a total probability of release for each functional area accident scenario.

METHODOLOGY OVERVIEW

Since the end of the practice of burying waste in pits such as this example, waste containers have been stored above ground and are retrievable. Improved methods for sampling contents and assaying radioactivity have been developed and applied with good success. Therefore reasonably good data exists for waste that is now being stored. But the waste being generated and processing and packaging methods has not varied significantly over this same time period. Therefore, the above ground stored containers are very representable as a population base to the buried waste for which no data exists. This assumption is the key to the following example case. This assumption was researched and validated to the best extent possible. Some minor variations in waste methods and waste classifications between the buried waste and the above ground stored waste occurred but were accounted for in the analysis.

By making the above assumption, we were allowed to apply the data from thousands of above ground waste containers that were generated in the same manner from the same place as the buried waste containers. Statistics from the above ground data were related directly to the buried waste to form probabilistic distributions for the various waste forms and container contents and locations within the burial pit. This allowed the use of probabilistic source terms in analyses involving the retrieval and processing of the buried containers resulting in a risk based (probability versus consequences) hazard and safety analyses. Furthermore, the results of the probabilistic source term calculation were compared against a radioactive material mass balance estimate of the total contents of the pit. The mass balance method provided a conservative estimate of total radionuclide content to be not more than 20 kg. The probabilistic sum of all containers method provided an estimate of approximately 15 kg of radionuclides. These results are shown in Table 1 and provide a good independent validation.

To define a reasonable source term for the pit excavation source term and the in process waste source term, first a maximum waste volume of 50 cubic meters was assumed to bound the volume available in the pit excavation and in process. Then the maximum amount of containers that could reside within this volume is either drums or boxes. Based on Table 1, we see that the largest concentration of radionuclides resides within either the

Table 1. Pit waste container contents results.

Description	Number of Cont	Total Vol	Cont. %	Vol %	Min Plut /Cont	Avg Plut/ Cont.	Max Plut/ Cont	Avg PU Total	Avg. Plut/Vol Density
Sludge	2106	74973	35.21	41.9	0.0	0.7	157.0	1482	0.02
Paper, Wood, Metal, Plastic, Glass, Rubber, Misc.	1512	11304	25.28	6.3	0.0	1.5	98.0	2241	0.20
Graphite, Paper, Wood, Metal, Glass, Plastic	303	2265	5.07	1.2	0.0	10.8	198.0	3272	1.44
Empty	26	312	0.43	0.1	--	0	--	0	0.00
Wood Scrap	96	17952	1.61	10.0	0.0	12.5	164.0	1200	0.07
CWS-Type Filters	66	528	1.10	0.3	0.0	25.3	80.0	1670	3.16
Filters	1	118	0.02	0.1	0.4	45.5	135.0	46	0.39
Paper, Plastic, Rubber, Scrap Metal, Wood, Glass, Concrete, Equipment	423	52260	7.07	29.2	0.0	11.9	164.0	5034	0.10
Equipment and Scrap Metal	3	1569	0.05	0.8	0.0	8.7	302.0	26	0.02
Empty	1445	17340	24.16	9.7	--	0	--	0	0.00
Total	5981	1.79E+05						14970	

graphite containers or the filter containers. Since these two container codes are located at differing spots within the pit. The graphite code contains more total source term in one spot (defined as the worst-case "Hot Spot"), therefore the graphite containers were selected as the worst-case volume Hot Spot. The graphite containers are all drums and there are 227 drums in 50 cubic meters. The solution took the form of a four step process:

- Correlate disposal records from after 1970 to before 1970.
- Define a distribution for a drum in the "Hot Spot."
- Develop a distribution for the sum of 227 drums (the number of drums identified in the "Hot Spot").
- Integrate the distribution of the sums to come up with a confidence interval at selected probabilities.

The correlation of disposal records was based on descriptions of wastes provided by the generator and data collected in the more recent history. The major assumption that validates this correlation is that, intrinsically, the waste streams did not change at the generator in the time frame under scrutiny.

Once the disposal records were correlated, data was available to create a distribution. The data consisted of the maximum, minimum and average plutonium amounts in drums. A lognormal distribution was fit to these data with some confidence that no other distribution was as good at estimating the population. The lognormal distribution allows for exceptionally large radiological overloadings which are not in the records and therefore

assigns some probability to account for undetected errors.

The single drum distribution was sampled repetitively to total 227 drums using a Latin Hypercube sampling routine. This was performed 1000 times to develop a distribution of totals. The resultant histogram, shown in Figure 1, was tested and found to be lognormal.[2]

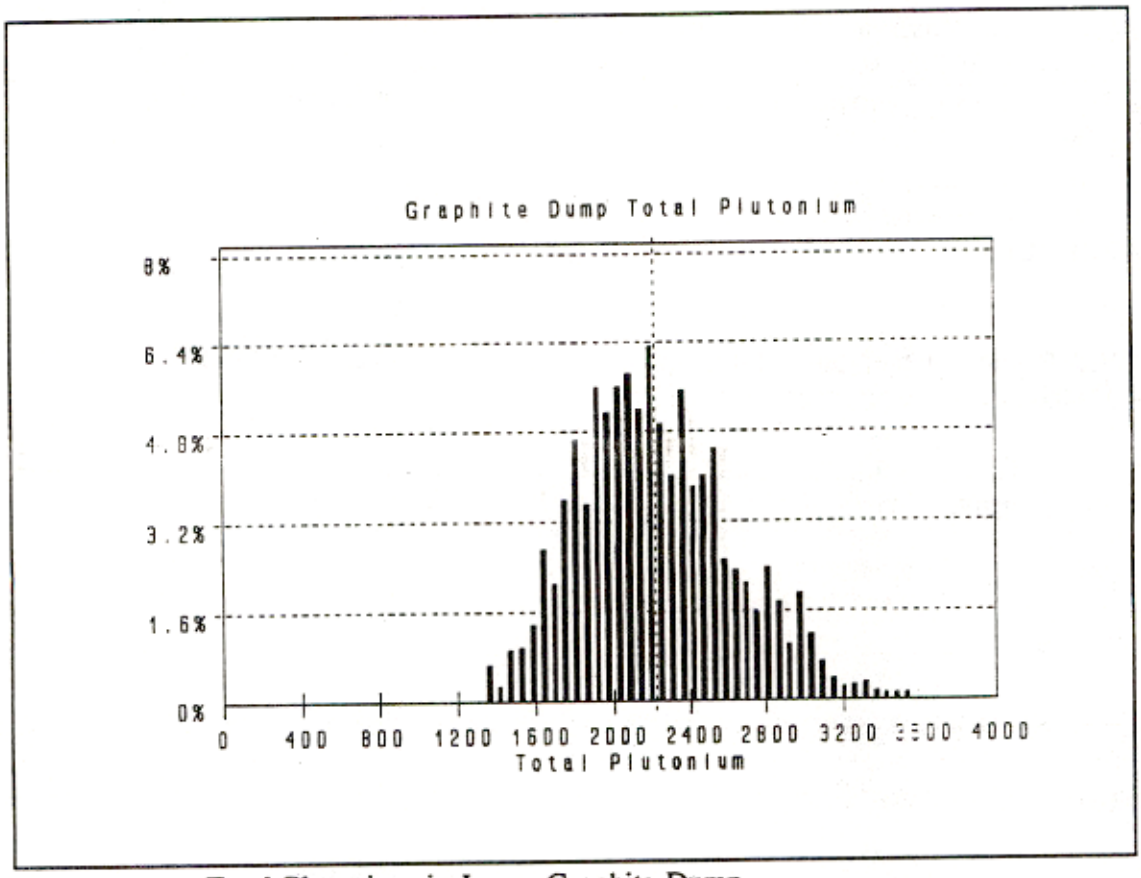


Figure 1 Total Plutonium in Large Graphite Dump

Since the distribution of the totals was determined to be lognormal, the integration was performed analytically. However, the distribution could have been integrated numerically if it was not a defined distribution. The integration gives us the probability that the total is equal to or greater than a specific value. The converse is also true, in that for a given probability (confidence) the total is not greater than a value determined by the integration. The results for the hazard classification source term showed that the bounding worst-case hot spot within the pit could be no larger than 5kg with a high confidence in the statistical results. Otherwise a conservative deterministic estimate of the source term would have been much greater possibly being two to four times as high.

Once the distribution of the total material is developed, we can select an amount of material at a certain probability and incorporate the value in the analysis as the material at risk in any given accident scenario for any given location of material in the pit excavation, in process, or the total pit contents for in storage at end of activity. The above process can be repeated and varying distributions of source term developed to meet the requirements of the hazard classification or more detailed accident analyses in the safety analysis report.

CONCLUSIONS

Past analytical methods have used overly conservative assumptions to represent source terms involved in accident release and consequence calculations. This has lead to overly conservative results driving excessively restrictive safety design requirements. Using probabilistic methods to represent accident release source terms can provide a defensible and more realistic source term. The probabilistic source term in conjunction with the probability of the accident event occurrence provides a more realistic representation of the risk that is also conservatively bounded with analytical data but overly conservative. This leads to more realistic accident probability consequence results. When evaluated with risk criteria, these results provide a well defined basis of a cost effective graded approach to safety design.

REFERENCES

1. W. J. Brynda, et al., Nonreactor Nuclear Facilities: Standards and Criteria Guide, DOE/TIC--11603-Rev. 1, September 1986.

2. L. G. Blackwood, The Lognormal Distribution, Environmental Data, and Radiological Monitoring, EGG-M-90316, EG&G Idaho Inc., Idaho Falls, ID, 1991.

MANAGING UNCERTAINTY IN RISK ANALYSIS DECISIONS

W. D. Rowe, Ph.D., K. J. Beierschmitt, Ph.D. PE

Risk Management Department
Battelle Pantex
P.O. Box 30020
Amarillo, TX 79177

INTRODUCTION

The Department of Energy (DOE) has undertaken a major change in the manner in which they address and regulate safety activities through the issuance of DOE Order 5480.23. This document should be thought of as an enabling document for significantly restructuring risk and safety management at DOE facilities rather than just one more routine DOE order.

The DOE order addresses normal, abnormal and accident conditions. While all these must be addressed, a primary focus is on accidents, particularly those with low probability of occurrence, but large consequences. There are very large uncertainties involved in estimating these accident conditions. While management would like to have a straightforward engineering procedure that will provide unequivocal results, such procedures do not and cannot exist. Dealing with irreducible uncertainty requires subjective judgments, except perhaps in *de minimis* cases where the risks are so small as to be below the level of reasonable concern. Management may not want to either admit or address the need for subjectivity, but it must be addressed and dealt with. Here, we seek to understand the nature of these judgments and manage them effectively and advantageously.

A. Uncertainty in Risk Decisions at Technical and Managerial Levels

1) Safety Basis and the Use of Risk Performance Standards.

In the past twenty years there has been increased effort in the area of standards to move from design standards to performance standards. This has been particularly true in the civil engineering field where the competition for designing and building structures such as bridges, buildings and industrial operations is high. Designs which have demonstrated performance in service over long periods have been reproduced without regard to inherent over-design. Such over-design is no longer competitive. Performance standards--levels of acceptable operation--provide opportunities for alternate, more effective, less costly

designs. The shift to performance standards requires means to explicitly establish levels of acceptable performance and means to measure whether a particular design can meet the performance requirement. *In many instances the performance cannot be measured directly, and lengthy in-service experience is not available.* In such cases designs whose performance have been demonstrated through testing, or designs that have not even been tested may be used. In the latter case models are used to "estimate" performance.

Risk and safety are system performance goals. They cannot be directly measured a *priori* (before the fact), only after the fact. Therefore, the only way to estimate risk and safety levels are through the use of models. There are a variety of models to choose from many of them unverifiable in any empirical sense. The choice of models, especially when unvalidated, leads to wide ranges of uncertainty. Selection of models then are based upon good engineering judgment, and such judgment is subjective. Who should make such judgments?

2) Risk Analysis Limitations

Risk analysis addresses the assessment of risk and how to manage that risk. In risk assessment we are concerned with the probability of a future event which has a consequence of a specified magnitude. In risk management the concern is how to prevent unwanted events and/or mitigate consequences of such events to acceptable levels.

It has been thought that risk assessment and risk management were two different tasks, and different people with different skills were needed. While this may be true to some extent, dealing effectively with the high levels of uncertainty present in risk analysis precludes absolute separation. Decisions about dealing with uncertainty, such as how much margin of safety to allow as a means to cope with uncertainty, are often made at the lowest engineering level. Although these decisions affect the cost and performance of the system, they are seldom made visible to management. Moreover, these margins of safety accumulate and multiply. Management needs to address them individually and in the aggregate to assure cost-effective, safe operations.

This type of management is called for in Section 3 of DOE 5480.23, and it is essential that management have appropriate tools. Managers have to be involved in understanding the uncertainties in critical decisions; and, when judgment is used for coping with uncertainty, the manager and the technician are jointly responsible.

B. Perspectives in Risk and Uncertainty

Scientists, regulators, design engineers, and management each have different perspectives on how they will address and cope with uncertainty. Unless the uncertainty is addressed explicitly and uniformly, these differing perspectives cannot be accommodated and commonly understood. More importantly, consensus cannot be reached and conflicting points of view may be suppressed, only to emerge after a decision has been made. Table 1 provides a characterization of how experts commenly will address uncertainty, and the limitations of each approach. All of these perspectives are valid, and there are probably others.This becomes very important when different professionals attempt to communicate with each other their approaches to establishing margins of safety to deal with uncertainty. The framework presented in the following sections provides a means of bridging this communication problem by explicitly making the extent of uncertainties and the use of margins of safety visible, repeatable, traceable and manageable. In the framework we seek to wed the Performance Management Approach with the Regulatory Approach. We are concerned that actual risks do not exceed estimates, but we also must know and understand the margins of safety (contingencies) involved and

what we pay for them. Decisions about how much margin of safety to allow are primarily subjective judgments

C. Range/Confidence Estimates and Sensitivity Analysis

Making uncertainty clearly evident in Safety Analysis Reports (SAR) has tremendous benefit in defending the models used to illustrate risk. In a high hazard industry one will typically find that the risk is dominated by extremely low frequency high consequence events. When having to deal with the extremely low frequency events it becomes evident that the models have a great deal of subjectivity. However, due to the absence of good frequency data these models attempt to be overly conservative. This makes the defense of the risk estimates very difficult.

Use of Range/Confidence Estimates provide a very clear picture of this conservatism and allow managers, those responsible for accepting or rejecting risk to play "what if" games with the models themselves. Experience has shown that when the Range/Confidence approach is used, that extremely low frequency events are relatively insensitive to the subjectiveness of the model and thus can be easily defended. In most cases, the Range/Confidence approach clearly illustrates that the resources needed to reduce the level of uncertainty in the model are not beneficial. In short, clear understanding and presentation of uncertainty in the SAR allows managers to ask the right questions, to be concerned with those uncertainties which do actually impact risk.

OBJECTIVE	LIMITATIONS
Scientific Risk Approach Provide the best estimate of risk and the ranges of uncertainty above and below the best estimate.	Tend to measure that which is measurable rather than that which is critical, but difficult to measure.
Regulatory Risk Approach Assure, with a given degree of confidence, that the actual risk does not exceed the risk estimate.	Very high margins of safety, may have high cost and preclude some beneficial activities.
Design Engineering Approach Use conservative, proven designs to produce engineering structures with minimum liability.	Very high margins of safety, may have high cost, and are subject to unwelcome surprises when applied in new environments.
Performance Management Approach Risks are one parameter used in balancing risk, costs, benefits and the performance of the structure. Uncertainty is addressed in all four parameters.	Risks cannot be measured, only modeled. Empirical verification of performance is often very difficult.

Table 1. Generic Approaches to Addressing Uncertainty

D. Range/Confidence Estimates as a means to address uncertainty.

The framework is based upon the use of Range/Confidence estimates of parameters rather than point estimates. At least three estimates are made of any parameter. In the case of risk, each estimate is a level of risk with a specified confidence that the actual risk lies below the stated level. The higher the risk level established, the more confidence one has that the actual risk lies below the level. The concept is directly analogous to setting confidence limits on one side of a statistical distribution. When a statistical sampling distribution is well established, then one knows all the possible levels and their confidence levels. It is called the power curve. However, in the case for uncertainty in risk, we only seek to estimate three specific levels. Moreover, these estimates may be entirely subjective (based upon unverified models) rather than reprinting empirical data as in the

analogy. Since actual data is sparse, and precise subjectiveness is ridiculous, further estimates are usually unwarranted.

The combining of these parameters and their confidence limits in a risk estimate provides a means to show management the range of estimates at various levels of confidence, leaving the subjective judgment of how much confidence is enough to management. When cost parameters are also considered, unique decision points are often found. Moreover the process has been automated such that management and interested parties can ask the "what ifs" and immediately see the impact of changes graphically.

THE RANGE/CONFIDENCE LEVEL APPROACH

A. Basic Perspectives

There are many ways to make range estimates. However, the method of making range estimates illustrated in Table 2 and described more fully below has been shown to be highly useful. Three estimates of a parameter (e.g., probability of an event with a given consequence magnitude) are made using alternative models or alternative levels of parameters within a model.

A "bare estimate" is made with *no margins of safety*. This is, by definition, a best estimate of what is likely to occur, but the actual risk that is being estimated may be either higher or lower. This type of estimate is very difficult to make with engineers who are trained to build in margins of safety. However, it is necessary to force this type of analysis if the margins of safety are to be made subsequently visible and used as a tool for addressing uncertainty.

ESTIMATE	MEANING	LEVEL OF CONFIDENCE*	
		QUALITATIVE	QUANTITATIVE**
BARE	Bare engineering estimate with no (minimal) margins of safety.	Most likely condition	50%, mean mode, median
CONSERVATIVE	Larger estimate than the bare estimate based upon effect of extraneous factors and engineered margins of safety.	Fairly sure that this estimate exceeds the actual risk	90-95% About 2 std. dev. above the mean.
WORST CASE	Larger estimate than the conservative, taking all reasonably possible excursions into account	Outside limit	99-100% 3 or more std. dev. above the mean
OTHER CASES	Interpolation between range limits as is useful.		

* The degree of confidence that the actual level of risk lies below the estimate.
** Assuming a normal distribution (which seldom occurs).

Table 2. Alternative Analytical Models with Different Margins of Safety.

A "conservative estimate" is made using margins of safety high enough to provide confidence (a reasoned subjective judgment) that actual risk lies below the estimate. This type of estimate is consistent with conservative engineering design. If the underlying

process was a normal distribution[1] then an illustrative example is the 90th to 95th percentile.

A "worst case estimate" attempts to make sure that the actual risk is always below the model estimate. The estimate takes into account all reasonable, imaginable excursions. In a normal distribution it would exceed the 99th percentile. It is also possible to use more than three estimates when warranted.

The three (or more) estimates make up a range estimate. Any one of the three estimates cannot be taken out of context with the other two. To do so invalidates the framework. The distance between the bare and the worst case estimate of a parameter is a measure of its uncertainty, and an uncertainty index may be derived by dividing the result of the worst case estimate by that of the bare case:

Uncertainty Index (UIX) = Worst Case Result/Bare Case Result

The magnitude of the index is used as a means to make comparisons about the relative uncertainty of range estimates. A higher index implies higher uncertainty in the range estimate.

Figure 1 shows the difference information provided by a range/confidence estimate over a point estimate. Both the range and the confidence intervals are shown. The concern is only with that part of the curve represented by the heavy line. The shape of the curve is determined by the three estimates, and no extrapolation beyond the heavy line is made.

Confidence levels are set by the estimator, and the basis for the estimate documented. Confidence levels may be set on the basis of: 1) uncertainty in measurement such as confidence limits in statistical distributions, 2) uncertainty in future events such as probability of occurrence of events, and 3) uncertainty in the validity of models used to describe complex system relationships. The first case is based upon empirical observations, the second case is based upon beliefs about the future, and the latter case upon established system behavior for validated models and wholly subjective for unvalidated models.

B. Combining Estimates

The advantageous use of range/confidence estimates becomes evident when multiple parameters are combined in a risk assessment model. Since there are three estimates for each parameter and all combinations of estimates must be made there are many more computations to be made. For example, if there are two parameters, nine estimates of risk are required. In general, the number of risk calculations to be made (N) is determined by:

$N = 3^n$ where n is the number of variables

Since all the calculations are arithmetic, they are easily automated. Spreadsheets work very well and a number of templates have been designed for this purpose. An example of a multiplicative model is the determination of the risk of ingestion of a chemical considered as a carcinogen in well water:

Lifetime Cancer Risk Increase = I x C xD x P/(W x 1000 x 25550)

Where

I = Ingestion in liters per day	Measurement Uncertainty
C = Concentration in ug per liter	Measurement Uncertainty
D = Days of exposure to factor C	Measurement Uncertainty
P = Potency-slope value in 1/(mg/kg/day)	Model Uncertainty
W = Weight in kg	Measurement Uncertainty
1000 = 1000 ug/kg	Conversion Factor
25550 = Number of days in 70 years	Conversion Factor

There are five parameters in the multiplicative model of which two, I and W, represent distributions of the general population. Range/confidence estimates are made for each parameter leading to $(3)^5$ calculations or vertices(243).

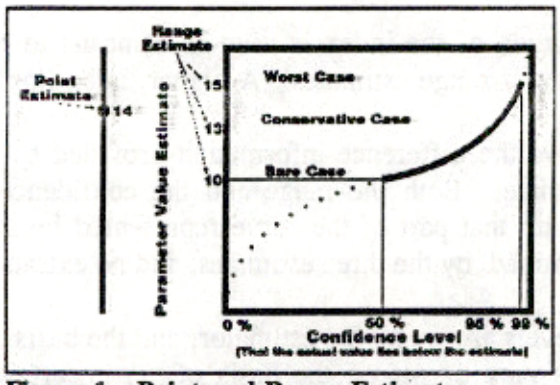


Figure 1 - Point and Range Estimates

C. Combining and Interpreting Confidence Levels

The combined confidence (C_k) for each level for each of the 243 cases (k=1 to 243) is also calculated. This can be done by integration over the confidence range or a conservative estimate can be made by the following formula:

$$C_k = (1 - 2^n \prod_{i=1,j=1}^{n,m} (1 - C_{ij})^n) \times 100\%$$

where n is the number of variables and m is 3, the range estimates for a parameter

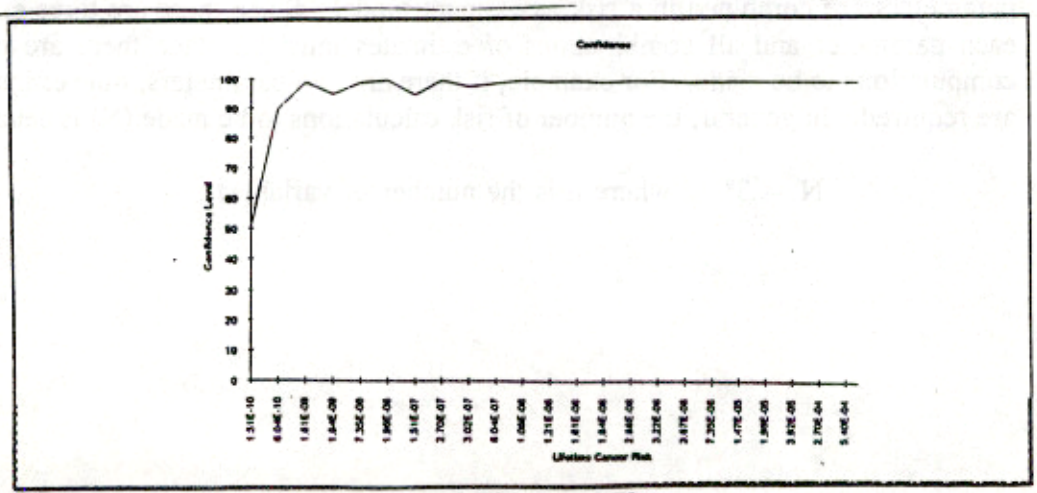


Figure 2 - Combined Confidence and Risk Level Plot

The risk and combined confidence pairs as well as the costs associated with each case can be sorted in order of increasing risk and plotted against each other. Figure 2 shows the results of such a calculation.

First, the levels of risk range over 7 orders of magnitude, from 1.5E-10 to 6.67E-03. Secondly the combined confidence rapidly increases to over 99% and exceeds 99.99% at very low risk levels. One can argue that a subjective choice of 99% confidence is well above normal practice, and that 99.99& is ultraconservative.Next, the unevenness at the beginning of the curve is an artifact of the ordering of the risk levels and the different uncertainty ranges (Uncertainty Indices - UIX) of the five parameters. However, the right hand downward slope segments represent conditions where a *decrease* in risk leads to *higher* confidence. These segments provide unique decision points for acceptance.

D. Trading Off Risk, Confidence and Cost

Since a separate cost estimate can be made for each vertex, these can be plotted against the risk level as well. An example of such a plot is shown in Figure 3. This plot is lumpy since the costs for the example shown are for different alternative actions regardless of the risk level. However, if one overlays the two figures, a zero or at worst a very low cost level can easily be found at a low risk level with a very high degree of confidence that the risk will not be exceeded. For example, an increased lifetime risk of 1.08E-06 (round to 1E-06) is obtained at 99.998% confidence at zero cost.

This is only one way of making such tradeoff decisions. Not only is the range of uncertainty made visible along with confidence levels, but management and the public can understand how the decision was made. Moreover, since the calculations are easily automated, it is very simple to plug a what if into the program for any or all parameters to see if they have any significant impact in making decisions.

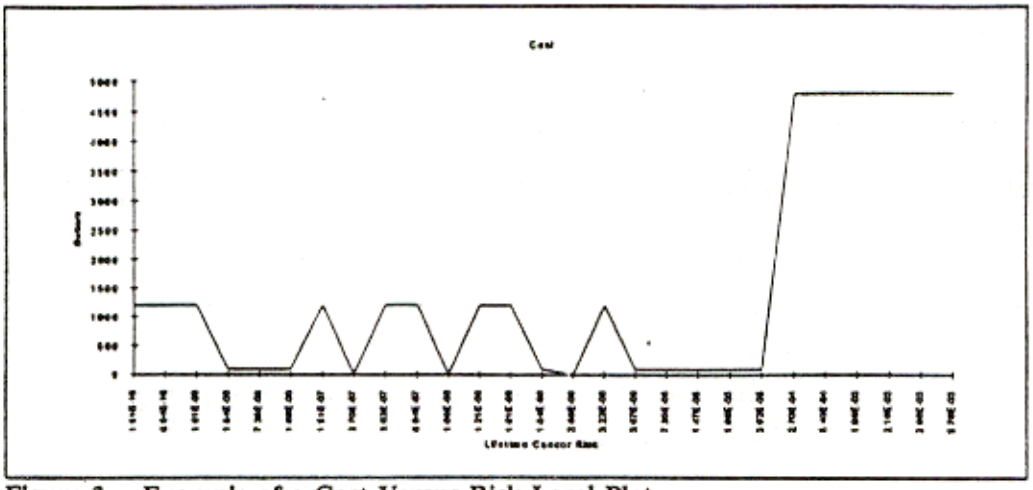


Figure 3 - Example of a Cost Versus Risk Level Plot

SUMMARY

Managing uncertainty in risk analysis decisions is a critical task in todays competitive environment. No longer can the analyst simply present risk with the uncertainty cloaked in subjective models. The Range/Confidence approach facilitates the presentation of uncertainty in an easily understandable fashion and can be readily used for cost benefit analysis. In addition, use of this approach greatly adds to the defensibility of the analysis, and can be used directly to perform sensitivity analysis on subjective assumptions made by the models. This approach has been applied to many different aspects of risk management, both to the analysis element, and the design and engineering elements. It has been found to be an effective tool for bridging the gap between the decision makers, and the designer/analyst. The Range/Confidence approach provides an effective tool the manage uncertainty in the risk analysis decision making process.

PRA AS A MANAGEMENT TOOL: IMPROVING THE SAFETY OF THE TILES OF THE SPACE SHUTTLE ORBITER

Elisabeth Paté-Cornell[1] and Paul Fischbeck[2]

[1]Professor of Industrial Engineering and Engineering Management, Stanford University
[2]Assistant Professor, Department of Engineering and Public Policy, Carnegie Mellon University

INTRODUCTION

This paper presents a probabilistic risk analysis (PRA) for the black tiles of the heat shield of the space shuttle orbiter, and the management improvements that were recommended and implemented based on this PRA (Paté-Cornell and Fischebck, 1992a and 1992b). The black tiles cover the lower surface of the orbiter and protect the aluminum skin from failing under the heavy heat load to which it is subjected at reentry. They are, therefore, a critical part of orbiter safety systems.

The tiles and their purpose

The space shuttle at launch, includes the orbiter itself, an external tank (ET) that contains the fuels (liquid oxygen and liquid hydrogen) for the orbiter's main engines, and two solid rocket boosters (SRB's). The fuel is brought from the external tank to the main engines by a fuel line that runs along the right side of the ET's surface (under the orbiter's right wing).

A typical flight profile includes a launch phase in which the orbiter is propelled by its main engines and the SRB's. During this phase, the shuttle is subjected to heavy loads (vibrations, aerodynamic forces, possible debris hits) that can damage the tiles. The SRB's are then jettisoned and retrieved at sea. When the orbiter reaches orbit, it separates from the ET. After completing its mission, the orbiter reenters the atmosphere, at which point it is subjected to increasing particle friction and heavy heat loads. It is at this stage that a failure of the heat shield could lead to a weakening or failure of the orbiters's aluminum skin, severe damage to critical subsystems and loss of the orbiter. The flow of hot gases along the orbiter is laminar at first, then becomes turbulent. The frictions increase dramatically during this stage. Therefore, the later this transition, the lighter the total heat load. The surface of the orbiter must therefore be smooth so as to prevent early transition to turbulent flow.

Motivations and challenges

NASA and the astronauts were worried about the tiles (a definitely low tech part of the shuttle) and their bonding to the orbiter: even though the system has been certified for a hundred flights, some uncertainties remain about the performance of the bond in the long run. PRA was recommended after the Challenger accident to set priorities among the different improvements that seemed needed at that time. The accident had revealed some management weaknesses and problems created by NASA's general optimism about risk. Finally, in recent years NASA's budget has shrunk and the agency had to do more with less resources. It seemed, therefore, desirable to re-examine some of the procedures.

The scope of this study is an extended PRA for the black tiles. We computed the contribution of the tiles to the overall probability of an accident, the risk-criticality levels of the different tiles, and we extended the analysis to include key organizational factors such as the effect of time pressures and the geographic dispersion of the main contractors. The challenges of this study included the complexities of the system, the scarcity of statistical data, and the fragmentation of NASA as an organization and consequent turf problems (particularly among space centers). This study was done as part of a cooperative research agreement between NASA and Stanford University. It was funded by NASA headquarters (Office of Safety and Mission Assurance).

THE PRA MODEL

System and failure modes

There are about 22,000 black tiles on the lower surface of most orbiters (about 27,000 on Columbia). They are silicate blocks (roughly 6"x6"x2") covered with a black glazing (see Figure 1). They are displayed by arrays, slightly out of line to reduce the exposure of adjacent tiles to hot gases if one tile is lost. They are glued by a "room temperature vulcanized" (RTV) material to a felt pad (strain isolation pad) bonded to the aluminum skin of the orbiter. Gaps between the tiles provide flexibility and permit the venting of the gases at ascent. Some of the spaces between the tiles are filled with a gap filler which must fit perfectly in order to keep the orbiter's skin as smooth as possible.

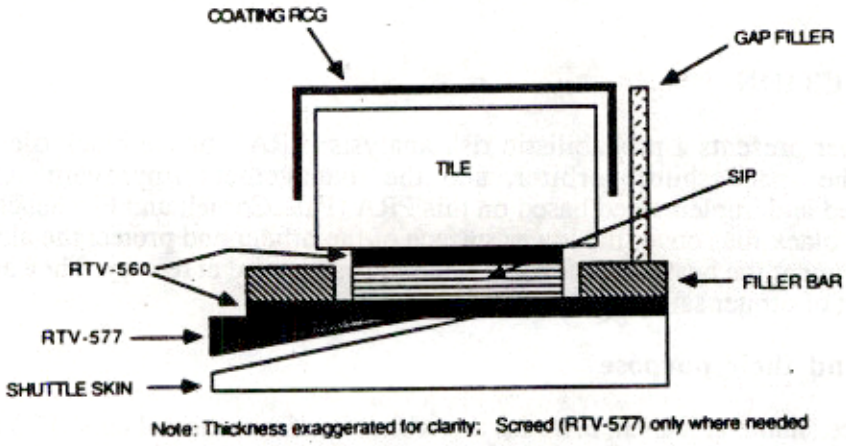


Figure 1. The tile system

There have been few tile problems: only two tiles were lost in flight, both on orbiter Columbia. One tile debonded under regular loads because the bond had weakened due to a reaction with the waterproofing agent, another because of a debris hit at ascent during flight STS-27. Debris hits have been a problem in most flights. We obtained from one of the contractors a map showing the debris impacts after every flight. We compiled a cumulated map of such debris and observed an asymmetry in the pattern: the debris hits were much more likely to occur under the right wing of the orbiter because the fuel line along the ET was weakening its insulation on that side. The two main failure modes that are considered in this study are therefore : (1) a tile is lost under debris impact or (2) a tile debonds under regular expected loads because of a weak or inexistant primary bond.

Structure of the probabilistic risk analysis model

The model is base on two concepts: *susceptibility* (i.e., the probability of losing tiles either under excessive loads or because of a weak capacity), and *vulnerability* (i.e., the consequent loss of critical shuttle function, for example, the loss of the hydraulic system that controls the landing gears and the control surfaces necessary for landing).

Accident scenarios involve: (1) a loss of initial tile(s) that causes at reentry a gas turbulence in the cavity and an increase of the heat load on the bond of the adjacent tiles, (2) potential loss of adjacent tiles and the possibility of a formation of a failure patch of size

greater than the initial tile loss, (3) high temperatures at the bottom of the cavity and exposure of the aluminum skin to hot gases, (4) a burnthrough if the aluminum skin fails under the heat load, (5) loss of critical subsystems (e.g., the avionics or the loss of the hydraulic lines) due to hot gases penetrating inside the structure, and (6) loss of the orbiter (Loss of Vehicle and Crew: LOV/C).

The influence diagram shown in Figure 2 was used for the computation of the probability of LOV/C.

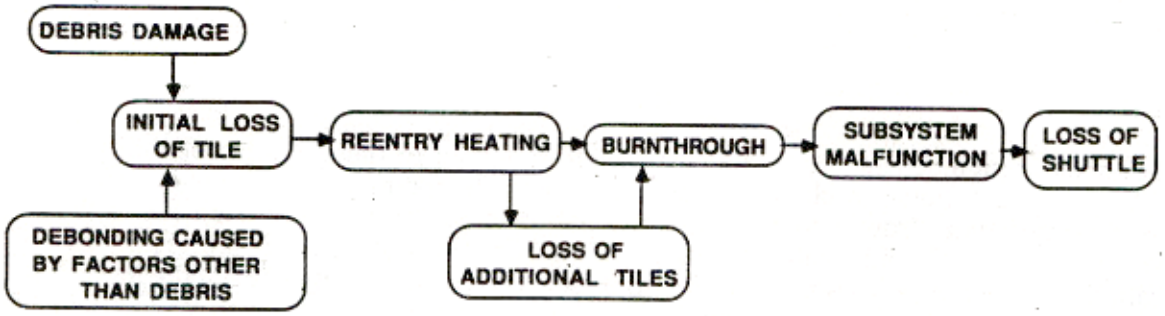


Figure 2. Influence diagram for the computation of the probability of LOV/C

This influence diagram includes the following events and random variables:

° The initiating events, either the spontaneous debonding of one tile or the debonding of up to four adjacent tiles initially lost to debris hit:

° The final patch size characterized by the probability distribution of the number of adjacent tiles finally lost conditional on the initial loss of tiles;

° A burnthrough characterized by the probability of a hole in the orbiter's skin conditional on a failure patch of a given size;

° The loss of a subsystem characterized by the probability of failure of a subsystem under the skin conditional on a burnthrough;

° The loss of the orbiter characterized by the probability of LOV/C conditional on a failure of some subsystems due to a burnthrough.

The analysis thus relies on a certain number of probabilities, some of which were available from existing statistics (e.g., the density of tiles hit by debris larger than one inch); others were encoded as expert opinions, for example, the probability of loss of critical subsystems under the skin given a burnthrough. When there were fundamental uncertainties in these expert estimations, we made consistent use of means (e.g., mean future frequencies of events). The objective of this pilot study was a first-order analysis only since our goal was to rank the tiles by order of risk-criticality.

The probability of spontaneous debonding was estimated to be the same for all tiles. 130,000 tiles had been installed on all orbiters at the time of the study and half of them had been processed. Twelve had been found to be without primary bond, and the probability of debonding of such a tile was estimated by experts at 10^{-2} per flight. Therefore, for any tile, the probability of spontaneous debonding for lack of a primary bond was estimated at 9×10^{-7}. In addition, the probability of losing a tile due to a weak but existing bond was estimated at 2×10^{-4}, 50 times less likely to cause debonding but 10 times more frequent. Therefore, for each tile, the probability of debonding due to such a bond was estimated at 2×10^{-7}. 80% of the risk of debonding was thus found to be attributable to tiles without primary bond.

The other events and variables of the PRA depend on the location of the tiles on the orbiter's surface. The orbiter was therefore partitioned into zones where tiles shared similar characteristics along four dimensions: the density of debris hits, the potential loss of adjacent tiles given loss of the first ones (which depends mostly on aerodynamic forces), the potential for burnthrough which depends mostly on the surface maximum temperature in each zone, and the criticality of the subsystems under the skin at the location of the corresponding min-zone.

For each of these four factors, we constructed a map of two or three zones (e.g., high or low probability of secondary tile loss). We superposed the four maps and obtained by intersection, 33 min-zones where all tiles shared similar characteristics. These four maps are shown in the original report (Paté-Cornell and Fischbeck, 1990).

For each min-zone, we then computed the probability of LOV/C due to tile failure and the risk-criticality of each tile. To do so, we computed in sequence:

- The probability distribution of the final patch size given the loss of an initial tile by spontaneous debonding, or of one or more tiles due to debris hit;
- The mean number of failure patches;
- The probability of failure of the orbiter for a given failure patch given its size and its location;
- The probability of failure of the orbiter due to all tiles of a specified min-zone;
- The probability of failure of the orbiter due to all tiles and both failure modes.

Results

The results included the contribution of each min-zone to the overall probability of LOV/C, the contribution of each tile in each min-zone to the overall probability of LOV/C, a risk-criticality factor (from 1 to 100) proportional to the contribution of each tile to the probability of LOV/C, and finally, a ranking of all min-zones by order of individual risk criticality. This ranking allows tile priorities to be set. The risk-criticality of each tile in each min-zone is shown in Figure 3. We showed that the most risk-critical areas were on the right side under the crew cabin and at the location of the right main landing gear.

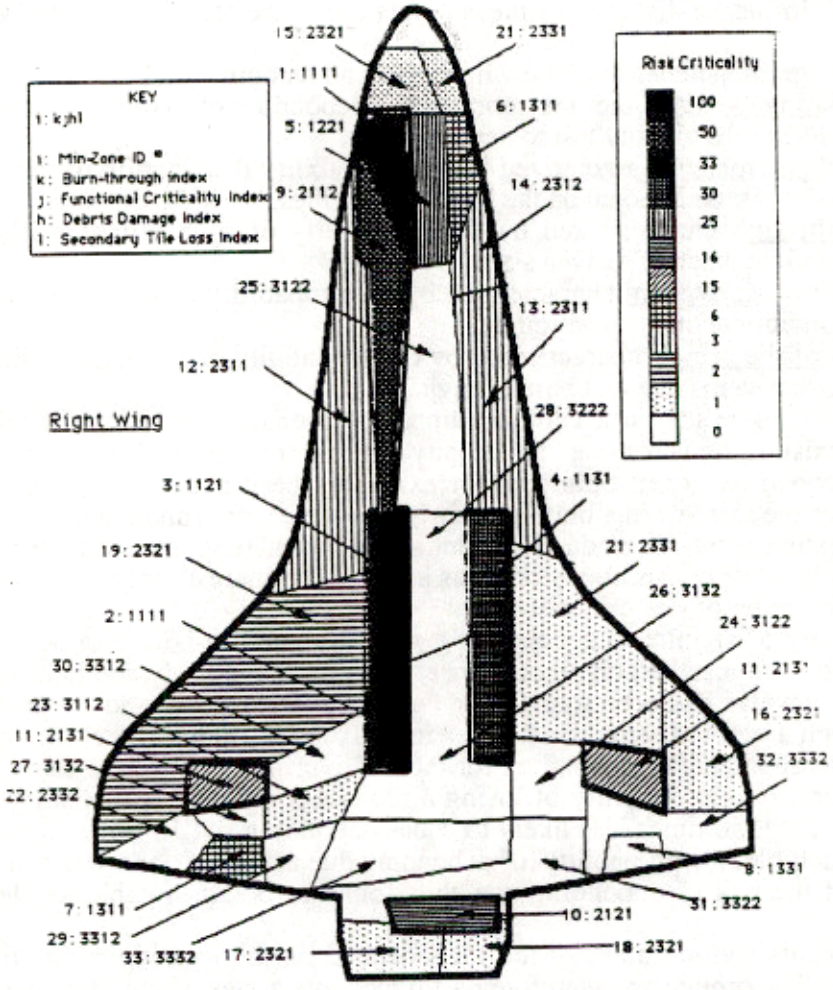


Figure 3. Map and zonation of the lower surface of the orbiter and risk-criticality factor for each tile in each min-zone.

We found first that the probability of LOV/C due to the tiles was in the order of 10^{-3} per flight, or about 10% of the overall probability of losing each mission as estimated by NASA for the Galileo mission. We also found that 85% of the risk was attributable to 15% of the tiles. Finally, we showed that 60% of the risk comes from spontaneous debonding whereas 40% comes from debris hits. The contribution of the tiles to the overall risk of accident was lower than generally feared. It was also observed that the most risk-critical tiles could not be

easily guessed *a priori*, in part because they resulted from the superposition of four maps, one of which was asymmetrical. Note again that our study did not include the effect of space debris, the possibility and consequences of a failure of the guidance system at reentry, and the effects of uncertainties about the probabilities involved.

TILE MAINTENANCE: RECOMMENDATIONS AND IMPLEMENTATION

After each landing, the tile maintenance process involves first a damage inspection of all tiles and a decision of what should be done. Some tiles are fixed; others are replaced and a pull test is used to check the strength of the bond. Step and gap measurements allow the smoothness of the surface to be checked, and in some where necessary, a gap filler is installed. At the end of this process a final inspection by NASA takes place. It is a detailed inspection of about 10% of the tiles to monitor any signs of deterioration, slumping, aging, and heat damage. It is this in final inspection that we proposed that NASA use our risk-criticality scale to inspect for tiles that have nonexistant or minimal bonds.

Key organizational issues

Some key organizational issues affect the quality of these operations. Most of the work is performed by two contractors, one mainly related to Johnson Space Center, the other to Kennedy Space Center. NASA specifies the tasks but intervenes only in the initial inspection and the final stage.

Time pressures have affected the quality of the tile maintenance because tile work was often on the critical path to the next launch, especially after flights where the damage had been extensive. Under pressures, the tile technicians can be either rushed or tempted to cut corners when specific production targets have to be met. In fact, at least one of them was caught spitting in the RTV to make it cure faster. The problem is that it may also cause the RTV's catalytic reaction to revert earlier to a liquid state than it would have otherwise. Time pressure may also lead to tiles being installed partially resting on the filler bars thus reducing the contact surface.

At the time of the study, conflicts among contractors were caused by competition for all major contracts, and for legal reasons, both contractors had legitimate motives to protect themselves from liabilities should an accident occur. The result was that the flow of critical information had sometimes been slowed down.

The status of the tile technicians prior to this study was quite low. They little input into the launch decisions. Furthermore, they described the attitude of other technicians towards the tiles as "no respect." The result was that some tiles were damaged when other work was done and additional tile repair was needed, which added further to the tile work load.

Under these time pressures and resource constraints (for example, the limited total number of inspectors), it seemed logical to set priorities. Yet, the concept of priorities did not exist for fear that some parts of the system might be neglected, the philosophy being that everything had to be done perfectly. It is only after the Challenger accident that NASA recognized that it was in fact living with some compromises and that priorities were needed.

Finally, the different subsystems were managed independently. This is understandable given the geographic dispersion of the different organizations involved. Yet, the performances of some subsystems are linked in ways that may not appear clearly until a good top-down PRA is performed. This was the case of the coupling between the insulation of the external systems (ET and SRB's) and the safety of the tiles.

Effect of human errors

The technicians' errors that occur in the maintenance phase affect the reliability of the tiles in several different ways. First, some tiles were poorly bonded, either because there was no primary bond between the SIP and the aluminum skin (it had dried before pressure was applied) or because the tile was resting on the filler bars. Second, the smoothness of the orbiter's surface is critical to the time of shift from laminar to turbulent flow at reentry. When this occurs is largely determined by the accuracy of the measurement of the steps and gaps between tiles and the efficacy of the correction procedure. Yet, this measurement at the time of our study was done using plastic gauges that did not provide a very good reading. Automation of this process should permit better results.

Problems of insulation debonding from the ET and the SRB's have been studied for quite a while. They are particularly acute along the fuel line on the ET's surface and seem to be caused by difficulties of installation of the insulation. If part of this insulation debonds, it can seriously damage the orbiter's tiles. Some work has been done at NASA to simulate the trajectories of insulation debris after debonding. These trajectories depend on the many factors (i.e., speed, attitude, loadings, altitude, etc.) of the vehicle, but a systematic analysis should permit the identification of risk-critical areas on the surface of the external systems.

Recommendations, implementation, and benefits

Based on our study, we made a number of recommendations:

1. NASA should use our risk-criticality scale to set priorities in its final inspection;
2. These priorities should be extended to insulation management on the ET and SRB's;
3. A subsequent tile PRA should be completed using better probability assessments for the probability of failure of subsystems given burnthrough and a full study of secondary uncertainties;
4. Time pressures on the tile technicians should be reduced;
5. Information flow among the contractors should be improved;
6. The technicians' pay scales should be improved to reduce turnover and the corresponding loss of expertise.

Most of our recommendations were implemented. The priority map of the tiles that we developed has been used on the shop floor to select the tiles to be inspected before launch (along with a map of the orbiter's surface temperature since NASA must monitor the effect of heat cycles on the aging of the bond). Perhaps the most important effect of this study is that it contributed to NASA's decision to perform a PRA for the whole of the space shuttle. The notion that *this PRA could be used as a management tool* and not only to "prove" that specific systems were safe seems to have been recognized. The management of the external systems has been improved as a result of many factors (our study was only one of them) and the insulation has been reinforced along the fuel line. Consequently, the mean number of debris hits per flight has been reduced from 40 to 14. Still, more work needs to be done on the debris trajectories. The information flow among the contractors has been improved and the technicians at KSC have been given direct access to relevant parts of the data base. The tile technicians' pay scale has been changed to close the gap with that of other workers. Finally, their training has been improved to include the nature of the subsystems under the skin at the different locations.

We computed the risk reduction benefits of simultaneously detecting the tiles that had weak bonds in the most risk-critical areas and of reinforcing the insulation of the external systems. We found that the combination of these two measures yields a risk reduction of the about 75% of the initial tile risk and, therefore, of about 7.5% of the total probability of accident per flight. The consequences of an accident can be evaluated at a cost of about $5 billion, the loss of 5 to 7 astronauts, and considerable political damage to NASA. Therefore, even a modest reduction of 7% of the risk per flight for a minimum of ten flight per year lead to an expected value of $35 million annual benefits.

In conclusion, this pilot study has contributed to a change in NASA's perspective about risk and priorities. This PRA for the tiles and the study of its management implications will be followed by further work for the whole of the space shuttle.

REFERENCES

Paté-Cornell M.E. and P.S. Fischbeck: Safety of the Thermal Protection System of the STS Orbiter: Quantitative Analysis and Organizational Factors. Research Report to NASA Kennedy Space Center, December, 1990.

Paté-Cornell M.E. and P.S. Fischbeck: Probabilistic Risk Analysis and Risk-based Priority Scale for the Tiles of the Space Shuttle, Reliability Engineering and System Safety, Vol. 40, pp. 221-238, 1993a.

Paté-Cornell M.E. and P.S. Fischbeck: PRA as a Management Tool: Organizational Factors and Risk-based Priorities for the Maintenance of the Tiles of the Space Shuttle Orbiter, Reliability Engineering and System Safety, Vol. 40, pp. 239-257, 1993b.

REACHING END OF LICENSE - BIG ROCK POINT

James R. Schepers[1] and Gregory C. Withrow[2]

[1]Nuclear Performance Assessment Department
[2]Big Rock Point
Consumers Power Company

Introduction

There are 107 licensed operating reactors in the US today. Collectively we provide about 20 % of this country's electrical energy. A short review of recent generation statistics indicates this is a stable contribution. However, since 1989, six units have been removed from service well prior to their 40 year design life. As never before, we are an industry under fire to live up to the promise of safe and affordable electric generation from the nuclear option.

While there are many issues, probably the most important one facing a utility with an old plant is economic. Although average U.S. plant capacity factors have been generally increasing over the past few years, costs, until recently, have also increased, generally faster. "Life Extension" beyond 40 years, for Big Rock Point, has not been shown to be economic. Therefore, Consumers Power has chosen a simple approach for Big Rock Point ; address the issues directly and work cooperatively with the regulators to achieve the End of License (EOL). We believe this goal is appropriate for both the electric customers of the plant output, as well as an example to the industry.

Big Rock Point

Following the 1992 closing of Yankee Rowe, Big Rock Point became the oldest operating plant in the industry. Big Rock is a 70 MWe General Electric Boiling Water Reactor that went into commercial operation in 1962. There are many unique design features, including;

- Single Steam and Feedwater Lines,
- Gravity Feed Liquid Poison System,
- Passive Emergency Condenser,
- Scram Dump Tank,
- In-Containment Spent Fuel Pool, and
- Steel, ventilated Containment.

Big Rock has led the industry in several innovative areas, including ;

- One of the earliest power applications of mixed oxide fuel
- An early user of PRA to resolve generic industry safety issues
- Use of a 'Living Schedule' to address regulatory and plant generated issues

Big Rock has always been a ground breaking plant. Along the way, the plant has generated more than 10 million MWHr for the Michigan electric grid, and accumulated a 60 % unit capacity factor (MDC). In 1991 Big Rock was awarded the status of Nuclear Historic Landmark by the ANS. The plant has operated for 16 years without a lost time accident.

Perhaps the most significant aspect of Big Rock's performance is that it continues in the current regulatory environment with only 154 plant employees (and 20 non-plant staff individuals).

Big Rock EOL

The last 'first' we hope to accomplish at Big Rock Point is to be the first to operate for the full licensed period. For BRP, this is May 31, 2000. Many challenges stand between us and that goal. As a strategy, we have chosen to establish reaching EOL as the primary plant goal, and ordered our efforts toward addressing the issues at hand. We have as a first matter, refined our thinking as to what success means for Big Rock Point . To achieve EOL, we will need to ;

- Foster commitment to robust Operations, Maintenance, and Engineering.
- Grow away from long-term initiatives to focus resources on maintaining facility in top condition and retaining experienced personnel to assure safe plant operation.
- Develop a relationship with the NRC that assures resources are correctly allocated.
- Prepare the facility for decommissioning concurrent with day to day safe and economic operation.

A primary philosophical underpinning of this effort is our commitment to safe and efficient operation. Assurance of nuclear safety is and will continue to be of paramount importance. Our principles of plant operation will be as follows;

- Be risk attentive, evaluate risk and react to risk conservatively.
- Assure selection of actions and programs provide the most cost effective risk benefit.
- Communicate with the NRC so they can be aware of the BRP actions and programs effect upon risk.
- Build upon the successful risk program that already exists.
- Terminate plant operation if safety levels cannot be maintained.

Big Rock has organized a team to manage these issues, led by a senior plant staff manager. In considering our regulatory processes, we have concluded we can accomplish these above objectives within the current structure.

Integrated Plan (IP)

To accomplish the above in the most economic fashion, requires a single decision making process that addresses both company internal and regulatory initiated issues. At Big Rock Point, this process is called the Integrated Plan (IP). Big Rock Point has for

several years been one of the few plants using an " Integrated Living Schedule" to rank new regulatory issues within current commitments. This process evaluates the use of engineering resources with respect to modifications and programs. The purpose of this process is to work on activities that are the most important for BRP and to communicate the resulting priorities to the NRC.

The evaluation of issues is performed by the Technical Review Group (TRG) based upon four criteria. The criteria are;

1. The ability to achieve safe shutdown
2. Minimization of radionuclide release
3. Enhancement of personnel safety
4. Improvement of plant availability

Recently an improved method has been developed to provide a more quantitative evaluation. The value ranking methodology has been updated to include insights and lessons learned from other utility experiences, and for example, applicable local, state and federal regulations as they apply to utility operations.

In order to better allocate scarce resources, Big Rock Point has begun implementing this more quantitative form of project ranking. This improvement attempts to explicitly achieve a better balance among plant goals. Projects (and thereby issues) are evaluated and ranked according to their benefit and cost contribution to the following plant goals : Business Performance, Safety Performance, Human Performance, Reliability, and Regulatory Performance. The nuclear safety values of the method are supported by the plant IPE. This method produces an initial ranking, that is input to the TRG process.

The membership of the TRG is diverse, representing operations, engineering, probabilistic risk assessment, health physics and nuclear licensing. The diversity is important as final rankings are necessarily subjective with quantitative input. The membership nominally involves six people of which half represent the BRP plant organization. Use of non-BRP expertise is intended to provide a more balance evaluation. Some of the industry generic issues evaluated by this process include; Station Blackout, Alternate Rod Injection, Recirc Pump Trip, and Seismic Weak Links. It is our intention to use this methodology to also evaluate ; SQUG, Reactor Vessel Structural Integrity, and the Maintenance Rule.

Human Resources Plan

Attracting and retaining critical and experienced staff to the end of license is a crucial issue. We are addressing this issue directly by initiating focus group meetings with all employees. Reducing the uncertainty for these employees is the primary focus of the Human Resources portion of the EOL strategy. Along with the Decommissioning Planning, the Human Resources Plan, will reduce employee uncertainty regarding length of future service at Big Rock, Company re-employment and relocation. Employee direct participation in deciding their future is the employed strategy. The plan includes new job and personal development training to prepare employees for future new jobs, in or out of CPCo. Presently there are approximately 174 CPCo employees at Big Rock Point. We recognize that maintaining the right 'climate' is absolutely essential to success in this area, as well as continued safe operation for any period, at any plant.

Communication Plan

As with 'routine' plant operation, there are many stakeholders related to those decisions occurring near the end of a plants licensed operating period. Some of those

stakeholders are; employees, NRC, Michigan Public Service Commission (MPSC), media, local government bodies, environmental groups, and local residents. All these parties need a reliable source of routine information to satisfy their diverse values and interests. Planning for this communication process early in the EOL development effort permits timely and reliable information services. The Communications Plan continues in-place community activities such as ; an active plant tour program, sponsoring local Chamber of Commerce 'After Hours Nights', and periodic briefings of elected local officials and major media contacts. Increasingly, these contacts will contain EOL specific content. Additionally, the plan calls for the development of a Citizen's Advisory Board, comprised of local 'opinion leaders', and the development of an EOL booklet specifically for employee - community communications. The basic underlying assumption of this plan is that we have an obligation to the local community, and stakeholders at large, to meet their information needs, on their terms, as the information becomes available.

Decommissioning Plan

This portion of the EOL effort is not only important in and of itself, but also for its impact upon the other portions of the EOL effort. Knowing how and when decommissioning will occur is important for planning purposes of all stakeholders and allows them to define their position with respect to BRP. In order to accomplish EOL, CPCo will submit a Final Decommissioning plan in June of 1994. A letter to this effect will be docketed, and presented by senior CPCo management to senior level NRC management. This submittal will be the cornerstone of the EOL strategy. CPCo will use a 50.59 analogous review process to "maintain" the plan during its use. This will allow the plan to be modified during its use without NRC approval when such changes do not affect safety analysis or the health and safety of the public.

Industry Initiatives

Given the generic significance of the BRP EOL effort, several industry discussions have been initiated , including the following;

- Research Issues (INEL and NRR)
- BWROG
- General Electric
- INPO

Status Summary

The above status of the Big Rock Plan provides a window into how Consumers Power is approaching "End of License" at it's oldest nuclear plant. More importantly this presentation was intended to convey some of the reality of the pursuit of "End of License". It is a form of " life extension", the one to which all operating reactors should soon give their attention.

A RISK ASSESSMENT AND MANAGEMENT TOOL FOR THE CHEMISTRY AND METALLURGY RESEARCH (CMR) BUILDING

Jeffrey LaChance[1], Alan Kolaczkowski[1], Gordon Medford[2], Arthur Crawford[1], and James Holderness[1]

[1]Science Applications International Corporation
[2]Los Alamos National Laboratory

INTRODUCTION

The Chemistry and Metallurgy Research (CMR) Building at Los Alamos National Laboratory (LANL) has been analyzed for potential accidents and the consequences of such accidents. This analysis was conducted on the basis of requirements for performing Safety Analysis Reports (SARs) contained in the Department of Energy (DOE) Order 5480.23 and related guidance documents. The analysis identified the dominant accident scenarios and generated a detailed model that can be used to manage risk in the facility.

REQUIREMENTS AND GUIDANCE

In April 1992, the DOE issued DOE Order 5480.23 which established revised safety analysis requirements for nuclear facilities. In section 6 of that order, the DOE stated that "It is the policy of the Department that nuclear facilities and operations be analyzed to identify *all* (italics provided here for emphasis) hazards and potential accidents associated with the facility..." Section 8 of the order provides for a graded approach for the level of analysis commensurate with "(a) the magnitude of the hazards being addressed; (b) the complexity of the facility...; and (c) the stage or stages of the facility life cycle..."

Attachment 1 of the order provides guidance for meeting the requirements of 5480.23 in which it is stated that "DOE expects that safety analyses prepared in accordance with this Order will be a significant upgrade from those previously required..." Particularly, "SARs are to make appropriate use of new safety analysis methods, including, but not limited to, risk assessment, reliability engineering methods, and human factors safety analysis." Lastly, "A continuous spectrum of such scenarios should be evaluated in order to identify the dominant risk contributor."

In additional guidance on the graded approach recently provided to LANL by the DOE Albuquerque Field Office, hazard category 2 facilities like the CMR are allowed to "...focus on identifying bounding, worst case sequences."

COMPLIANCE CONSIDERATIONS

The above requirements and guidance clearly demonstrates DOE's desire to produce safety analyses that go beyond those formerly done under DOE Order 5481.1B. The CMR facility is a relatively old structure which was designed to meet building code and "good engineering practices" at the time of its design and construction. It is a facility that, because of its research-oriented purpose, has continuously changing processes that hence provide continuously changing hazards and risks. Finally, the CMR management staff desired a risk model with which to more formally identify and manage risks at the facility especially as processes change. These factors all affected the decision to perform the CMR accident analysis using formal Probabilistic Risk Assessment (PRA).

METHODOLOGY

PRA has embodied within it, many of the characteristics described above for addressing compliance with DOE Order 5480.23. PRA's ability to (a) inherently handle both the likelihood and consequences of accidents, (b) automatically provide the dominant contributors to risk, (c) include human reliability and uncertainty considerations on overall safety, (d) analyze a range of accidents stemming from normal to beyond design basis events, and (e) produce a safety model to quickly analyze changes to the facility design or operations; resulted in the selection of PRA techniques for the accident analysis of CMR. For the CMR SAR, the PRA process and deterministic evaluations have been used to analyze both radiological and chemical risks for the facility. The accident analysis addresses both risks to the public as well as worker risks. Figure 1 illustrates the methodology that was used.

Step 1: The Walkthrough Questionnaire

A questionnaire was developed with which to record information required to perform the accident analysis. As the facility makes future changes, which is typical of the research nature of the CMR, the questionnaire provides a formal and consistent means for providing the input to an assessment of the safety impact of these changes.

The content of the questionnaire is such that the majority of the facility information required to perform the accident analysis is contained in a filled-out questionnaire. It should be noted that the questionnaire is designed to record information on a room-by-room basis if desired so that as a process changes in a given laboratory, the changes applicable to that location can be identified and subsequently analyzed using the risk model. This provides a *practical* means to address risk management by being able to identify specific corrective actions to mitigate specific hazards in particular locations of the CMR facility.

Step 2: Initiator Screening

A systematic search was conducted to identify possible events that could occur at the CMR facility that if not properly mitigated, could result in a hazardous release of radiological or chemical inventory. Such events are called accident initiating events, or for brevity, "initiators". This initiator screening step focused on identification of the events which could possibly lead to a release of radiological inventory from the CMR facility. This was done by constructing a logic model which was used to systematically identify the possible locations of radiological material and the possible release pathways of that material. While the model was constructed with the explicit intent of identifying release pathways to the public, the identified initiators in the model also apply to potential releases to the workers

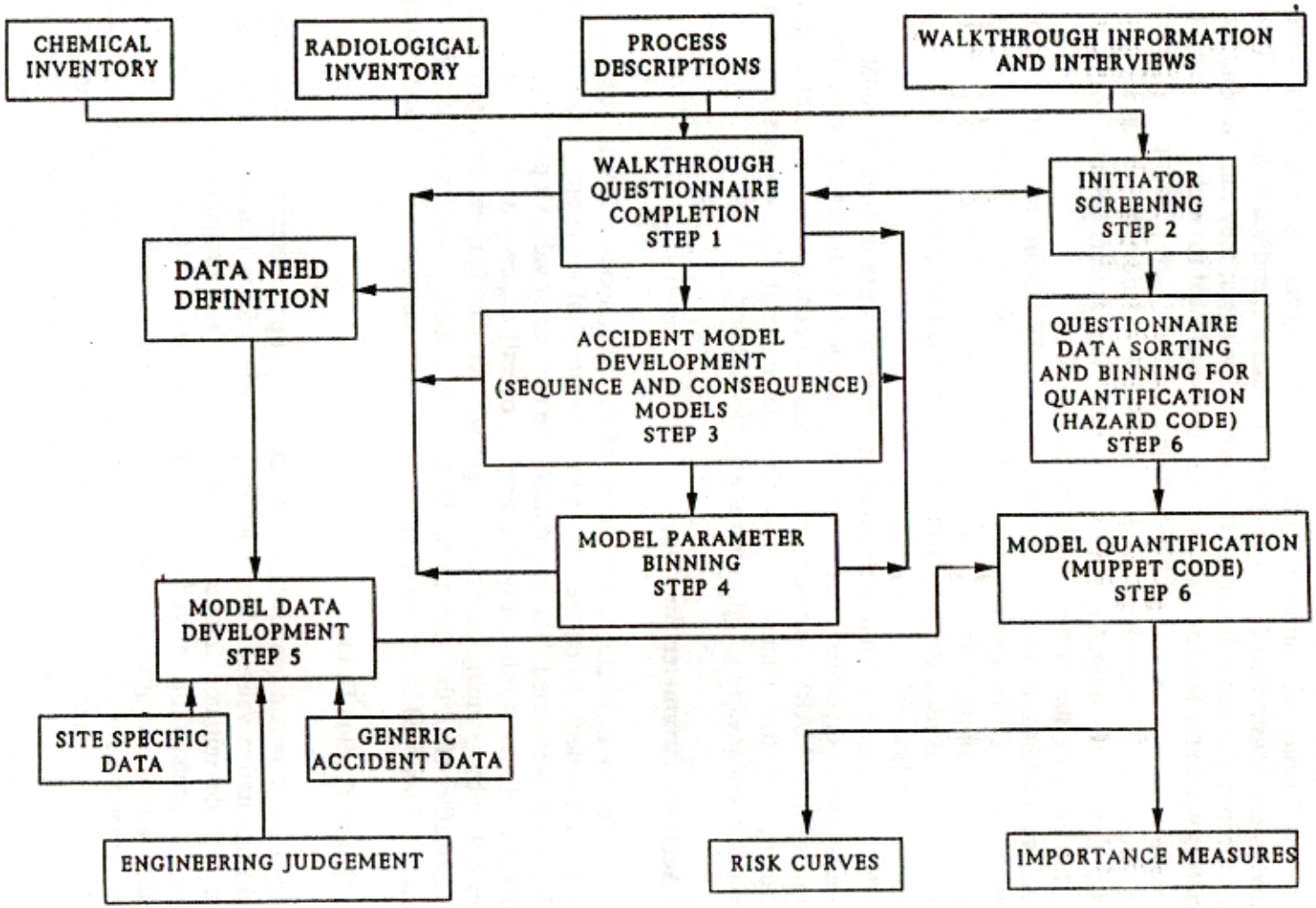


Figure 1. Major Steps and Types of Inputs Used in the CMR Building Accident Analysis

at CMR. Additionally, the insights and specific initiators from the results of this modeling activity were used to address possible chemical release initiators as well.

Step 3: Accident Model Development

The next step in the methodology is to model the possible sequences of events that could occur following each initiator defined in Step 2. This was done using event trees. Event trees were constructed for CMR for each initiator identified in Step 2. The series of trees collectively cover radiological and chemical releases; they can cover all locations and initiators within the facility since each tree is re-evaluated for each room in the facility and for each initiator associated with each room; and they address both public and worker risk. The tree structures are based on defining the combinations of successes and failures of the availabie CMR mitigating systems or operational aspects potentially important to defining the outcome should the initiator occur.

Active accident mitigating systems such as HVAC are made up of numerous components, each of which have historical failure probabilities. Therefore, in order to derive an overall failure probability for such a system, a different modeling technique, called a fault tree, is used to identify the ways (and the corresponding probabilities) that the system can fail.

The consequences from each accident sequence were defined in equation form. Important factors incorporated into the consequences equations include the type and amount of material of risk (MAR), the amount of respirable material that becomes airborne during the accident, and the amount of this airborne material that escapes the available confinement boundaries (e.g., gloveboxes and the building).

Step 4: Accident Parameter Binning

In order to facilitate quantification of the likelihood and consequences of the accident scenarios depicted on the event trees, "binning" of numerous parameters used in the analysis was performed. Binning reduces the number of values a particular parameter might assume without significantly affecting the overall accuracy of the results. Binning is accomplished by grouping parameter ranges with similar characteristics into "bins" that are representative of all the items placed in that "bin". Such a process reduces the amount of different values used in the entire model thus saving computation time and resources.

Step 5: Quantification Data

In order to obtain quantitative risk results, input parameters in the model had to be assigned quantitative values. Examples of parameters for which data values had to be assigned include initiator frequencies, equipment failure probabilities, human failure estimates, the probabilities of various phenomenological events such as the chance a fire will self-extinguish or grow, various leakpath factors, airborne release fractions and respirable fractions for all radiological MAR categories, and chemical property data.

Numerous sources were used to directly estimate or otherwise derive the necessary data values. These included CMR records, a LANL fire department database, various LANL event reports, other non-reactor nuclear facility analyses (e.g., Rocky Flats), commercial nuclear power plant equipment and human error data sources, studies of fire and seismic events, DOE guidance on material release rates and fractions, chemical property and compatibility information, hand and computerized deterministic calculations, and engineering judgment.

In most cases, estimates were made regarding the uncertainty in this input data so that the analysis results could properly reflect the lack of precision in most all of the

estimates. These uncertainties were typically characterized by assigning a mean (best estimate value), distribution shape, and 95% and 5% estimates (upper and lower bounds) based on statistical analysis of the data or sometimes expert judgment.

Step 6: Model Quantification

The various analytical and informational products of the previous steps are combined into an integrated risk model to obtain the accident analysis quantitative results. Two computer codes have been generated and combined into a PC-based risk management computer workstation to perform the above manipulations and calculations. These are the HAZARD code and the Multidimensional Uncertainty Propagation in Process Event Trees (MUPPET) code. In general, the HAZARD code performs the walkthrough information tabulation and manipulations, applies the binning rules and defines the binning assignments to the various parameters which are binned in the analysis, and calculates the chemical release portions of the accident analysis. MUPPET solves the sequences for their cut set expressions, applies the data values, performs the frequency and consequence calculations for the radiological release portions of the accident analysis, and is used to do the importance measure/sensitivity analyses as well as provide risk plots of the results.

FACILITY RISK OVERVIEW FROM INTERNAL INITIATORS

To illustrate the results available from the CMR risk model, preliminary public risk results from radiological releases for events that begin with an internal initiator (fires, explosions, overpressures, spills) are presented.

Figure 2 displays the overall radiological public risk curve for the CMR facility incorporating all internal accidents identified by the models for all wings/rooms within the facility and for all the internal initiators. The consequence measure for the risk curve is the 50 year committed effective dose equivalent (CEDE) for the maximum exposed public individual at a 1 kilometer boundary distance from the CMR site. When compared with the safety criteria it can be seen that over the full range of accident frequencies and consequences, the public risk from accidents at CMR is well below the criteria except near the 1E-06/year "credible" range for accidents.

In order to understand what is driving the risk curve presented above, a number of perspectives are presented to identify the dominant public risk contributors for CMR.

Relative Room Contributions

The risk is dominated by very few rooms within the facility. The most important room (and hence process) in the facility from a public risk perspective is Room 5121 where handling of Pu-238 is conducted. The risk from the activities in this room alone contributes approximately 85% of the total public risk for the facility. Two rooms, 3111 and 3135, are next most important contributing about 6% while all remaining rooms collectively contribute a total of about 9%.

Relative Initiator Contributions

Most of the CMR public risk is dominated by explosion accidents which contribute 91%. Next are overpressure which contribute about 6% followed by fires which contribute 3%. Radiological spills provide virtually no measurable risk to the public.

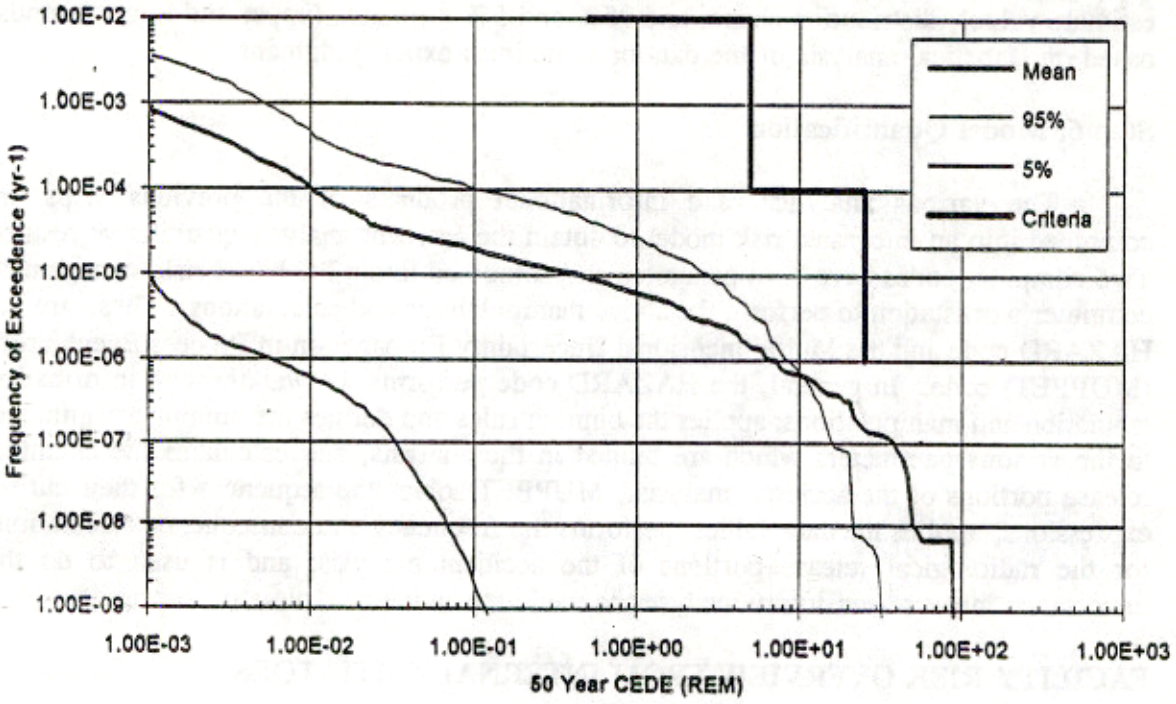


Figure 2. CMR Risk Profile for Full Facility

Relative Sequence Contributions

The CMR public risk is dominated by an accident which involves a flammable gas explosion as the initiating event with a subsequent fire, the building is breached as a result of the explosion, and the room sprinklers are successful at putting out the fire. A ground release is expected out the leakage pathways caused by the building breach. This sequence contributes 79% of the total public risk. The dominant fire scenario involves self-extinguishment and a limited release through the HVAC filters.

Mitigating System Importance

The most important mitigating system is the CMR Building itself. Explosion scenario rupturing the building boundary contributed to 80% of the public risk. Failure of facility fire suppression systems contributed to 17% of the risk while failure of manual fire suppression efforts by the fire department contributed to 12% of the risk. Failure or degradation of the HEPA filters in the HVAC system contributed to 4% of the public risk. Failure of the HVAC systems had a negligible impact (<1%) on risk.

CONCLUSIONS

The accident analysis conducted for the CMR Building provides a comprehensive assessment of the risk associated with the facility operation. The analysis results allowed for identification of the dominant accidents and provides valuable information to the facility operators to manage the risk. The facility models can be updated quickly in order to evaluate the risk from associated changes in the analytical procedures performed in the facility or due to facility modifications.

016 Uncertainty in Performance Assessment

Chair: M.G. Marietta, SNL

Uncertainties in Probabilistic and Non-Probabilistic Risk Assessment
K.E. Petersen (Riso Natl. Lab.)

Management/Technical Assessments on Yucca Mountain
C.P. Gertz (USDOE); S.R. Mattson (SAIC)

Risk Assessment of Coordinate Measuring Machine-Based Dimensional Inspection Technology
Y-L. Shen, X. Zhang (George Washington U.)

The Effect of Uncertainties in Dose-Response Data on Risk Management of Air Toxics
J.C. Huang, W.E. Kastenberg (UCLA)

UNCERTAINTIES IN PROBABILISTIC AND NON-PROBABILISTIC RISK ASSESSMENT

Kurt E. Petersen

Systems Analysis Department
Risø National Laboratory
DK-4000 Roskilde, Denmark

INTRODUCTION

The nuclear safety programmes of the Commission of the European Communities and the Nordic Council of Ministers both included investigations of uncertainties in safety assessment. Special attention was paid to human errors, CCF's and treatment of entire event sequences.

A specific analysis was carried out concerning uncertainty assessment at event sequence level taking into account the uncertainties related to the various element of the sequence. A probabilistic approach was used and to a large extent sensitive studies were recommended to supplement the uncertainty calculations.

In a recent initiative uncertainties related to, in particular, consequence assessment for non-nuclear installations are studied. The work is supported by the Commission of the European Communities under the name "Model Evaluation Group", which aim is to improve the quality of models developed and used in risk assessment and to provide users and developers with a protocol to be used in assessing the quality of a model. The background is the large number of models provided to users and the lack of consensus on the model quality aspects.

The main difference between the two initiatives is that within the nuclear field focus is on the estimation of the likelihood of occurrence of certain events given failure characteristics for the elements of the event sequence, while the consequences from toxic releases, fires and explosions are the important issues in risk assessments within the non-nuclear field. The likelihood of occurrence certainly plays a role, but it is very seldom assessed explicitly or the assessment is based on judgements.

The Model Evaluation Group has developed a first draft of a model evaluation protocol which is intended for users who wish to assess if a certain model is appropriate for use solving a given problem. The protocol includes the scientific aspects as well as the fitness-for-purpose aspects of a model. Further, guidelines are developed describing requirements to model developers to ensure a high quality of new models and in particular to assure a comprehensive and complete documentation comprising boundary conditions, assumptions, limitations and areas of applicability, which are lacking or are insufficiently documented for the majority of models used in risk assessment.

UNCERTAINTIES IN PROBABILISTIC SAFETY ASSESSMENT

Probabilistic safety assessment (PSA) which has proven to be an important tool for safety assessment within the nuclear society, has been the topic for research programmes financed by the Commission of the European Communities (CEC) and the Nordic Council of Ministers. As the basic approach they both used Benchmark exercises where independent analyses of a reference subject were carried out by different analysis teams. The exercises consisted of phases focusing on various important aspects of PSA:

- common cause failures
- human interactions
- event sequence assessment.

The CEC research programme was carried out in 1984-90[1,2,3] and Risø participated in all the Benchmark Exercises. One of the main results is that consensus has been established on the usefulness of the PSA approach, in particular on systems reliability modelling and CCF analysis. Analyzing human interactions was found much more complex and controversial, and no common consensus on procedures and assessment techniques was obtained.

In the Nordic research programme the same experience was gained in a number of Benchmark exercises[4]. Of particular interest was a reference study on sensitivity and uncertainty analysis[5]. One of the objectives was to demonstrate the impact of uncertainties, in particular these associated with the treatment of common cause failures and human interactions on the uncertainty of an investigated accident sequence.

The selected accident sequence consisted of a loss of feedwater transient, followed by a CCF in four motor-operated valves in the auxiliary feedwater system which causes a loss of the system. Finally, an operator fails to initiate a manual depressurization. This sequence is one important sequence in the PSA for a Swedish nuclear power plant.

Data for loss of feedwater were available from the plant. CCF's have been carefully studied based on failure reports from motor-operated valves. Human interactions were studied using the available human reliability techniques. Based on this set of characteristics uncertainty and sensitivity analyses were carried out to assess the importance of the uncertainties associated with each element of the sequence on the overall uncertainty.

Firstly, we found that the uncertainty at the sequence level was three order of magnitude. Secondly, we found, not surprisingly, that the largest contributor to the sequence uncertainty is the uncertainty associated with the human interaction. In particular, a sensitivity analysis was performed assuming no uncertainty associated with one of three elements in turn. The sensitivity analysis showed that the mean values did not change very much, while the uncertainty intervals diminished substantially, especially when uncertainties associated with the human interaction were eliminated.

The Benchmark exercises were all limited to level 1 PSA's focusing on estimation of the likelihood of occurrence of certain events given failure characteristics for the components in a system.

UNCERTAINTIES IN MAJOR HAZARDS ANALYSIS

In the period 1988-90 the CEC initiated a Benchmark exercise on major hazard analysis for a chemical plant[6,7]. The results showed that some of the findings from the nuclear Benchmark exercises were valid also for non-nuclear installations, i.e. difficulties arising from the scarceness of reliability data, inappropriate CCF models and data and lack of knowledge and suitable approaches for analysis of human interactions. Further, it was found that the modelling of the physical phenomena and the selection and use of an analysis tool have a very strong impact on the result.

The aspects of model deficiencies and the selection of boundary conditions have been further studied by Hanna[8] and Britter[9]. The latter study was aimed at evaluation of technical models used for major-accident hazard installations. The study was limited to technical models mainly used for consequence assessment and did not consider hazard identification techniques, probability assignment techniques, behavioural models or management models.

The conclusions were that there is little formalized evaluation of the quality of the models and there is a need by users for a more structured evaluation of the quality of models.

MODEL EVALUATION GROUP

In 1993 the CEC decided to establish a Model Evaluation Group (MEG) with the objective to improve the culture in which models are developed and used and to ensure that the models used in major hazards assessment are up-to-date with technical developments and utilized by personnel well-versed in their applicability and functioning.

The members of MEG are:

R. Britter, Cambridge University, United Kingdom
T. Cartage, SOLVAY, Belgium
S.J. Jones, AEA Technology Consultancy Services (SRD), United Kingdom
M. Schatzmann, University of Hamburg, Germany
B. Stork, TNO, The Netherlands
K.E. Petersen, Risø, Denmark (chairman)

The intention is to develop guidelines for model developers and a protocol for model evaluation of any model used in major hazards assessment. This means that the guidelines and the protocol should be applicable for any model used in any part of an accident scenario, as shown in table 1.

The tasks MEG is carrying out consist of:

- Classification of available models in major industrial hazards
- Development of a general evaluation protocol for evaluation of technical models in major industrial hazards
- Development of guidelines for model developers
- Initiation of working groups for selected classes of models
- Survey of models within the subject area of working groups
- Specification of lacking data/model deficiencies within the subject area of working groups
- Identification of research needs
- Preparation of a European seminar to present the results.

The evaluation protocol and the guidelines for model developers in a draft form have been send out for a preliminary review and will be updated and issued by the end of the year.

The next step is to establish working groups on the scientific areas indicated in table 1, starting with dense gas dispersion and pool fires. Their task is to adjust the protocol and the guidelines to fit to the specific conditions and requirements of each scientific area. Further, they will set up a list of available models and data sets in their area. Finally, they will establish the conditions and procedures for a model evaluation where model developers and users are invited to evaluate the models using the evaluation protocol and a data set selected for that purpose. The idea is to invite users and researchers to a thorough review procedure to allow for a balanced evaluation and subsequently to arrive at a consensus on models, their advantages, limitation and applicability.

TABLE 1. Model types in an accident scenario

	models	submodels
Failure/disturbance	- equipment - operator (human) - management	
System response	- chemical - physical	
Direct effect	- release/source term - explosion	
Consequence	- fire	- fire escalation - toxic fumes
	- subsequent explosion	- confined - unconfined - missiles
	- structural impact	
Dispersion	- air - water - soil	- dense
Effects	- environmental impact	- immediate - ecosystem damage
	- health effects	- immediate - long term effects
Frequency		

CONCLUSIONS

Safety assessment of complex industrial installations has become more and more important as industry, authorities and society at large set up requirements for higher reliability and safety of plants. The safety assessments are based on extensive use of models which have never been through a procedure of evaluation. Research has shown that uncertainties are associated with models and their use. They originate from the selection of a model, its boundary conditions, assumptions and limitations and further from data uncertainties.

In the nuclear field PSA's are extensively used with its focus on estimation of the likelihood of severe accidents. The major contributions to the uncertainty are associated with CCF's and human interactions. In the non-nuclear field like the petro-chemical or chemical area, much more emphasis is put on the technical models and their uncertainties, even though human interactions certainly are of importance here as well.

REFERENCES

1. A. Poucet and A. Amendola, State of the art in PSA reliability modelling as resulting from the international benchmark exercise projects, NUCSAFE'88 Conference, Avignon, France, 1988.
2. A. Poucet, A. Amendola and C. Cacciabue, Common Cause Failure reliability benchmark exercise, EUR 11054, CEC-JRC, Ispra, 1987.
3. A Poucet, Human factors reliability benchmark exercise, EUR 12222, CEC-JRC, Ispra, 1989.
4. S. Hirschberg, "Dependencies, human interactions and uncertainties in probabilistic safety assessment", NORD, 1990.
5. K.E. Petersen and H.E. Kongsø, Reference study on sensitivity and uncertainty analysis, Risø-report RAS-470(89)7, 1989.
6. S. Contini, A. Amendola and I. Ziomas, Benchmark exercise on major hazards analysis, Vol. 1, EUR 13386EN, 1991.
7. A. Amendola, S. Contini and I. Ziomas, Uncertainties in chemical risk assessment: Results of a European benchmark exercise, J. of Haz. Mat., 29:347(1992).
8. S.R. Hanna, D.G. Strimaitis and J.C. Chang, Evaluation of 14 hazardous gas models with ammonia and hydrogen fluoride field data, J. of Haz. Mat., 26:127(1991).
9. R.E. Britter, The evaluation of technical models used for major-accident hazard installations, EUR 14774EN, 1993.

MANAGEMENT/TECHNICAL ASSESSMENTS ON YUCCA MOUNTAIN

Carl P. Gertz[1] and Steven R. Mattson[2]

[1]U. S. Department of Energy
Yucca Mountain Site Characterization Project
P.O. Box 98608
Las Vegas, NV 89102

[2] Science Applications
International Corporation
101 Convention Ctr. Dr.
Las Vegas, NV 89193

INTRODUCTION

This paper covers the status of the Yucca Mountain Project (YMP) efforts to characterize and evaluate an underground geologic repository for the potential storage of high-level nuclear waste. The Yucca Mountain site is located, in a small portion of the Mohave Desert within Nye County, Nevada, 160 kilometers NW of Las Vegas and is being evaluated through many geologic studies including: drilling, trenching, and the initial phases of a underground Exploratory Studies Facility (ESF). The paper also focuses on the appropriate use of geotechnical and engineering information in evaluations of compliance with the regulatory criteria, thereby keeping the risks within prescribed limits. An application for licensing a geologic repository will require predictions of ground-water travel times for both 1,000 and 10,000 years and an engineered barrier system (including waste package) that meets time-related regulatory criteria for waste containment and isolation. Ultimately, all of this information and the associated uncertainties will be used to gage the risk to the public health and safety. The appropriate use of geotechnical and engineering information in evaluations of compliance with criteria covering such time frames presents an unprecedented challenge to geoscientists and engineers because the links between measurable site data, subsequent models/evaluations, and demonstrations of compliance with the regulatory criteria promulgated by the responsible federal agencies are often complex and controversial.

BACKGROUND

Currently, in 1993, more than 20,000-30,000 metric tons of civilian high-level nuclear waste (spent fuel) are being stored in approximately 65 temporary above-ground sites at nuclear power plants across the continental United States. Although many alternatives for the disposal of high-level nuclear waste have been proposed, the Congress of the United States currently mandates emplacement in an underground mined geologic repository which has the capacity to store at least 70,000 metric tons of waste.

Three federal agencies are mainly involved in the repository program and the implementation of the Nuclear Waste Policy Act (NWPA, 1983). Table 1 contains a brief description of the regulations. The Environmental Protection Agency (EPA) is responsible for setting standards for protection of the general environment and public from off-site

releases of radioactive material (EPA, 1985). The Nuclear Regulatory Commission (NRC) is responsible for preparing regulations and for approving or rejecting license applications 1) to construct repositories, 2) to receive and possess high-level radioactive wastes, and 3) to close and decommission repositories (NRC, 1983). The Department of Energy (DOE) is responsible for screening, recommending, characterizing, and preparing license applications for potential sites and is responsible for managing licensed sites under construction, operation, or decommissioning. At the end of or during site characterization the DOE may determine, based upon the site data collected, that the site is unsuitable and recommend to Congress and the President that another site be characterized. If the site is found to be suitable, then the DOE will submit a license application to the NRC. If the license application is approved then construction of a repository can begin; another license would need to be granted to operate the facility for the storing of waste.

Table 1 Repository-specific Federal regulations[1]

Agency or Department	Title and Part	Purpose
EPA	40 CFR Part 191	10,000-yr release limits for repository system: ground water and individual protection requirements
NRC	10 CFR Part 60	System and subsystem performance requirements for natural and engineered barriers: siting and design criteria for repository and waste package
DOE	10 CFR Part 960	General siting guidelines for recommendation of sites for repositories

1 Note: The repository program must also comply with other federal, state, and local regulations, such as the National Environmental Policy Act of 1969 (EPA, 1969). Table after Blanchard et al. (1991).

In 1987 the 100th U.S. Congress passed the Nuclear Waste Policy Amendments Act (NWPAA, 1987), which narrowed and modified the scope of the Nuclear Waste Policy Act (NWPA, 1983). The 1987 amendment reduced the number of sites to be investigated from three sites to one site; and mandated that the initial repository siting efforts be directed toward evaluating the suitability of a single site, Yucca Mountain.

The preliminary investigations at Yucca Mountain started in the late 1970s when many sites across the United States were under investigation to determine potential locations for characterization. Activities began to ramp up in approximately 1984 and led to an Environmental Assessment (DOE, 1986) and a Site Characterization Plan (DOE, 1988) being completed. Site characterization that is directed toward evaluating the suitability of the site has started during the last few years. Total program costs are projected to be 6.3 billion dollars at the time of possible license application in the year 2001.

GENERAL GEOLOGIC SETTING AND CURRENT STATUS OF SITE CHARACTERIZATION STUDIES

The Yucca Mountain site is located in a volcanic terrain with complex stratigraphy of 11-14 m.y. ash-flow tuffs. The potential repository horizon is located approximately 300 meters below the surface and at least 180 meters above the water table. Although located in the unsaturated zone, moisture passing through the tuffs is, perhaps, of tantamount importance because this water is the most likely transport medium for radionuclides that have escaped a deteriorated waste package and engineered barrier system, and begun to react and move in the natural environment. Other important investigations include studies of the general rock properties, climate, geologic structure, and the potential for rare or unexpected events such as volcanic eruptions, large flooding events, or significant climatic changes.

Site characterization achievements and advances at the site in 1992-1993 include the start of excavation for the Exploratory Studies Facility (ESF) in November 1992. An ESF is required by NWPA (NWPA, 1983) during site characterization. The ESF is planned to be an 8 kilometer system of underground tunnels and alcoves used to collect geologic and engineering information from rock above, in, and possibly below the proposed emplacement horizon. Other new work has included drilling of approximately 3,000 ft in five different boreholes (hydrologic, geologic, and rock property studies), and the drilling of 23 neutron access boreholes (water infiltration studies). These activities have addressed issues related to the excavation of the ESF, soil and rock properties for design planning, Quaternary fault studies, environmental activities, evaluation of the potential for future volcanism, modeling activities of site performance, and many other studies. All of these activities address a main question: Can Yucca Mountain safely isolate high-level nuclear waste through the use of geologic and engineered barriers for 10,000 years? The DOE currently plans to use expert judgement and a risk-based approach to provide interim evaluations of the the suitability during site characterization (e.g., Younker et al., 1992a, 1992b) and for any license application that may be prepared.

REDUCING UNCERTAINTY AND RISK THROUGH SITE CHARACTERIZATION

An important objective of the YMP during site characterization is the acquisition and appropriate use of geotechnical and engineering information in the evaluations of compliance with the regulatory criteria. The manner by which an improved data base of site information, obtained through site characterization, enhances confidence in repository performance is complex. Predictions of performance of a combined engineered and natural system over long time periods involve use of quantitative analyses coupled with formal expert judgment (Blanchard et al., 1991). Uncertainty in the repository program can be viewed as geologic uncertainty and regulatory uncertainty.

Geologic uncertainty is defined as the uncertainty in the determination of existing natural site conditions and the processes that can act to change them. The determination of "reasonable assurance" about protection of public health and safety over the 10,000 year period of regulatory concern can be viewed as regulatory uncertainty. The uncertainties are related, as the degree of confidence about site conditions and processes (geologic uncertainty) will certainly influence the perception of reasonable assurance.

The goals of site characterization that focus on the reduction of geologic uncertainty include: 1) better knowledge of the ranges, spatial distribution, and heterogeneities of hydrologic, mineralogic, and rock properties, 2) increased confidence in geologic and hydrologic models, and 3) improved understanding of the geologic and hydrologic processes that could change current conditions.

These investigations will lead to an improved three-dimensional data base for modeling radionuclide transport and an increased confidence in both the probabilities and possible consequences of disruptive events.

Several approaches to reducing regulatory and scientific uncertainty are being applied and include the following (e.g., Blanchard et al., 1991): 1) developing a clear understanding and link between the site conditions and processes and the performance of the engineered and natural barriers that can be relied upon for containing and retarding the movement of radionuclides, 2) involving the broad technical community to reach consensus on the expected-case site models and processes and bounds and ranges, 3) identification and understanding of sources of uncertainty and where new data can be used to test the bounds of repository performance and aid in gaining reasonable assurance, and 4) identification of testing strategies and priorities that maximize the likelihood of resolving uncertainties in the regulatory and technical arena.

The uncertainty in the regulatory environment comes from many sources and includes differing interpretations among and between agency staff, regulatory agencies, and external oversight groups, such as, the Advisory Committee on Nuclear Waste or the Nuclear Waste Technical Review Board (Blanchard et al., 1991). Changes in the regulatory criteria can also lead to uncertainties, for example, the EPA regulation 40 CFR Part 191 is under revision and the current probabilistic standard may change to an individual dose standard. In addition, regulatory uncertainty can be derived from a loss of staff responsible for the preparation of regulations or technical positions developed and based on site data. All of these factors can

change the view of the licensee (DOE) who must consider the level of uncertainty that is acceptable to proceed with a license application and the view of the agency responsible for granting a license (NRC) who must consider the level of uncertainty about containment and waste isolation that provides reasonable assurance of the public health and safety.

Some level of uncertainty is inherent in predictions of radionuclide releases, particularly, for the long-term models of releases that will be required for the repository program. This uncertainty will be difficult to quantify and reliance on formally elicited expert judgement is the only way that final conclusions about the safety of a geologic repository can be reached. Systematic techniques involving the rigorous use of expert judgment and risk assessment are being investigated (e.g., Bonano et al., 1990; Mattson et al., 1991; Younker et al., 1992a, 1992b; Barnard et al., 1992; Eslinger et al., 1993; Judd et al., 1993) and incorporated by the DOE.

CURRENT USES OF EXPERT JUDGEMENT AND RISK ASSESSMENT

Expert judgement and decision analysis have been used in the past on the Yucca Mountain Project to aid in making decisions about ESF design, prioritizing the testing program (site characterization), the total system performance of the Yucca Mountain site, and a preliminary assessment of the suitability of the Yucca Mountain site. Each of these efforts has differed in the level of detail and in the focus of the effort, but all have incorporated some form of elicitation of expert judgements which is used to perform simple to sophisticated model calculations.

The Test Prioritization Task (TPT) (Mattson et al., 1991) and the ongoing Integrated Test Evaluation (ITE) (Judd et al., 1993) both aid the DOE in making decisions about which studies are the most important to conduct based on a set of evaluation criteria. The TPT effort was predominantly based on the criterion of detecting site unsuitability and was based on the DOE regulation 10 CFR Part 960 and the site disqualifying conditions contained therein. The current ITE effort has attempted to incorporate many of the other reasons for conducting site studies (Figure 1) including the detection of site unsuitability, meeting the performance criteria in the NRC regulation 10 CFR Part 60 or demonstrating regulatory compliance, the ability of a study to build scientific confidence in the scientific community or the the many oversight boards, studies whose results could lead to a significant design change, and lastly, the cost of conducting a study. In general, the results of these analyses indicate that studies that can increase knowledge about the hydrologic environment, the likelihood of faulting near the facilities, and the likelihood of volcanic eruption are the highest ranked tests. However, the dominant criteria in the analysis was the achievement of scientific confidence. If scientific confidence is eliminated, then only the hydrologic studies rank

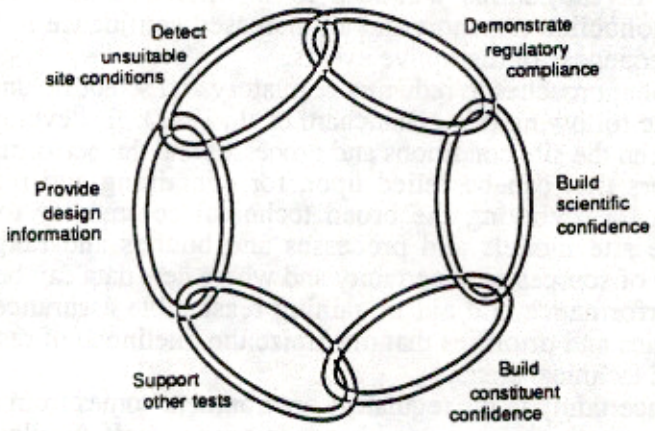


Figure 1. Six interrelated reasons for testing. Building constituent confidence has not been explicitly evaluated in the studies described, but is a major concern of the Project. The four other reasons for testing have been explicitly evaluated and the fifth (provide design information) is currently being added to the decision framework in the ITE. After Judd et al. (1993).

highly and by 1/5th the magnitude lower. In the future other reasons for testing could be incorporated into the model.

The Early Site Suitability Evaluation (ESSE) performed a preliminary assessment of the suitability of the Yucca Mountain site (Younker et al., 1992a) based upon the DOE 10 CFR Part 960 regulation including the criteria contained in the disqualifying conditions and the qualifying conditions. The assessment was done to support a decision of whether to continue with site characterization of the Yucca Mountain site or abandon the site and begin to characterize a different site. These criteria cover a wide gamut of geologic conditions, the total system performance of the site in relation to the site's waste isolation and containment capabilities, and the ability to protect the public health and safety. Within 10 CFR Part 960 four different types of findings are allowed for each of the criteria and paraphrases of these possible findings are presented here: compiled evidence indicates that the site 1) should be disqualified, 2) is likely to be disqualified, 3) is likely to be qualified, and 4) is qualified based on assessment of the qualifying condition (and disqualifying condition)

Based upon current information and expert judgement the ESSE recommended that in respect to 8 of the 24 criteria the site is "qualified" and for the remaining 16 criteria, the site is likely to be qualified. No conditions (criteria) were judged to fall within categories 1 and 2, above. A peer review panel of experts external to the Project was assembled and reviewed the findings and information compiled by the internal experts (Younker et al., 1992b). Continued site characterization was recommended by both groups. Areas in which little or no further testing was needed in order to qualify the site included the geologic concerns of extreme erosion and rock dissolution, and the non-geologic concerns of site ownership and control. Areas where additional site data would be required to support a decision on the qualification of the site included total system performance, geohydrology, rock conditions, climatic conditions, environmental quality, and socioeconomic impacts.

In the last several years two other efforts have been completed and include the Calico Hills Risk-Benefit Analysis (CHRBA) (DOE, 1991) and the Exploratory Studies Facility Alternatives study (ESFA) (Dennis, 1991). The CHRBA was mainly initiated for the purposes of assessing the risk of compromising or disturbing the effectiveness of a rock layers (Calico Hills Unit) ability to isolate waste and provide containment by site characterization (e.g., drilling, ESF construction, ESF tests). The CHRBA used expert judgement in the risk/decision analysis and concluded that all ESF design options were not likely to compromise the site. The CHRBA study did recommend two ESF design options and these were considered by the ESFA study. The ESFA, based on expert judgement and risk/decision analysis technics, was a study that ranked ESF design alternatives against a set of criteria including ease of construction, ability to provide testing sites early, not creating new water pathways that could interact with the waste, and being compatible with a repository if it was built. As reported earlier, the ESF is presently under construction.

Finally, total system performance evaluations of the Yucca Mountain site have been performed to evaluate the sensitivity of different scenarios of repository performance against the probabilistic based EPA radionuclide release limits. Recently, these efforts have included the elicitation of expert judgements on the range of a particular parameter for insertion in repository models and includes the work of Barnard et al. (1992) and Eslinger et al. (1993) and similar work by agencies external to the Yucca Mountain Project including the work of the Electric Power Research Institute (EPRI, 1993a; 1993b).

FUTURE USES OF EXPERT JUDGEMENT AND RISK ASSESSMENT

The Yucca Mountain site characterization is currently planned to be finished in the year 2001. As site characterization continues on the Yucca Mountain site many additional roles for the use of decision analysis, risk assessment, and expert judgement will be defined and utilized in the decisions on whether the site is suitable for repository location, in the prioritization of the testing in the site characterization program, in the calculations involved in performance assessment and technical licensing positions, and likely in the license application to be filed with the NRC for the potential construction of the underground repository. Other roles for this type of defensible, rigorous, and quantifiable analysis will likely be found in the site characterization process.

REFERENCES

Barnard, R. W., Wilson, M. L., Dockery, H. A., Gauthier, J. H., Kaplan, P. G. Eaton, R. R., Bingham, F. W., Robey, T. H., 1992, TSPA 1991: An Initial Total- System Performance Assessment for Yucca Mountain, Sandia National Lab., Sand91-2795/UC-814, Albuquerque, NM.

Blanchard, M. B., Dobson, D. C., Voegele, M. D., and Younker, J. L., 1991, Licensing a geologic repository: types of uncertainties, Environ. Geol. Water Sci., V. 18, No. 3, pp 215-220.

Bonano, E. J., Hora, S. C., Keeney, R. L., and von Winterfeldt, D., 1990, Elicitation and use of expert judgment in performance assessment for a high-level radioactive waste repository: SAND89-1821, NUREG/CR-5411, Sandia National Lab., Albuquerque, NM.

Dennis, A. W., (ed), 1991, Exploratory Studies Facility Alternatives Study: Final Report, SAND91-0025, 2 Vols., Sandia National Lab., Albuquerque, NM.

DOE (U. S. Department of Energy), 1986, Environmental Assessment, Yucca Mountain Site, Nevada Research and Development Area, Nevada, DOE/RW-0073, 3 Vols., Office of Civilian Radioactive Waste Managment, Washington, D. C.

DOE (U. S. Department of Energy), 1988, Site Characterization Plan, Yucca Mountain Site, Nevada Research and Development Area, Nevada, DOE/RW-0160, 9 Vols., Office of Civilian Radioactive Waste Managment, Washington, D. C.

DOE (U. S. Department of Energy), 1991, Risk/Benefit Analysis of Alternative Strategies for Characterizing the Calico Hills Unit at Yucca Mountain, Record Memorandum YMP/90-3, 2 Vols., Yucca Mountain Project Office, Las Vegas, NV.

Eslinger, P. W., Doremus, L. A., Engel, D. W., Miley, T. B., Murphy, M. T., Nichols, W. E., White, M. D. Langford, D. W., Ouderkirk, S. J., 1993, Preliminary Total-system Analysis of a Potential High-Level Nuclear Waste Repository at Yucca Mountain, Pacific Northwest Lab., PNL-8444/UC 814, Richland, WA.

Judd, B. R., Hoxie, D. T., Mattson, S. R., and Younker, J. L., 1993, Integrated test evaluation decision framework for the Yucca Mountain Project, Proceedings of the Fourth Annual International Conference on High Level Radioactive Waste Management, American Nuclear Society, April 26-30, Las Vegas, NV, pp. 1623-1632.

Mattson, S. R., Judd, B. R. , Sinnock, S. R., and Hoxie, D. T., 1991, Testing Priorities at Yucca Mountain: Recommended Early Tests to Detect Potentially Unsuitable Conditions for a Nuclear Waste Repository: Report of the Test Prioritization Task Force, Vols. I and II, U.S. Department of Energy-Yucca Mountain Site Characterization Project,YMP/91-25, Las Vegas, NV.

NRC (U. S. Nuclear Regulatory Agency), 1983, Disposal of High-level Radioactive Waste in Geologic Repositories, Technical Criteria, Federal Register, V. 48, p. 28194, U. S. Government Printing Office, Washington, D. C.

NWPAA (Nuclear Waste Policy Amendments Act), 1987, Nuclear Waste Policy Act of 1987, Title V, Subtitle A to the Omnibus Budget Reconciliation Act of 1987, U. S. Congress, Washington, D.C.

NWPA (Nuclear Waste Policy Act), 1983, Nuclear Waste Policy Act of 1982, Public Law 97-425, U.S. Congress, Washington, D.C.

EPA (U. S. Environmental Protection Agency), 1969, National Environmental Policy Act of 1969, Public Law-91-190, U. S. Congress, Washington, D. C.

EPA (U. S. Environmental Protection Agency), 1985, Environmental Standards for the Management and Disposal of Spent Nuclear Fuel, High-level and Transuranic Radioactive Wastes, Federal Register, V. 50, No. 182, p. 38066, U. S. Government Printing Office, Washington, D. C.

EPRI, 1993a, Proceedings: EPRI Workshop 2-Technical Basis for EPA HLW Disposal Criteria, Electric Power Research Institute, TR-101257, Palo Alto, CA.

EPRI, 1993b, Proceedings: EPRI Workshop 1-Technical Basis for EPA HLW Disposal Criteria, Electric Power Research Institute, TR-100347, Palo Alto, CA.

Younker, J. L., Andrews, W. B., Fasano, G. A., Herrington, C. C., Mattson, S. R., Murray, R. C., Ballou, L. B., Revelli, M. A., Ducharme, A. R., Shepard, L. E., Dudley, W. W., Hoxie, D. T., Herbst, R. J., 1992a, Early Site Suitability Evaluation, Yucca Mountain, NV, SAIC-91/8000, Science Applications International Corp., Las Vegas, NV.

Younker, J. L., Andrews, W. B., Fasano, G. A., Herrington, C. C., Mattson, S. R., Murray, R. C., Ballou, L. B., Revelli, M. A., Ducharme, A. R., Shepard, L. E., Dudley, W. W., Hoxie, D. T., Herbst, R. J., 1992b, Report of the Peer Review Panel on the Early Site Suitability Evaluation, Yucca Mountain, NV, SAIC-91/8001, Science Applications International Corp., Las Vegas, NV.

RISK ASSESSMENT OF COORDINATE MEASURING MACHINE-BASED DIMENSIONAL INSPECTION TECHNOLOGY

Yin-Lin Shen, and Xianping Zhang

Department of Civil, Mechanical, and Environmental Engineering
The George Washington University
Washington, DC 20052

INTRODUCTION

Dimensional inspection is a process for ensuring the dimensional correctness of manufactured parts by comparing the inspection results with the specified dimensions and tolerances of the parts. Toleranced dimensions are a critical attribute of the more than $500B worth of discrete-part products produced in the United States each year (Swyt, 1992). Dimensional inspection of discrete product is important because dimensions and tolerances of the products play an important role on product functional performance and costs. Coordinate measuring machine (CMM) is an emerging flexible dimensional inspection technology in modern manufacturing systems (Bosch, 1992; Schreiber, 1990), and is accepted by industry. CMMs are commonly used in aerospace and automotive industry because they provide fast and accurate dimensional inspection. The advantages of CMM-based dimensional inspection over traditional gaging techniques are greater flexibility, reduced setup time, improved accuracy, and improved productivity. The inspection results from the CMM-based dimensional inspection are used to make decisions as to accept or reject the part, or to ascertain if the manufacturing process is stable. One important aspect in dimensional inspection is the control of risk. Since it is usually not economical to eliminate measurement uncertainty completely in dimensional inspection applications, the decision making is in fact risk-based. It is necessary to reduce both pass error, which is passing a part which is out of tolerance, and fail errors, which is failing a part which is within tolerance.

The basic idea of CMM-based dimensional inspection is that a probe (usually a tough-trigger probe), mounted onto the ram of the inspection machine structure, is used to measure the coordinates of points on part surfaces. The measurement data is thus collected and then processed by post-inspection data analysis algorithms in order to extract geometric feature parameters that best represent the actual part dimensions and tolerances. The measurement results (fitted parameters) are then used for making dimensional inspection decisions. It is a sample-based approach, that is, coordinate measurements are "samples" from part surfaces and are processed to obtain measured results, which are used to determine part quality. In order to assess the risks in such processes, the following factors need to be considered.

Sampling Strategy. The issues are how many points to measure on a specified part surface, and the spatial distribution of these points. It is impossible, technically and economically, to measure all points on part surfaces in CMM-based dimensional inspection. For a 2-D (two-dimensional) circle, three or more points may be taken in determining the center and the radius (or diameter) of the circle. As for spatial distribution for simple cases

such as a 2-D circle, usually equally-spaced sampling is used. For complicated geometric features, special care is needed to spread the measurement points.

Measurement Uncertainties. There are uncertainties in the measurement data (Phillips, 1993). Factors contributing to measurement uncertainties include probe repeatability, pre-travel variations, axis hysteresis and geometric errors of the machine, probe approach angle and speed, etc. These factors are interrelated and need to be considered in assessing inspection risks.

Data Analysis Algorithms. Post-inspection data analysis software is typically proprietary software provided by CMM manufacturers. Issues related to errors results from algorithms include fitting algorithms selection and calculational approximations in implementing the selected algorithms. The least-squares method is the most commonly used method in post-inspection data analysis. The impact of the algorithms used on inspection results and the subsequent inspection decisions also needs to be considered.

In this paper, a risk assessment method for CMM-based dimensional inspection is presented. The Monte Carlo simulation method is used to reveal the uncertainty propagation effects in data-analysis fitting, and a model of calculating the risk probability based on the Monte Carlo simulation results and the part tolerance is described. An example illustrating the application of the method is also included.

RISK ASSESSMENT METHOD

In this paper, simulation based on the Monte Carlo method and an analytical method based on the error analysis theory are used to assess the risks.

Least-Squares Method

The least-squares method is the most commonly used data-analysis algorithm. The fitting algorithm is to minimize the sum of squares of the deviations of the measurement data from the mathematical expression of the ideal geometry of the feature (Caskey et al., 1991). While the cost function to be minimized may be a nonlinear function of the feature parameters, numerical search methods, such as conjugate gradient method or the steepest descent method, are used to find the best fit in finding the set of parameters associated with the feature being inspected.

Monte Carlo simulation

The Monte Carlo method is used to evaluate the uncertainties of the fitted parameters, which result from the uncertainties in the measurement data. The method can be summarized as follows:

Step 1. For a particular geometric feature, choose an appropriate fitting algorithm.

Step 2. Given the uncertainty range or the standard deviation of data points, generate a new set of data points by adding a randomly generated uncertainty component to each coordinate of the measurement data. So a set of simulated measurement data is generated.

Step 3. Use the simulated measurement data set to calculate a simulated geometric feature using the algorithms selected in Step 1. A set of measured result data will be obtained.

Step 4. Repeat step 2 and step 3 until a pre-determined number of simulations are performed. For each simulation, the simulated geometric feature parameters are stored in a "simulation-result file."

Step 5. Calculate simulated result distribution characteristics, such as mean value and standard deviation, for each simulated result data set.

Using this approach, uncertainty characteristics of the measured results can be obtained, which can be used in the analytical method described in the following sub-section.

Risk Probability Analysis Method

Given a dimensional tolerance specification on a feature, let the feature be denoted as D. Let D_l and D_u present the lower bound and the upper bound of the feature D, and let D_m be the fitted feature parameter. The inspection decision is made based on if Dm falls between D_l and D_u. That is, the part is accepted if D_m is between D_l and D_u (within tolerance), and the part is rejected if D_m is smaller than D_l or D_m is larger than D_u. Furthermore, risks in committing pass error and fail error can be evaluated based on information regarding the values of D_m, D_l, and D_u, and the distribution characteristics of D_m resulting from measurement data uncertainties. Assuming that the probability distribution function of the feature can be obtained from the Monte Carlo simulation, the probability of accepting a bad part, $Pr_{pass\ error}$, can be expressed as:

$$Pr_{pass\ error} = 1 - \int_{D_l}^{D_u} f(D)\, dD \tag{1}$$

where f(D) is the probability density function of the geometric feature D, and the probability of rejecting a good part, $Pr_{fail\ error}$, can be expressed as:

$$Pr_{fail\ error} = \int_{D_l}^{\infty} f(D)\, dD \tag{2}$$

when $D_m \leq D_l$, and $Pr_{pass\ error}$ can be expressed as:

$$Pr_{fail\ error} = \int_{-\infty}^{D_u} f(D)\, dD \tag{3}$$

if $D_m \geq D_u$. It is assumed that sufficient information about the uncertainty distribution can be obtained from Monte Carlo simulation.

EXAMPLE

A 2-D circle fitting example is presented in this section in order to illustrate the application of the risk assessment method. The radius of an ideal circle is 100 mm, and its location is at origin (0,0) in the inspection machine coordinate system. Three sampling schemes are used, and they are (1) three points, equally distributed on the circle, (2) five points, equally distributed on the circle, and (3) seven points, equally distributed on the circle. While the possible uncertainty ranges in the measurement point (xi, yi) are assumed to be 0.02 mm, 0.05 mm, and 0.005 mm. The three different uncertainty ranges represent three different machines. The measurement uncertainty range represents the accuracy of the machine.

A 2-D circle fitting software based on the least-squares method is developed and used to generate the uncertainty patterns for the radius and the circle center. Each case is simulated one thousand times. In each simulation, an uncertainty value from a uniform distribution is generated and added to each measurement component (xi and yi) in the fitting. The reason of choosing the uniform distribution is due to the performance characteristics of CMMs. The simulation results indicate that the distribution of the fitted parameter

uncertainty patterns seem follow the normal distribution. Figure 1 shows the simulation results of the x coordinate of the circle center for a three-point sampling scheme, and the uncertainty range is 0.005 mm. Since the radius is the main concern in this example, the following discussion is focused on the uncertainty pattern of the fitted radius.

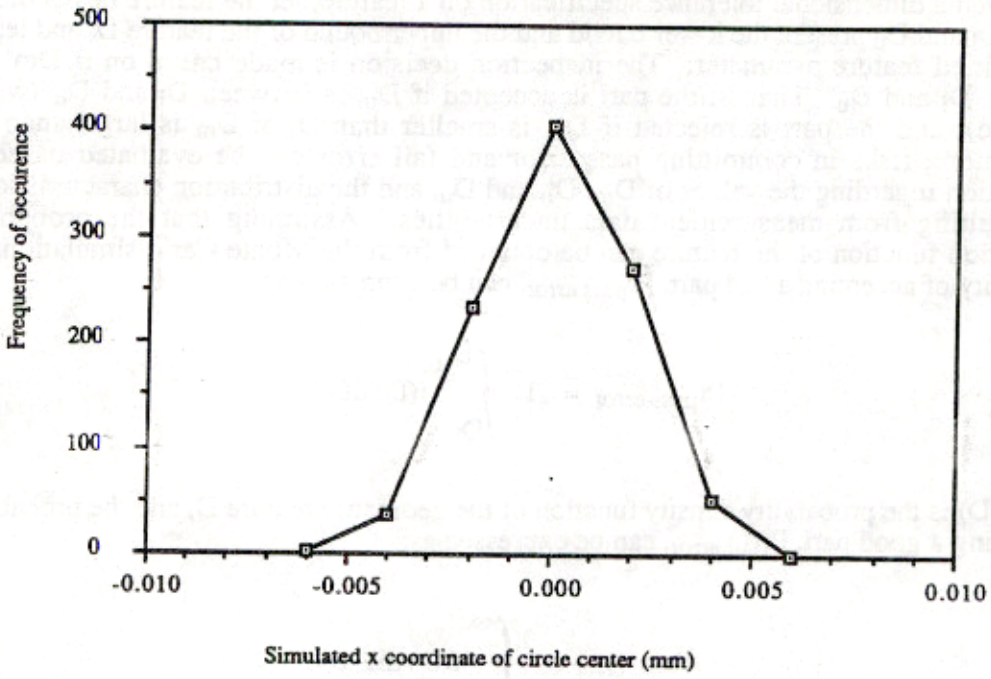


Figure 1. Distribution of simulated x coordinate of the circle center, measurement number = 3, uncertainty range = 0.005 mm.

Table 1 shows the standard deviation of each case obtained from Monte Carlo simulation. Standard deviation is used since the uncertainty patterns follow normally distributed curves. Based on the following results, the following observations can be made:

- The standard deviation of the fitted radius data increases when the uncertainty range of the measurement data increases.

- With the uncertainty range of the measurement data fixed, the standard deviation decreases when the sample points increases.

Table 1. Standard deviations[1] of fitted radius from various simulation cases.

Uncertainty Range	3 points	5 points	7 points
0.05 mm	0.0167	0.0134	0.0109
0.02 mm	0.0067	0.0054	0.0044
0.005 mm	0.0016	0.0013	0.0010

[1]Unit of standard deviation: mm.

With the simulation data based on an ideal circle of radius 100 mm, the following two cases show how risks can be calculated.

Case 1: Tolerance Specification: 99.94 ± 0.05 mm

It is apparent that the part shall be rejected, because the true size of the part is known as 100 mm. However, due to measurement errors in the inspection process, some fitted results may fall within the tolerance specification range and accept decisions may be made. The probability of committing pass error can be obtained by evaluating the following equation:

$$Pr_{\text{pass error}} = \int_{99.89}^{99.99} f(\mu, \sigma, r)\, dr \qquad (4)$$

where $f(\mu, \sigma, r)$ is the probability density function of a normal distribution with mean μ and standard deviation σ described by the following equation:

$$f(\mu, \sigma, r) = \frac{1}{\sqrt{2\pi}\sigma} \exp - \frac{1}{2}\left(\frac{r-\mu}{\sigma}\right)^2 \qquad (5)$$

Mean values and standard deviations of various simulation cases are available in Table 1 and the pass error risks in Case 1 are summarized in Table 2.

Table 2. Probability of pass errors for case 1.

Uncertainty Range	3 points	7 points
0.05 mm	Pr = 0.2578	Pr = 0.1587
0.02 mm	Pr = 0.0581	Pr = 0.0030
0.005 mm	Pr = 0	Pr = 0

Case 2: Tolerance Specification: 100.04 ± 0.05 mm

It is apparent that the part shall be accepted, because the true size of the part is known as 100 mm. However, due to measurement errors in the inspection process, some fitted results may fall outside the tolerance specification range and accept decisions may be made. The probability of committing fail errors can be obtained by the following equation:

$$Pr_{\text{fail error}} = 1 - \int_{99.99}^{100.09} f(\mu, \sigma, r)\, dr \qquad (6)$$

where $f(\mu, \sigma, r)$ is shown in equation (5). Mean values and standard deviations of various simulation cases are available in Table 1. The fail error risks in Case 2 are summarized in Table 3.

CONCLUSIONS

Risk assessment method for CMM-based dimensional inspection is described in this paper. The Monte Carlo simulation method is used to generate uncertainty patterns of the fitted parameters and the uncertainties in the measurement data come from inaccuracy of the inspection process. It is shown that the uncertainty patterns seem to follow the normal distribution. Therefore, standard deviation and mean value of the simulation are used to characterize the uncertainties in the measured results and to calculate the probability of risks.

Number of measurement data represents the sample scheme selected for the inspection task. It is shown in the simulation data that the uncertainty range (of a fitted parameter) decreases when the number increases. The trend is verified by the simulation results. Another factor considered is the uncertainty range of the measurement data. This uncertainty range has to do with the accuracy of the selected machine and the operating condition. A simple 2-D circle example is used to illustrate the application of the method. More complicated tolerancing cases should be investigated to handle general CMM-based dimensional inspection cases.

Table 3. Probability of fail errors for case 2.

Uncertainty Range	3 points	7 points
0.05 mm	Pr = 0.2578	Pr = 0.1587
0.02 mm	Pr = 0.0581	Pr = 0.0030
0.005 mm	Pr = 0	Pr = 0

ACKNOWLEDGEMENTS

This material is based upon work supported by the National Science Foundation under Grant No. (DDM-9308648).

REFERENCES

ANSI/ASME B89.1.12M-1990, 1990, "Method of Performance Evaluation of Coordinate Measuring Machines," ASME, New York, NY.

Bosch, J.A., 1992, The changing roles of coordinate measuring machines, *Industrial Engineering*.

Caskey, G., et al., 1991, Sampling techniques for coordinate measuring machines, *NSF Review*.

Groover, M.P., 1987, Automated inspection and testing, in: "Automation, Production Systems, and Computer-Integrated Manufacturing," Prentice-Hall, Inc., Englewood Cliffs, NJ.

Phillips, S.D., Borchardt, B., and Caskey, G., 1993, Measurement Uncertainty Considerations for Coordinate Measuring Machines (NISTIR 5170), National Institute of Standards and Technology (NIST), Gaithersburg, MD.

Schreiber, R.R., 1990, CMMs: traits, trends, triumphs, *Manufacturing Engineering*.

Shen, Y., and Duffie, N.A., 1993, Comparison of combinatorial rules for machine error budgets, *Annals of the CIRP*, Vol. 42/1, pp. 916-622.

Swyt, D.A., 1992, Challenges to NIST in Dimensional Metrology: The Impact of Tightening Tolerances in the U.S. Discrete-Part Manufacturing Industry (NISTIR 4757), National Institute of Standards and Technology (NIST), Gaithersburg, MD.

THE EFFECT OF UNCERTAINTIES IN DOSE-RESPONSE DATA ON RISK MANAGEMENT OF AIR TOXICS

Jeff C. Huang[1] and William E. Kastenberg[1]

[1]Mechanical, Aerospace and Nuclear Engineering Department
School of Engineering and Applied Science
University of California
Los Angeles, CA 90024-1597

ABSTRACT

Due to the regulatory emphasis on air toxics and the more prominent role of risk based priority setting in the environmental pollution arena, this paper provides a methodology to quantify the uncertainty in the dose-response data. Further, these uncertainties are analyzed and their impacts on the associated health risks of air toxics are assessed. Two air toxics, arsenic and tetrachloroethylene, are selected as the basis of this study. A methodology incorporating probability distributions and Monte Carlo simulation utilizing two computer codes, GEOTOX and Crystal Ball, is used to estimate the risk from air toxics emission. Risk is calculated as the product of exposure rate and cancer potency factor. Examples using point values and probability distributions are provided. The results are compared and analyzed, and their implication regarding risk management is discussed.

INTRODUCTION

During the last decade, air toxics have gained much attention in the environmental pollution arena. In California, two assembly bills, AB 1807 (1983) and AB 2588 (1987), were signed into law by the state government that specifically address the issue of air toxics.[1,2]

The purpose of AB 1807 is to provide: identification of toxic air contaminants, a determination of control priorities, implementation of advanced control technologies and alternatives, assistance to local air pollution control districts, and a consistent level of protection throughout California. As a result, arsenic was identified as a toxic air contaminant in July 1990, and tetrachloroethylene (also known as perchloroethylene or PCE) in October 1991.[3,4]

The purpose of AB 2588 (also known as the Air Toxics "Hot Spots" Act) is to establish a statewide air toxics emission inventory and require stationary sources, or facilities, to report the type and quantity of toxic substances released into the air. Each regional Air Pollution Control District (APCD) places these facilities into three categories: high, intermediate, or low priority. Any facility designated as high priority is required to submit a public health risk assessment. The APCD may also require facilities not in the high priority category to submit public health risk assessments. The submitted public health risk assessment is reviewed by the California Department of Health Services and approved by the APCD. If the public health risk assessment indicates a significant health risk from the emission, appropriate actions must be implemented by that facility. These appropriate actions include: informing the exposed individuals of the public health risk assessment result, and adopting and implementing appropriate control technology to comply with regulation.

From such a perspective, it is not difficult to see the important role of risk assessment in managing air toxics in California. However, risk assessment has many inherent uncertainties. One major source of uncertainty lies in the dose-response data. Dose-response describes the relationship of a unit of dose to its associated adverse health effects (usually the development of cancer). This type of data is usually obtained from animals that are administered very high doses (usually several orders of magnitude higher than what a human would normally be exposed to) in order to observe adverse health effects. Thus, extrapolation is necessary when applying animal data to humans. Several extrapolation models are available, such as the one-hit model, the multistage model, the linear multistage model, and others. Due to different assumptions, different models usually provide values that would sometimes vary by several orders of magnitude. A good example comes from formaldehyde, in which the values of cancer potency factor from the probit and multistage models differ by nineteen orders of magnitude![5]

To be health protective, the US Environmental Protection Agency (US EPA) has adopted data that have only a 5% chance of underestimating risk. The adaptation of such data has raised many concerns and skepticism from industry and the scientific community. Industry is concerned because conservative dose-response data lead to conservative risk estimates that usually exceed the regulatory value, which can cost industry a great amount of money to comply with regulations. The scientific community is concerned because the conservative values are not in agreement with other studies, such as the physiologically based pharmacokinetic models (PBPK models). The values obtained from the PBPK models are usually lower and accepted as more realistic.

The purpose of this paper is to address the issue of dose-response data uncertainty by providing a methodology that would take into account the different values of dose-response data and make risk assessments more realistic to ensure robust decision making.

RISK ESTIMATION

The simplest way of estimating cancer risk is to calculate risk as the product of the exposure rate and the cancer potency factor:

$$\text{Risk} = \text{Exposure Rate} \times \text{Cancer Potency Factor} \qquad (1)$$

In this paper, the exposure rate is obtained from a computer code GEOTOX.[6] GEOTOX is a multimedia (e.g., air, water, soil) compartment model that predicts the transport and transformation of chemicals in the environment and estimates human exposure. GEOTOX does so by utilizing physicochemical properties of a pollutant and landscape property data to determine how a substance partitions in the environment.

Furthermore, it utilizes environmental concentrations and human intake data to determine exposure to humans. The cancer potency factors are available from many sources, such as the US EPA (see Table 1).[7]

Risk Estimation Using Point Values

To obtain exposure rates from GEOTOX, chemical file(s) and a landscape file of interest must be selected. Two chemical files, one for arsenic and one for PCE, were created for this study. The landscape file selected is the California landscape, which is already available in GEOTOX. The source term used is the 1989 state emission estimation from the California Air Resource Board (CARB), 4,500 lb./yr for arsenic and 5,630,000 lb./yr for PCE.[8]

From GEOTOX, utilizing the emission data, physicochemical property data, and the landscape property data, the exposure rates are calculated and shown in Table 2. These exposure rates indicate that the exposure to arsenic is mostly from ingestion (others being negligible), and the exposure to PCE is mostly from inhalation (others being negligible).

Ignoring the negligible contributions and applying Equation (1) the risk can be calculated as:

$$\text{Risk from arsenic} = (8.50 \times 10^{-7})(50) = 4.25 \times 10^{-5}$$

$$\text{Risk from PCE} = (4.69 \times 10^{-5})(1.82 \times 10^{-3}) = 8.54 \times 10^{-8}$$

This value is the individual lifetime risk.

Risk Estimation Using Probability Distributions

To take uncertainties into account, we propose to assign a probability distribution to each variable, i.e., exposure rate and cancer potency factor. From these probability distributions, the risk can be estimated as the joint probability distribution using Monte Carlo simulation (a software package called Crystal Ball is used for this task).[9] The advantage of doing so is to present the possible range of values of each parameter, thus it is more informative and more useful to a decision maker.

For illustration purposes, we have assumed that the source term takes on a uniform probability distribution. For arsenic, we have assigned a uniform probability distribution with a minimum of 4,000 lb./yr, and a maximum of 5,000 lb./yr. For PCE, we have assigned a uniform probability distribution with a minimum of 5,000,000 lb./yr, and a maximum of 6,000,000 lb./yr. Using the upper and lower bounds of the source terms as inputs for GEOTOX, we can obtain the exposure rate distributions for arsenic and PCE. From GEOTOX, the uniform probability distribution for arsenic has a minimum of 7.55×10^{-7} mg/kg/day and a maximum of 9.44×10^{-7} mg/day/day. For PCE, the uniform probability distribution has a minimum of 4.22×10^{-5} mg/kg/day and a maximum of 5.16×10^{-5} mg/kg/day.

To assign a probability distribution to the cancer potency factor, we have adopted a method used by Hattis and Froines.[10] In a study, Hattis and Froines have found that the values of the cancer potency factors from PBPK models are roughly 7.2% (an average value from three PBPK studies: ethylene oxide, butadiene, and perchloroethylene) of those from the US EPA. Hattis and Froines proposed using the EPA values as the 95th percentile and the PBPK values as the mean of a lognormal distribution. In assigning a lognormal distribution in the software package Crystal Ball, the mean and standard deviation (s.d.) are required. The mean can be estimated as 7.2% of the EPA value:

$$\text{mean} = 0.072 \times \text{EPA value} \quad (2)$$

and the standard deviation can be calculated from the following:

$$\ln(\text{mean}) + 1.6449 \ln(\text{s.d.}) = \ln(95\text{th}\%) \quad (3)$$

since in a lognormal distribution, the 95th percentile is 1.6449 standard deviations away from the mean. Rearranging Equation (2), the standard deviation can be calculated as:

$$s.d. = \exp\left(\frac{\ln(95th\%) - \ln(mean)}{1.6449}\right) \quad (4)$$

For arsenic, using Equations (2) and (4), we obtain a lognormal distribution with a mean of 3.6 and a standard deviation of 4.95. For PCE, using the same equations, we obtain a lognormal distribution with a mean of 1.31×10^{-4} and a standard deviation of 4.95.

Now that we have probability distributions for both exposure rate and cancer potency factor, the next step is to obtain a joint probability distribution for the risk. Monte Carlo simulation (the software package Crystal Ball) is used to perform such a task, and the results are presented in Table 3.

DISCUSSION

Two methods of risk estimation, one using point values and one using probability distributions, are performed. Comparing the results from the two methods, the estimated risk using point values is indeed very conservative. In both cases (arsenic and PCE), it falls in between the 95th and 100th percentiles of the risk value using probability distributions.

When using just point values, arsenic clearly requires regulatory action, since the risk is higher than the regulatory value (4.25×10^{-5} vs. 10^{-6}). However, when probability distributions are used, we observe that the 50th percentile is very close to the regulatory value (2.97×10^{-6} vs. 10^{-6}). Such a small number is hard to detect, therefore whether or not a regulatory action is to be called upon deserves more careful consideration. In the case of PCE, in using both methods, the risk is below the regulatory value, and thus no regulatory action may be required.

The illustration of both methods once again reinforces the belief that using conservative values do not necessarily justify the cause of being health protective when it can lead to unsound decision making. As in the case of arsenic, when applying probability distributions to risk estimation, there is 50% chance that the risk is below (or above) regulatory concern, whereas in the case of PCE, a risk manager can be nearly 100% confident that the risk is below regulatory concern. When the uncertainty is as great as in the case of arsenic, more research is needed to narrow the uncertainty before a robust decision can be made. If not, a large amount of money can be wasted when a regulatory action is called upon and the actual risk is below the regulatory value.

CONCLUSION

This paper has explored two methods of estimating risk for air toxics: one using point values and one using probability distributions. In comparison, the risk estimation is

very conservative when using point values. Although using point values can be health protective, it can also lead to unsound decision making. As demonstrated in this paper, in the case of arsenic, due to the uncertainty in the dose-response data, the estimated risk could be as low as 3.15×10^{-7} (5th percentile) and as high as 4.17×10^{-5} (95th percentile). For these two extreme cases, one requires regulatory action and the other doesn't. This clearly illustrates the importance in choosing the right values in performing such risk estimation. When a risk manager is not aware of such uncertainties in risk assessment data, the decision making process can be very dangerous.

Therefore it is desirable to take into account such uncertainties in the data by incorporating probability distributions to represent the possible range of values of each variable in the risk assessment process. Thus the risk estimation will provide the risk manager with some level of confidence on which a robust decision can be made.

Table 1. Cancer potency factors for arsenic and PCE.

Cancer Potency Factor	Arsenic	PCE
Inhalation $(mg/kg/day)^{-1}$	-	1.82×10^{-3}
Oral $(mg/kg/day)^{-1}$	50	5.1×10^{-2}

Table 2. Exposure calculations for arsenic and PCE from GEOTOX.

Pathway	Arsenic (mg/kg/day)	PCE (mg/kg/day)
Inhalation	1.54×10^{-10}	4.69×10^{-5}
Drinking Water	3.51×10^{-7}	6.13×10^{-9}
Biota Ingestion	1.89×10^{-7}	2.09×10^{-9}
Meat/Dairy Ingestion	2.44×10^{-7}	4.43×10^{-9}
Fish Ingestion	4.41×10^{-8}	6.25×10^{-10}
Soil Ingestion	1.39×10^{-8}	1.47×10^{-12}
Dermal Absorption	7.79×10^{-9}	8.27×10^{-13}
Total	8.50×10^{-7}	4.69×10^{-5}

Table 3. Risk percentiles of arsenic and PCE.

Risk Percentiles	Arsenic	PCE
0%	4.87×10^{-8}	9.77×10^{-11}
5%	3.15×10^{-7}	5.03×10^{-10}
25%	1.09×10^{-6}	2.18×10^{-9}
50%	2.97×10^{-6}	5.94×10^{-9}
75%	8.18×10^{-6}	1.63×10^{-8}
95%	4.17×10^{-5}	8.31×10^{-8}
100%	2.90×10^{-4}	5.79×10^{-7}

REFERENCES

1. California Air Resources Board, "Program Update: Air Toxics Update #1," (1986).
2. California Air Resources Board, "Program Update: Air Toxics Update #5," (1989).
3. California Air Resources Board, "Program Update: Air Toxics Update #7," (1991).

4. California Air Resources Board, "Program Update: Air Toxics Update #8," (1992).
5. Dennis J. Paustenbach, "Important Recent Advances in the Practice of Health Risk Assessment: Implications for the 1990's," *Regulatory Toxicology and Pharmacology*, 10:204-243 (1989).
6. Thomas E. McKone, L. B. Gratt, M. J. Lyon, and B. W. Perry, "GEOTOX Multimedia Compartment Model User's Guide," Lawrence Livermore National Laboratory (1987).
7. US Environmental Protection Agency, "Health Effects Assessment Summary Tables FY-1991 Annual," Washington, DC (1991).
8. Richard Bode, California Air Resources Board, personal communication (1993).
9. Decisioneering, Inc., "Crystal Ball for Windows User's Manual," Version 2.0 for Windows, Denver, Colorado (1992).
10. Dale Hattis and John Froines, "Uncertainties in Risk Assessment," *Chemical Risk Assessment* (1992).

018 Reliability, Models & PSA

Chair: K. Inoue, Kyoto Univ.

Identification of System States Based on Multistate Model

K. Nakashima (Faculty of Engineering, Japan); H. Matznaga (Toyama Prefectural U., Japan)

Safety Substantiation Analysis for Airplane Systems

B. Zilberman (Israel Aircraft Ind.)

Automatic Construction of Markovian Transition Matrices for the Treatment of Large Size Reliability Problems

B. Tombuyses (U. Libre de Bruxelles); B. Arien, D. Lamy (SCK/CEN, Belgium)

Markovian Models for the Reliability Analysis of Multichanneled Protective Systems

P.F. Frutuoso e Melo (COPPE/UFRJ, Brazil); L.F. Oliveira (PRINCIPIA Ltda. and U. Federal of Bahia, Brazil); R. Youngblood (BNL)

IDENTIFICATION OF SYSTEM STATES BASED ON MULTISTATE MODEL

Kyoichi Nakashima[1] and Hitoshi Matznaga[2]

[1]Faculty of Engineering
Department of Electronics and Informatics
[2]Research Institute for Technology
Toyama Prefectural University
Kosugi, Toyama, 939-03 JAPAN

INTRODUCTION

For large systems whose failures often cause undesired consequences and great loss, it is important to identify system states near system failure, so that we can take preventive measures before the occurrence of system failure. To do it, we need observe intermediate states, such as degraded states, of system components between completely functioning and failed states, and then have a method for testing from such observations of componet states whether the current status of the system is near system failure. This paper presents such a method by using the multistate model which is a mathematical model suitable for treating the reliability analysys of a system composed of components with many intermediate states.

The current status of the system can be represented by state vectors of components. However, it is unavoidable to involve uncertainty in judging the current state of each component. Then, the probability that any component is in a state is estimated by combining expert judgements on the subjective probability.

Given trasition diagram representing the transition possibility among states of each component, state vectors of components are classified based on the logical distance from failure, which is defined as the minimum number of component transitions required to reach system failure. If the transition rates among states of each component are obtained, state vectors of components are also classified based on the probabilistic distance from failure, which is defined as the probability of reaching system failure from the current status within a specified time interval. A procedure has been presented for obtaining the Boolean function which represents the structural relation between component states and system states classified by the logical distance, and a method for computing the probabilistic distance of the current status from the failure state has also been given[1]. If the probability of each component state is estimated by combining expert judgements, the expected value of the logical distance or the probabilistic

distance from the current state of the system to system failure is computed to judge whether the current state is near system failure.

MODEL

The system is composed of n componets $1, 2, \cdots, n$. Component i is in any one of α_i states and let $\Gamma_i = \{0, 1, \cdots, \alpha_i - 1\}, i = 1, 2. \cdots, n$ be the set of state of component i. Usually, state 0 and $\alpha_i - 1$ represent the completely normal state and failed state, respectively and states $1, 2, \cdots, \alpha_i - 2$ represent degraded states in the order of deteriorating toward the failed state. The status of the system is expressed by a state vector $X = (X_1, X_2, \cdots, X_n)$ of components, where $X_i \in \Gamma_i, i = 1, 2, \cdots, n$. Define the binary variable $x_{ij}, i = 1, 2, \cdots, n$ and $j = 0, 1, \cdots, \alpha_i - 1$ which takes 1 if component i is in state j and 0 otherwise. Let $x_i = (x_{i0}, x_{i1}, \cdots, x_{i,\alpha-1}), i = 1, 2, \cdots, n$ and $x = (x_1, x_2, \cdots, x_n)$.

The transition possibility between two states of each component is given; $\delta_{ijk} = 1$ if it is possible for component i to transit from state j to state k directly (without going through other states) and $\delta_{ijk} = 0$ otherwise. The transition rate λ_{ijk} form state j to state k of component i may be given if possible to estimate it ($\lambda_{ijk} = 0$ for $\delta_{ijk} = 0$).

The transition relation among state vectors of components is also represented by a transition diagram medeled as a digraph with node corresponding to state vectors and directed branches corresponding to the transition possibility among state vectors. Each branch (u, v) from node u to node v means the transition possibility from u to v by one transition of only one component. A failure path from node X which is not any failure state is defined as a path which reaches system failure for the first time from X.

ESTIMATING THE PROBABILITY OF COMPONENT STATE

The current status of the system is represented by state vectors of components which some experts judge from observations of current states of components by nondestructive testing and scientific measurements. However, it is unavoidable to involve uncertainty in such judgements due to the existence of observational errors and the lack of knowledge in understanding or interpreting observed results. Then, the expert judgement is made on the subjective probability that component i is in a state $X_i \in \Gamma_i$. The probability $\Pr\{X_i\}$ that component i is in a state $X_i \in \Gamma_i$ is estimated by combining expert judgements in the Bayesian framework[2].

If the expert judgement is permitted to be made on the basic probability assignment of a subset of component states, it may be possible to estimate the probability $\Pr\{X_i\}$ by combining expert judgements in the theory of evidence[3].

IDENTIFYING SYSTEM STATE BY LOGICAL DISTANCE

The logical distance of state vector X from system failure is defined as the minimum number of possible transitions of components required to reach system failure form X. This is also equal to the minimum length among failure paths from X. System states except the failure state F are defined by LD_d, the state for which the logical distance from system failure is $d (d = 1, 2, \cdots, m)$. This means that system state LD_d is the set of state vectors X with logical distance d from system failure.

Suppose that the Boolean function $f_F(x)$ of x corresponding to system failure is given by using fault trees etc. Then, we need how to get an expression of the Boolean function $f_d(x)$ of x corresponding to system state $LD_d, d = 1, 2, 3, \cdots, m$; $f_d(x) = 1$ if the system exists in any state of $\{F, LD_1, LD_2, \cdots, LD_d\}$ and $f_d(x) = 0$ otherwise. A

method is given below for obtaining $f_d(x)$ from $f_F(x)$ by using Boolean algebra with restricted binary variables[4, 5].

Procedure for obtaining $f_d(x)$

Let t be a term of a sum-of-product form of the Boolean function. A term obtained by replacing exatly one variable x_{ik} in t with variable x_{ij} such that $\delta_{ijk} = 1$ holds is called an adjacent term of t. Then, $f_d(x), d = 1, 2, \cdots, m$, are obtained by the following procedure.

Step 1. Simplify the sum-of-product form of $f_F(x)$ by removing redundant terms by the idempotence and absorption rules.

Step 2. Obtain all adjacent terms of each term of the simplified sum-of-product form of $f_F(x)$ and remove those absorbed by terms of $f_F(x)$. Let $g_1(x)$ be the logical sum of the remaining terms. Then $f_1(x) = f_F(x) \vee g_1(x)$.

Obtain the simplified sum-of-product form of $g_1(x)$ and set $d = 2$.

Step 3. Obtain all adjacent terms of each term of the simplified sum-of-product form of $g_{d-1}(x)$ and remove those absorbed by terms of $g_{d-1}(x)$. Let $g_d(x)$ be the logical sum of the remaining terms. Then, $f_d(x) = f_{d-1}(x) \vee g_d(x)$.

Obtain the simplified sum-of-product form of $g_d(x)$. Reset $d + 1 \rightarrow d$ and repeat Step 3. If $f_d(x) = 1$ holds, then set $d \rightarrow m$ and stop.

When the current state vector X is determined from observations of the current states of components, the current state of the system LD_{d^*} is identified from the minimum value d^* of d that satisfies $f_d(x) = 1$.

When the probabilities $\Pr\{X_i\}, X_i \in \Gamma_i, i = 1, 2, \cdots, n$ of current states of components are estimated from expert judgements, the probability $\Pr\{f_F(x) = 1\}$ that the system is in failure state and the probabilities $\Pr\{f_d(x) = 1\}, d = 1, 2, \cdots, m$ that the system is in any state of $\{F, LD_1, LD_2, \cdots, LD_d\}$ can be computed by using the Boolean functions obtained by the above procedure. Then, the expected value E_{LD} of the logical distance from the current status of the system to system failure is estimated by

$$E_{LD} = \sum_{d=1}^{m} d\left[\Pr\{f_d(x) = 1\} - \Pr\{f_{d-1}(x) = 1\}\right] = m - \sum_{d=0}^{m-1} \Pr\{f_d(x) = 1\}$$

where $f_0(x) = f_F(x)$.

IDENTIFYING SYSTEM STATE BY PROBABILISTIC DISTANCE

A system does not neccessarily reach system failure from a state vector earlier than from another state vector with larger logical distance, because the probability of reaching system failure from a state vector within a specified time interval depends on transition rates among component states. Given the transition rate for the possible transition of each component, an equation has been given[1] for computing the probability $PD(X, P, T)$ of reaching system failure from state vector X along the failure path P within a specified time interval T. If there exist Q failure paths $P_1, P_2, \cdots, P_n$ from the state vector X, then the probabilistic distance $PD(X, T)$ of X from system failure, defined as the probability of reaching system failure from the current status within the specified time interval T, is computed by the total sum of $PD(X, P_q, T)$ over all failure paths $P_q, q = 1, 2, \cdots, Q$.

In general, as the logical distance of the current status X from system failure increases, the number of failure paths also increases, and therefore the computation of

$PD(X,T)$ becomes time-consuming. However, we often need to compute the probabilistic distance for only the current status with a small logical distance, because we usually want to test whether the current status is near system failure.

State vectors of components are classified into system states $PD_1, PD_2, \cdots, PD_l$ by the probabilistic distance. PD_d is the set of state vectors X that satisfy $\theta_{d-1} > PD(X,T) \geq \theta_d (d = 1,2,3,\ldots,l)$, where $\theta_d, d = 0.1.2.\ldots,l$ are specified values satisfying $\theta_0 = 1 > \theta_1 > \theta_2 > \theta_3 > \cdots > \theta_l = 0$.

When the Boolean functions $f'_d(x)$ corresponding to system states $PD_d, d = 1,2,\cdots,l$ are obtained and the probabilities $\Pr\{f'_d(x) = 1\}, d = 1,2,\cdots,l$ that the system is in any state of $\{F, PD_1, PD_2, \cdots, PD_d\}$ are computed, the expected value E_{PD} of the probabilistic distance from the current status of the system to system failure can be estimated similar to that of the logic distance.

CONCLUDING REMARKS

Our method is applicable to testing from obserbations of component states whether the curent status of the system is near system failure. If transition rates among compnent states are obtained, we can test from the value (or expected values) of both measures, the logical distance and probabilistic distance, but otherwise we use only the logical distance. The practical applicability of our methods depends heavily on the development of techniques for identifying component states, such as nondestructive testing. The method is also applicable to devising a warning system which indicates which warning level the current status of a process system belongs to, from observations of sensor systems.

REFERENCES

1. K. Nakashima and G.G. Weber, A method to test whether a system is near failure, *Microelectronics and Reliability* 30:1049(1990).

2. C.A. Clarotti and D.V. Lindley (Eds), "Accelerated Life Testing and Experts' Opinions in Reliability," North-Holland,Amsterdam(1988).

3. G. Shafer, "A Mathematical Theory of Evidence," Princeton University Press, Princeton(1976).

4. L. Caldarola, Coherent systems with multi-state components, *Nucl. Eng. Design* 58:127(1980).

5. K. Nakashima and K. Yamato, Some properties of multi-state monotone systems and their Boolean structure functions, *Trans. IECE Jpn* E66:535(1983).

SAFETY SUBSTANTIATION ANALYSIS FOR AIRPLANE SYSTEMS

BENYAMIN ZILBERMAN

Israel Aircraft Industries
TASHAN Engineering Center, Dept.2491
Ben Gurion International Airport
70100 Israel

ABSTRACT

The safety of a modern airplane with its assembly of complex systems can only be achieved by a thorough asessment of potential failure conditions and their severities. Different methods are used to perform safety assessments.

This paper presents a new method, which is particularly efficient for safety analysis of fault tolerant airplane systems. It is based on Markov model, created to check the influence of single and multiple failures on airplane safety.

1. INTRODUCTION

All airworthiness standards are based on the principle of fail-safe design concept, which considers the effect of single failure and combination of failures in defining a safe design. As Advisory Circular AC 25.1309-1A states, the following basic objects apply[1]:

1. In any system/subsystem the failure of any single element, component or connection during any one flight should not prevent continued safe flight and landing, regardless of its probability.

2. Subsequent failures during the same flight whether detected or latent, should also not prevent continued safe flight and landing, unless their joint probability is shown to be extremely improbable (less than 10^{-9} per flight hour).

The usual way to satisfy these objectives is to perform the following analysis:

Failure Mode Effect and Criticality Analysis (FMECA) to prove that there is no single failure mode that can lead to catastrophical effect[2,3].

Fault tree analysis to prove that any combination of failures, leading to

catastrophical effect is beyond the required limits".

FMECA performs exhaustive analysis of all component failure modes, but since it considers only one failure mode at time,this technique alone can not prove, if the system satisfies the fail safe design concept.

The reliability of components in aircraft system is usually very high (in the range of 10 - 100 failures per 1 million flight hour). Combination of 2 independent failures, occurring in the same flight, is in the range of 10^{-8} - 10^{-9}, and probability of three independent failures is less than 10^{-12}.

During fault tree preparation, the analyst shall investigate all possible combination of failures leading to an undesired event. Sometimes he is forced to consider combination of 3,4,5 or more independent failures that can occur in one flight. The process of fault tree construction for a complicated system is time consuming. The effort needed to construct such a fault tree is not always justified because the minimum required probability of catastrophic failure condition occurrence is less than 10^{-9}, as FAR states. Therefore, in some cases it is permissible to consider not more than 3 subsequent failure in one flight, without sacrificing the accuracy of the calculation.

Markov modelling is an alternative, very flexible and powerful technique to use in system safety analysis of airplane systems. It can handle failure sequencing, repairable systems, fault-tolerant systems, can easily solve calculation problems in case of non-series parallel system architecture, consider transient, near-coincident failure, etc.[5]. The limitation of this technique is that the number of states in Markov model may grow rapidly as the size of the system increases.

A method considering the FMECA, Fault Tree, and Markov technique in safety substantiation of airplane systems is described.

2. METHOD DESCRIPTION

As a first step an FMECA should be performed (see Table 1). Each failure mode is assigned a value of probability, based on failure rate, failure mode ratio and operational time. Each failure mode is considered as failure on first failure level in a Markov model. All calculated probabilities are represented as transition rates from state 1 (all components are operating) to states on first failure level. A list of failure conditions, defining the "end effect" of assumed failures on system operation should be used in identifying states in Markov model. Each failure condition is given severity classification , according to FAR requirements.

Than a Markov model should be created, expanding the 2nd failure level. On this level the combination of two failures is considered. But in order to eliminate fast model grow, an aggregation technique is used.

All transitions from 1st level states can lead only to states representing the selected failure conditions - "end effect" states. In addition, a working state is used to count for all system states with no effect after two failures. The same approach can be used on the 3rd level (combination of 3 failures). From each state on the 2nd failure level, except failure states (catastrophical failure condition) the transitions, leading to end effect states on the 3rd level should be explored. The model can be truncated on the 3rd or 4th level. As it was already mentioned, consideration of 3 or 4 independent failures gives enough accuracy in safety assessment, considering the requirement of probability of catastrophical failure of 10^{-9} per flight hour. In Table 2 state 1 represents the initial condition of the system, when all components are operating. States 2 through 8 represent system's 1st failure level, e.g. failure at one of the components. State 9 is a failure state on the 1st level, it represents the failure of component H.

Table 1. Failure mode effect and criticality analysis (simplified example)

Part ident.	Failure mode	Severity of failure effect	Failure rate	Notes
A	Operation failure	Major	2E-6	
B	Operation failure	Minor	4E-5	
C	Operation failure	Minor	4E-6	
D	Dormant failure	Minor	5E-6	
D	Operation failure	-	1E-5	Second failure
E	Dormant failure	Minor	7E-6	
E	Operation failure	-	5E-5	Second failure
F	Operation failure	Minor	3E-5	
G	Dormant failure	Minor	6E-7	
G	Operation failure	-	7E-6	Second failure
H	Operation failure	Catastr.	7E-6	Second failure

States 10 and 11 are aggregated states, combining all working states on a 2nd failure level (normal operation and degraded operation consequently). States 12 and 13 are failure states on 2nd and 3rd failure levels respectively.

In the system being considered not all 3rd failures lead to system failure. So, the assumption for truncating the model leads to some overestimation in system failure probability. The sum of failure probabilities of states 9 and 12 provides a lower bound on the system failure probability, because these states have probabilities equal to the exact case and the truncation values have not been included. The upper bound is obtained by adding the system failure state 13 to the lower bound probability. The tightness of the bounds is measured by their difference (probability of state 13). If this approximation is too large for a given problem, the model must be constructed out to the next level.

3. ADVANTAGES OF THE PROPOSED METHOD

This method provides exhaustive analysis of all single failures and failure combination, leading to defined failure conditions. It eliminates the possibility of missing any failure combination during safety assessment procedure.

The fact, that Markov models are used to substantiate system safety, allows consideration of many additional conditions required by FAR/JAR (common-mode failure, human errors, etc.).

Table 2. Transitions in Markov model

States	Transitions	States	Transitions
1 2	A	5 10	B+C+ED+GD+F
1 3	B	5 12	A+H
1 4	C	6 10	B+C+DD+GD+F
1 5	DD	6 12	A+H
1 6	ED	7 10	B+C+DD+ED
1 7	F	7 11	A
1 8	CD	7 12	G+H
1 9	H	8 10	B+C+DD+ED
2 11	B+C+F+GD	8 11	A
2 12	D+E+H	8 12	F+H
3 10	DD+ED+F+GD	10 13	$\Sigma\lambda$
3 11	A+C	11 13	$\Sigma\lambda$
3 12	H		
4 10	DD+ED+CD+F		
4 11	A+B		
4 12	H		

Markov models used in the proposed method are relatively small, due to aggregation and truncation techniques.

The detection, isolation and reconfiguration logics can be analysed as coverage models for system components.

4. REFERENCES

1. Advisory Circular 25.1309 - 1A, System Design and Analysis (1985)

2. MIL-STD-1629A Procedures for Performing a Failure Mode, Effects and Criticality Analysis (1980)

3. ARP 926A Fault/Failure Analysis Procedure (1967)

4. Fault Tree Handbook. Nureq-0492 (1981)

5. K.S.Trivedi, Probability and Statistics with Reliability, Quening and Computer Science Application, Prentice Hall (1982)

AUTOMATIC CONSTRUCTION OF MARKOVIAN TRANSITION MATRICES FOR THE TREATMENT OF LARGE SIZE RELIABILITY PROBLEMS.

B. Tombuyses,[1*] B. Arien,[2] and D. Lamy[2]

[1]Université Libre de Bruxelles, Service de Métrologie Nucléaire, Belgium.

[2]SCK/CEN, Mol - Belgium

*Aspirant FNRS.

I. INTRODUCTION

The Markovian formalism has been generally recognized as a powerful tool for the solution of reliability and availability problems, allowing for dependencies between components and elaborate repair policies. However two main drawbacks have hampered their industrial use :

(a) a huge differential system to be solved (size = m^n, where m is the number of states of each of the n components).

(b) the need of full automatic construction of the transition matrix, given only the knowledge of the components and the system's logic.

We are developing the software CAMERA[1] to solve these difficulties. It will namely include a reduction technique of the differential system based on the component influence graph[2]. We describe here the automatic construction of the transition matrix, when operational rules create dependencies between components. The method is applied to a simple but realistic example and the results are compared with those obtained with a classical fault tree technique.

II. TRANSITION MATRIX

For a system of N components, any state I is a N-uple $(i_1 \ldots i_N)$, where i_k denotes the state of component k. The transition matrix is constructed from reliability characteristics of the components and influences between them. We consider two types of influences : the ordinary influences affecting the transition rates of the components and the essential influences for which the system state directly induces the states of some components.

The matrix is automatically set up in three steps :

1. construction of a basic matrix with independent components[3] → L_o
2. correction of L_o to take into account the ordinary influences → L_1
3. correction of L_1 to take into account the essential influences → L_2

The last point is explicited in the next two paragraphs.

III. ESSENTIAL INFLUENCES AND OPERATIONAL RULES

Essential influences are expressed by means of operational rules. An operational rule provides the action to be performed on a component, resulting from a change of the system state. It is described by three elements : 1) the situation A before the system changes, 2) the situation B after the system changes, 3) the action to be performed; the rule is symbolized by : **{A → B} => action.**

A situation corresponds to a set of system states satisfying some conditions, either on physical variables or on components states. If the physical variables are stationary, it is possible to express the situations in terms of component states only, because each system state uniquely determines the corresponding values of the physical variables.

A "mask" matrix M is associated with the transition from A to B : M_{IJ} equals 1 if J and I satisfy the conditions for A and B respectively, 0 otherwise. An action on a component C is described by a transition on demand matrix D^C, where $D^C_{i_c j_c}$ gives the probability of the transition $j_c \rightarrow i_c$ when the action is applied. D^C is the identity matrix if the action is not applied to C. This matrix takes into account failures on demand or human errors (incorrect applications of the rule by operators). A global matrix D is then constructed by tensorial product of the matrices D^C.

IV. MODIFICATIONS OF THE MATRIX DUE TO OPERATIONAL RULES

Let L_o be the initial transition matrix. Considering a rule, we get a new matrix $L = L_o + (D-I)\,(L_o * M)$, where D, M are defined as hereabove, I is the identity matrix and * symbolyzes the Hadamard product. Application of successive rules is not commutative. Rules have to be mathematically treated recursively in the same order as they are physically applied to the system.

Example

We consider a rule involving a pump P (2 states:working\failed; failure rate λ) and a valve V normally closed (2 states:closed\open; probability of failure to open q). The rule imposes that V opens when P fails, i.e. :

{P working → P failed} => opening of V

$$L^P = \begin{pmatrix} -\lambda & o \\ \lambda & o \end{pmatrix} \qquad D^V = \begin{pmatrix} q & o \\ 1-q & 1 \end{pmatrix}$$

Numbering the states of (P V) as 1 = (11), 2 = (12), 3 = (21), 4 = (22), we have :

$$L_o = \begin{pmatrix} -\lambda & o & o & o \\ o & -\lambda & o & o \\ \lambda & o & o & o \\ o & \lambda & o & o \end{pmatrix}; \; M = \begin{pmatrix} o & o & o & o \\ o & o & o & o \\ 1 & 1 & o & o \\ 1 & 1 & o & o \end{pmatrix}; \; D = \begin{pmatrix} q & o & o & o \\ 1-q & 1 & o & o \\ o & o & q & o \\ o & o & 1-q & 1 \end{pmatrix} \Rightarrow \; L = \begin{pmatrix} -\lambda & o & o & o \\ o & -\lambda & o & o \\ q\lambda & o & o & o \\ (1-q)\lambda & \lambda & o & o \end{pmatrix}$$

V. CLOSURE OF THE ABV ISOLATION VALVES OF THE BR2

As illustration we have applied the technique described hereabove with a simple problem. It concerns the closure system of the ABV valves of the research reactor BR2 in Mol. These valves are aimed at isolating the primary circuit when the reactor is shutdown and depressurized, and they are driven by a hydropneumatic system. The depressurization can be accidental or controlled, but in any case it must be accompanied by the reactor shutdown. The opening/closure operations are commanded via

solenoid valves by acting on the electric supply to the solenoids. This electric supply is controlled by a circuit including three pressure sensors located at the inlet and outlet of the reactor vessel, so that the primary circuit depressurization automatically initiates the ABV closure. For the sake of convenience we have considered only one ABV. A simplified version of the control circuit is shown on figure 1, where 1, 2, 3, 4, 5 denote electric contacts controlled by the pressure sensors S1, S2, S3, and R1, R2 are electric relays whose contacts close when the relay coils are energized.

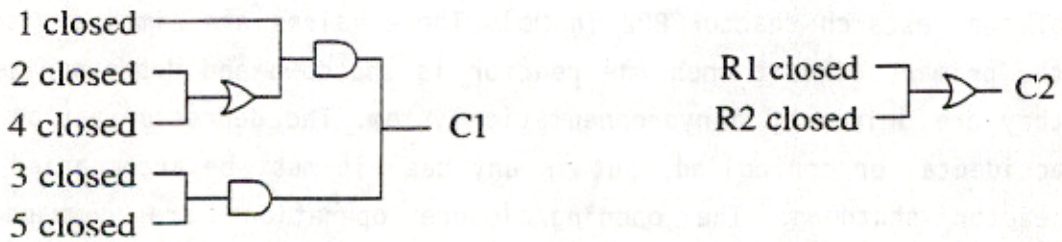
The whole system has been decomposed in 11 elements, each element being a component or a group of components.

Elements	States	Failure probabilities
1,2,3,4,5: electric contacts	open, closed	failure to close : $7\ 10^{-6}$/d
R1,R2 : electric relays	open, closed	failure to close : $7\ 10^{-6}$/d
SV : solenoid valve	positions 1,2	failure to change position : 10^{-5}/d
HP : hydropneumatic system & ABV	working, failed	failure rate : 10^{-6}/hr repair rate : $2\ 10^{-2}$/hr
ES : electric supply	working, failed	failure rate : 10^{-5}/hr repair rate : 0.3/hr
PC : primary circuit & sensors	1: nominal state 2: non detected LOP 3,4,5: LOP detected by 1 sensor 6,7,8: LOP detected by 2 sensors 9: LOP detected by 3 sensors	failure to detect per sensor : 7.10^{-4}/d The PC depressurization frequency is modelled by a Poisson's law with parameter 10^{-3}/hr. (LOP = loss of pressure)

The system's logic provides the following rules :

. Rule 1 (2\3) : {PC in nominal state → LOP detected by S1 (S2\S3)} => closure of contact 1 (2 and 3 \ 4 and 5)

. Let C1, C2 be the following conditions :



. Rule 4 : {ES working and (not C1) → ES working and C1} =>
closure of R1, R2

. Rule 5 : {HP and ES working and (not C2) → HP and ES working and C2} =>
closure of ABV.

VI. RESULTS

As results we provide the unavailability $\bar{A}(T)$ of the ABV closure system, i.e. the probability that the primary circuit depressurizes without ABV closure occurs before time T, and the probability f(t) that the ABV fails to close on demand at time t. If all the components are initially in good state, f(t) is a non-decreasing function and $\bar{A}(T)$ is bounded by :

$$(1-e^{-\lambda_{PC}T})\, f(0) \leq \bar{A}(T) = \int_0^T \lambda_{PC}\ e^{-\lambda_{PC}t}\ f(t)\, dt \leq (1-e^{-\lambda_{PC}T})\, f(T).$$

$\bar{A}(T)$ and f(T) have been calculated with our Markovian software CAMERA and compared with the same function produced by RISKSPECTRUM[4] (fault tree method). The results are compared on figure 2 and show a good agreement between both methods. The fault tree curve fits the upper bound and the small discrepancy with the Markov curve is ascribed to the fact that the Markovian method treats more rigorously the time dependency of the problem.

Characteristics of the Markovian system : The system of O.D.E. involves 9216 states and 127820 transitions. Our reduction technique[2] leads to a total of 199 O.D.E. and 730 elements to store.
Characteristics of the fault tree : The fault tree comprises 12 gates and 13 basic events. It produces 17 minimal cut sets.

VII. CONCLUSION

We have established the possibility of constructing in an automated process the Markovian transition matrices related to practical systems, even when the components states are linked by complex interdependencies. In this paper we have limited these dependencies to operational rules. However more general interactions between components can be treated. The example presented hereabove also shows that failures on demand can be taken into account. Combined with a reduction technique of the differential systems, the automatic construction of transition matrices allows the Markovian approach to handle large size and complex installations.

References

1. B. Arien, et al. "Reliability Analysis of Large Systems by the Markovian Technique - Development of the CAMERA Software", Proceedings of PS '91, Vienna 1991, p. 47-59.

2. J. Devooght, et al. "The Use of the Component Influence Graph to Reduce the Size of Markovian Reliability Problems". Proc. conf. ESREL93, Munich, May 1993, Elsevier.

3. V. Amoia, et al. "Computer-Oriented Formulation of Transition Rate Matrices via Kronecker Algebra", IEEE Trans. Reliability, Vol R-30 n° 2, june 1981.

4. Risk Spectrum, Users Manual, November 1992, RELCON Teknik.

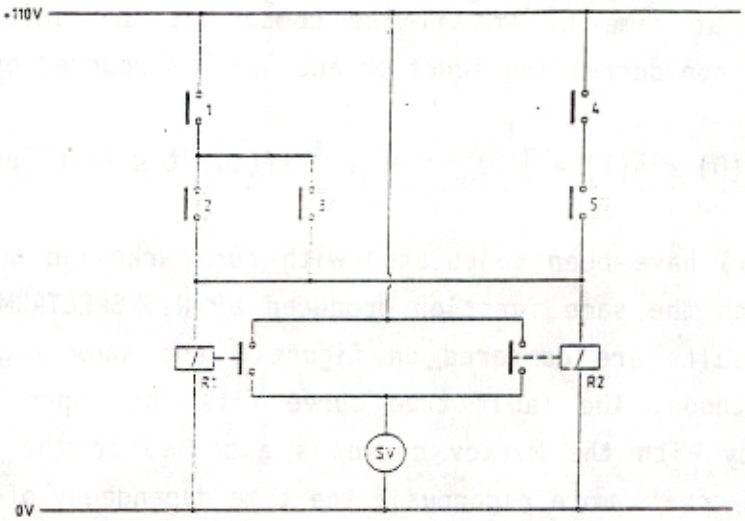


Figure 1 : control circuit of the ABV closure

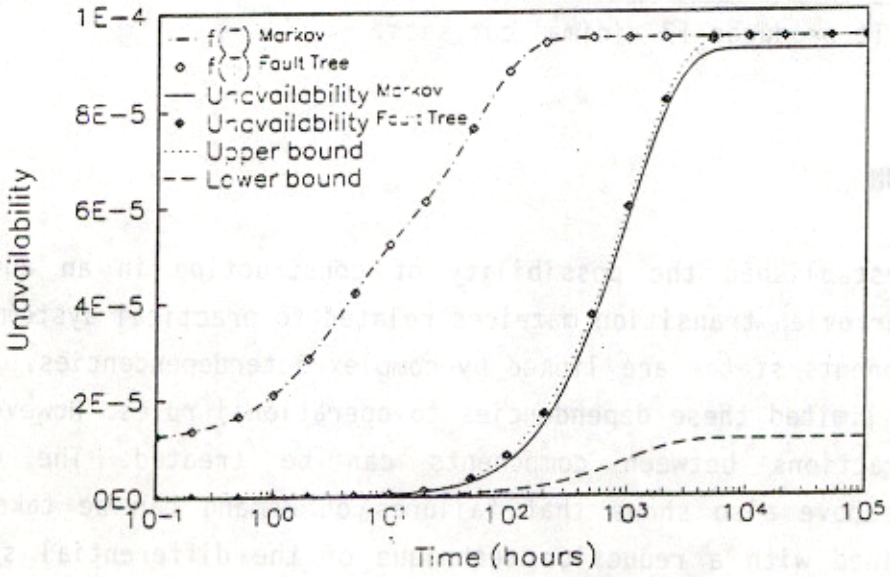


Figure 2 : unavailability and failure on demand

MARKOVIAN MODELS FOR THE RELIABILITY ANALYSIS OF MULTICHANNEL PROTECTIVE SYSTEMS

P. F. Frutuoso e Melo[1], L. F. Oliveira[2], and R. Youngblood[3]

[1]COPPE/UFRJ - Nuclear, Caixa Postal 68509, 21945-970
Rio de Janeiro, RJ, Brasil
[2]Principia Ltda. and Universidade Federal da Bahia, Salvador, Brasil,
Fax (55-71) 231-5332
[3]Brookhaven National Laboratory, Department of Nuclear Energy,
Bldg 130, Upton, Long Island, NY 11973, USA

INTRODUCTION

Our purpose is to present the results of Markovian models we have been developing so far for the reliability analysis of multichanneled protective systems considering higher configurations and new assumptions. Previous published papers consider the cases for one and two channels and the influence of the channel repair rate and also general expressions not considering the influence of the latter on the plant hazard rate[1-3].

Modeled here is the possibility of compairing between two criteria that are of practical concern: for a k-out-of-N: F logic, the system is able to reveal the failure of at least k failed channels; as an option, we consider the possibility of revealing the failure of a single channel only. Two new features taken into account are: the consideration of the effective time instead of the calendar time for evaluating the plant hazard rate, and the modeling of common cause failures by the α model[4].

GENERAL FEATURES OF THE MODELS

An important improvement over previous models[2,3] refers to the calendar time consideration instead of the effective one when calculating the plant hazard rate.

This problem is related to the fact that for evaluating the system mean unavailability it has been common practice to consider the calendar time; this means that even the residence times on those states for which failures have been revealed are taken into account when calculating the plant hazard rate.

Once the revealed failure states are identified the departure rate for each of them is evaluated[5]. This overall departure rate is the sum of all of its departure rates. Next,

the state residence time is evaluated as:

$$\tau_i^* = \frac{1}{\lambda_d}, \tag{1}$$

where λ_d is the sum of the state departure rates. Finally, the accident rate η is:

$$\eta = \sum \frac{1}{\theta - \tau_i^*} \int_0^\theta p_i(t)dt, \tag{2}$$

where θ is the proof test interval and $p_i(t)$ is the probability of being in the ith state at time t and the summation is taken over all failed states and i spans the revealed failure states.

The estimators used in the α model are based on failure event information and they explicitly take into account the dependency among the parameters that originate from the use of a common failure data bank. The characteristics mentioned allow for a more precise representation of the associated uncertainties.

Besides, less parameters need to be multiplied for obtaining the frequency of a basic event for the α model as compared to other ones. This reduces the impact of underestimating the uncertainties associated with the multiplication of dependent random variables.

FIRST MARKOVIAN MODEL: FAILURE OF A SINGLE CHANNEL REVEALED

We will assume that the protective system is subject to a *k*-out-of-*5*: *F* logic. Each channel may be in one of the following states: functioning; unrevealed failure; or revealed failure. As was the case in earlier calculations[3], the distinction between the two failures above aims at taking into account the possibility of considering higher demand rates for they have important practical implications as, for example, in the petrochemical industry[6,7].

Table 1 summarizes the codes employed for characterizing the model possibilities. For convenience purposes, the set of failed states is split into two: the first contains the revealed failure states and the other one the system unrevealed failure states.

An important feature of this model is the possibility of analysing the influence of detecting the failure of a single channel. This case has already been modeled[3]. We have extended this treatment by considering higher failure logics (Figure 1). The symbology employed therein is explained as follows. Each system state is assigned a triplet $<i, j, k>$, where i stands for the number or working channels, j for the number of unrevealed failure channels and k for the number of revealed failure channels. λ, μ, and ν stand for the failure rate, repair rate and demand rate, respectively. γ stands for the channel repair efficiency, being considered as a human error free maintenance action probability. The number displayed over the triplet is the state number.

Shown in the dashed rectangle in Figure 1 are the revealed failure states for the configuration at hand. Note that the set of failed states is {4, 5, 6, 7, 8, 9, 10}. Partial common cause failure transitions are considered as, for example, that from state 1 to state 4, where the transition rate $3\lambda_2$ takes into account that there are three possibilities of double failures. Three repairmen are assumed available. Note also that the transition from state 9 to state 10 is possible when considering the *QAR* model only.

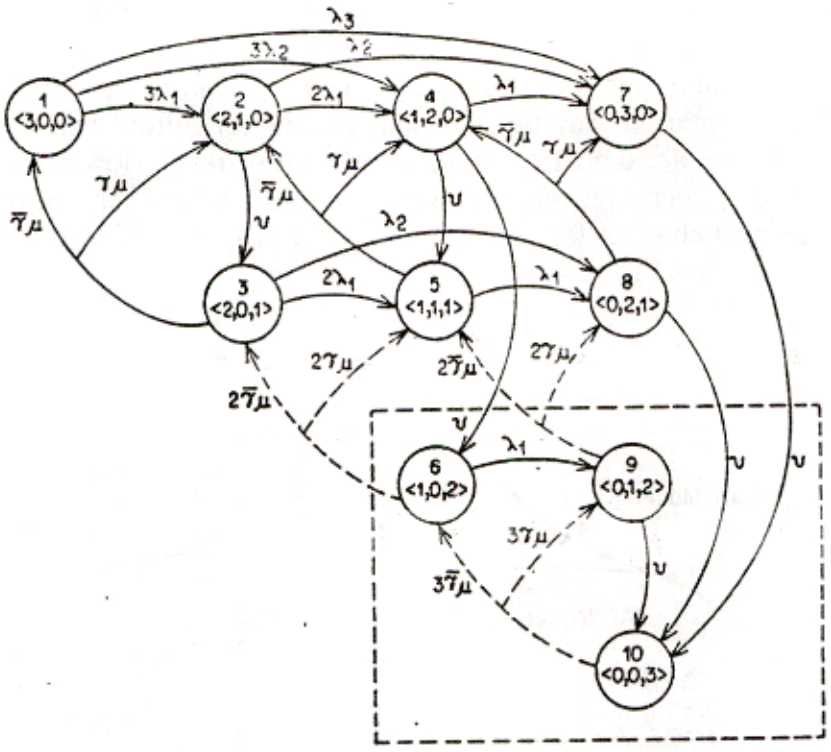


Figure 1 - Transition Diagram for the Three-Channel System Subject to the 2-3: F Logic

Table 1 - Codes Employed for Describing the Models Developed in Terms of the Repair Policies and Failure Status

CODE	EXPLANATION
Q	On line repair allowed
F	No on line repair allowed
A	Repair performed under accident condition
N	Repair under accident condition not allowed
R	Failure of a single channel revealed by a demand
U	Failure of a single channel not revealed by a demand

SECOND MARKOVIAN MODEL: AT LEAST K CHANNEL FAILURES REVEALED

Let us consider again Figure 1. For the assumed logic, only the failure of at least 2 channels will be revealed. This means that the dashed transition from state 1 to 3 is impossible here. Consequently, repair from state 3 is not allowed. A different feature of this model is related to the repairmen available and the repair policy. As long as only the failure of at least two channels is revealed, repair is initiated only when the system is in one of the states for which at least two channels are failed.

RESULTS OBTAINED

Let us consider the typical 2-out-of-3: *F* protective system for which the state transition diagram was shown in Figure 1.

Figure 2 displays the results of the comparison between the *QAR* and the *FAR* models. Significant differences are noticed only for demand rates higher than about 30 per year. Figure 3 presents the results concerning the influence of the repair rate on the accident rate. The upper curve considers a channel failure rate of 10 per year and the lower, of 1 per year. It may be seen that the higher failure rate produces a less sensible effect on the accident frequency as compared to the lower failure rate. For lower failure rates, η decreases more strongly due to the higher repair rate of the failed channels before new channel failures that can lead to system failure may occur.

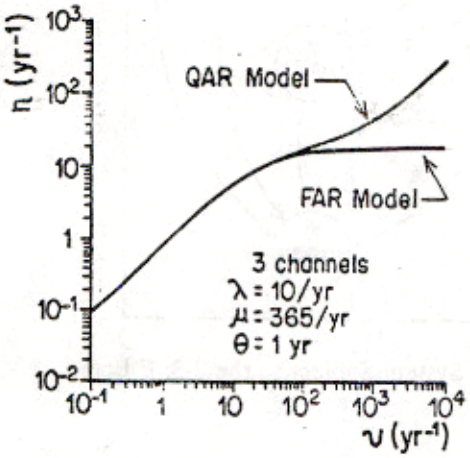


Figure 2 – Comparison between Models QAR and FAR.

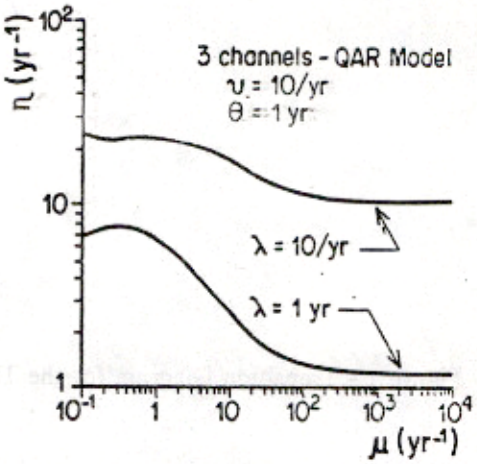


Figure 3 – Accident Rate Versus Repair Rate for the QAR Model.

Figure 4 presents the results of the comparison between the repair models *QAR* and *QAU*. It may be seen that both models furnish almost the same results with no significant differences due to the failure logic considered for the difference between them is related to revealing the failure of at least one channel (for the first) or at least two channel failures (for the second one).

The influence of common cause failures as modeled by the α model may be seen in Figure 5 for the *QAR* model. The α vector displayed means that for the upper curve, for example, 60% of the system failures are due to single failures, 20% to double common cause failures and the remaining 20% to triple common cause failures. It may be inferred from the figure that the effect of common cause failures is worthy considering for higher demand rates only (ν > 10 per year).

The time correction has been analysed for this configuration in order to check its influence. Figure 6 displays the results obtained. It may be seen that for lower demand rates no sensible effect is observed. Two curves were generated: the upper considered a lower repair rate of 52 per year and the lower one, a higher repair rate of 8760 per year. However, even for demand rates as high as 1,000 per year, no sensible effects have been observed on the accident frequency due to the time correction.

Finally, as the α model allows for considering partial common cause failures we

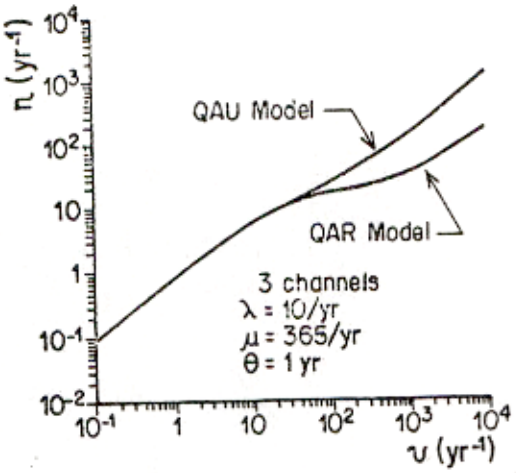


Figure 4 – Comparison between Models QAR and QAU.

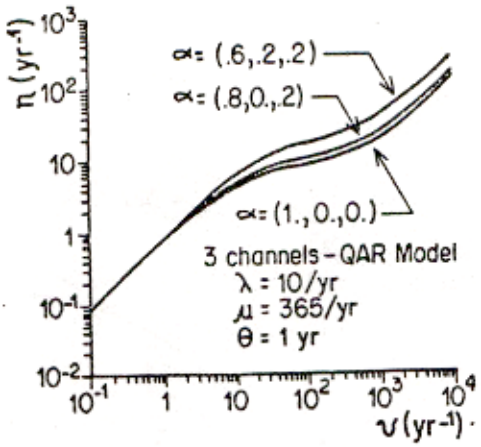


Figure 5 – Influence of Common Cause Failures on the Accident Rate.

have compared the results considering that no partial common cause failures are possible [by taking α = (.6, 0., .4)] to the alternative situation where partial common cause failures are taken into account [by taking α = (.6, .2, .2)]. Figure 7 displays the results obtained for the *QAR* and the *FAR* models. In this case the only partial failure possibility would be that of two channels. For this reason, the observed effect is almost neglibible. Even for a demand rate as high as 10,000 per year the difference observed for the first repair model is about 11. Once more it may be noticed that for lower demand rates no sensible effect is observed.

CONCLUSIONS

The generalization of previous Markovian models for treating higher logic configurations has shown that a general pattern may be observed. Explicitly, it may be concluded that for lower demand rates (tipically less than 10 per year) found in nuclear power plants, the effects of all the parameters studied may be neglected. However, in petrochemical plants, for example, where much higher demand rates can be found and where the number and type of protective systems are considerably higher these effects must necessarily be taken into account.

Initially, the effect of the demand rate both on the unavailability of the protective systems and on the accident rate must be clearly taken into account. Next, one should assess the effect of the repair rate on the accident rate.

An important feature is the consideration of the number of failures revealed by a system demand. We have seen that this feature is dependent on the system logic configuration. The system behavior from the point of view of common cause failures is not new. The point worth mentioning is related to the flexibility of the α model when considered in Markovian reliability modeling.

Also the accident rate behavior concerning the repair efficiency has shown that even for the typical situations found in petrochemical facilities, no sensible effect has been observed. Lower efficiencies would be observed under accident condition but no

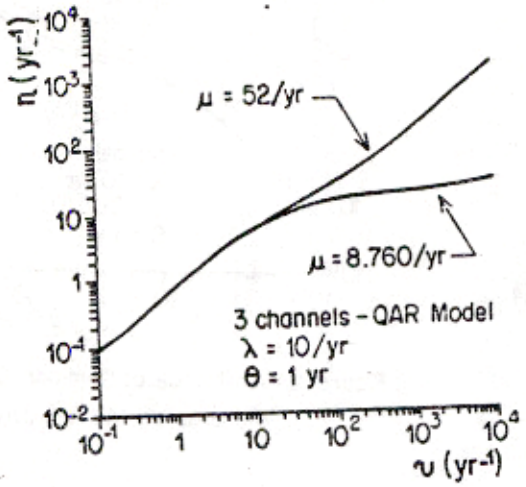


Figure 6 - Time Correction Considering the QAR Model.

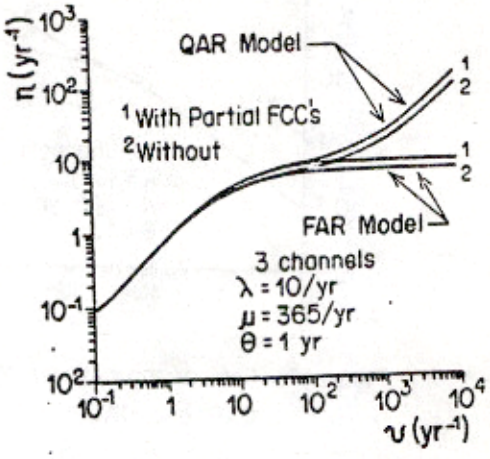


Figure 7 - Influence of Common Cause Failures.

repair actions are normally taken in this situation.

A final aspect analysed is related to the time correction. For all the cases that have been considered its effect on the accident rate has not been sensible enough.

REFERENCES

1. F. P. Lees. A General Relation for the Reliability of a Single-Channel Trip System, *Reliability Engineering*, 3:1 (1982).
2. L. F. Oliveira and J. D. Amaral Netto. Influence of the Demand Rate and Repair Rate on the Reliability of a Single-Channeled Protective System. *Reliability Engineering*, 17:267 (1987).
3. L. F. Oliveira, R. Youngblood, and P. F. Frutuoso e Melo. Hazard Rate of a Plant Equipped with a Two-Channel Protective System Subject to a High Demand Rate. *Reliability Engineering and System Safety*, 28:35 (1990).
4. A. Mosleh and N. Siu. A Multi-parameter Common Cause Failure Model. *Transactions of the 9th Structural Mechanics in Reactor Technology (SMiRT) Conference*, Lausanne, Switzerland, paper M7/3, p. 147 (1987).
5. C. Singh and R. Billinton. "System Reliability Modelling and Evaluation", Hutchinson of London, 1977.
6. H. G. Lawley and T. Kletz. High-Pressure Trip Systems for Vessel Protection. *Chemical Engineering*, 82:81 (1975).
7. G. L. Wells. "Safety in Process Plant Design". George Godwin Limited, London (1980).

019 Risk Management for Continuous Releases of Airborne Toxics

Chair: W.E. Kastenberg, UCLA

California's Air Toxics "Hot Spots" Law. I. Mechanics of the Law
J.F. Collins, M.A. Marty, , G.V. Alexeeff (Of. Environ. Hlth. Haz. Assmt.)

Uncertainties in the Health Risk Assessment of Fossil-Fueled Electric Power Stations
L.B. Gratt (IWG)

Automated Risk Assessment for California's Air Toxics Hot Spots Act
J.H. Stuhmiller (JAYCOR)

CALIFORNIA'S AIR TOXICS "HOT SPOTS" LAW. I. MECHANICS OF THE LAW

James F. Collins, Melanie A. Marty, and George V. Alexeeff

Office of Environmental Health Hazard Assessment
California Environmental Protection Agency
2151 Berkeley Way, Annex 11
Berkeley, CA 94704

INTRODUCTION

As an outgrowth of community right-to-know legislation and in response to public concern about industrial emissions and hazardous waste sites, California enacted the Air Toxics Hot Spots Information and Assessment Act of 1987. The law requires industrial facilities to quantify their routine air emissions of designated chemicals, to perform a risk assessment if the emissions warrant one, and to notify the public if the risks are deemed significant.

IMPLEMENTATION WORK BY PUBLIC AGENCIES

The agencies involved in implementation included the Air Resources Board (ARB) and the Office of Environmental Health Hazard Assessment (OEHHA) and the local Air Quality Management Districts (AQMD) and Air Pollution Control Districts (APCD) plus the Districts' umbrella organization, the California Air Pollution Control Officers Association (CAPCOA). One of the first tasks was the identification of chemicals to be inventoried. The law required that certain existing lists, including chemicals identified as toxic air contaminants in California and chemicals listed under Proposition 65, be used.

GUIDELINES FOR EMISSIONS INVENTORIES

A facility is subject to the Air Toxics Hot Spots Act if it manufactures, formulates, uses, or releases one or more of over 700 listed substances and emits (10 tons or more per year of) total organic gases (precursors of ozone formation), particulate matter, nitrogen oxides, or sulfur oxides. Currently, approximately 700 substances must be reported and emissions of approximately 400 must be quantified. The Act requires such a facility to prepare air toxics emission

inventory reports according to ARB-adopted Emissions Inventory Criteria and Regulations. A facility operator must submit to the local air district a proposed emission plan indicating the methods to be used to measure, model, and/or estimate the emissions of subject chemicals from identified locations. After district approval of the plan, the facility quantify the emissions and submit the report to the district. Possible sources of emissions include: point sources (e.g., stacks), fugitive emissions (e.g., flanges, valves, non-ducted operations), and area sources (e. g., landfills). Under the first phase of the program, approximately 3,400 facilities were required to report emissions. Of those, approximately 730 were required to prepare a risk assessment.

GUIDELINES FOR PRIORITIZATION OF FACILITIES

The air districts use the information on emissions, other data such as the potency and toxicity of the emitted substances, and the facility's proximity to potential receptors to prioritize facilities into high, medium, and low priority categories. The ARB worked with CAPCOA, OEHHA, and the air districts to develop a numerical scoring system based on amounts of emissions, cancer potency (for carcinogens) or reference exposure level (for non-carcinogens), and distance from facility to receptor. Details of the scoring system were published by CAPCOA as a guideline[1]. For carcinogens, the facility score is obtained by multiplying the amount of material emitted by its potency and a receptor proximity factor, then summing the results for all emitted carcinogens. For noncarcinogens, the score is determined by the ratio of emissions to reference ("safe") exposure concentrations. Based on the emissions inventory, facilities are prioritized by the local air districts into high, medium, and low priority using the prioritization guidelines prepared by district and ARB staff. Facilities emitting more than 25 tons per year of criteria pollutants and designated high priority were required to conduct a health risk assessment during 1991.

GUIDELINES FOR RISK ASSESSMENT

Guidelines for risk assessment were developed by a committee composed of CAPCOA, ARB, and OEHHA staff[2]. Cancer potency values and reference doses or concentrations for use in the Hot Spots program were compiled by OEHHA staff. For many chemicals, USEPA or California cancer potency values were not available. Instead of allowing affected facilities to develop values, OEHHA staff determined as many as possible so that all facilities would be using the same values. For carcinogenic oral potencies and inhalation unit risks, staff first compiled existing, peer-reviewed numbers, such as those for chemicals identified as toxic air contaminants in California and those for chemicals in the USEPA's Integrated Risk Information System (IRIS) database. Peer-reviewed values developed by the California Department of Health Services for the purposes of deriving drinking water standards or for implementing Proposition 65 and potency factors in USEPA's Health Effects Assessment Summary Tables (HEAST) were also used. Finally, values were derived by applying the linearized multistage model to data sets found

in the literature including the TD50 database. These last values were designated screening values which individual air districts could use at their option because there was not time available for extensive peer review.

Reference exposure levels for chronic exposure to noncarcinogens were obtained from the IRIS database listing of RfDs (references doses) and RfCs (reference concentrations), from USEPA's HEAST, from the USEPA's Superfund Public Health Evaluation Manual, or by applying an uncertainty factor of 420 to a workplace Threshold Limit Value (TLV). Where only an oral value (e.g., an RfD) was available, an equivalent inhalation concentration was obtained where appropriate by assuming that a 70 kg person breathes 20 m^3 of air per day and that absorption is similar by the two routes.

For a few chemicals, one hour acute reference ("acceptable") exposure levels, developed under a contract from the USEPA, were provided. Some acute exposure values were obtained by dividing the TLV by 100. The paucity of reliable numbers for assessing the effects of acute exposure is unfortunate since such exposures can pose imminent danger. However, imminent danger is considered unlikely for routine emissions assessed in the Hot Spots program. Work continues at OEHHA to develop chronic and acute reference exposure levels for a large number of compounds.

RISK ASSESSMENT

Facilities designated high priority are required to complete a health risk assessment to determine if their emissions pose a high risk. Air modelling is used to determine the ground level concentration (GLC) of emitted chemicals at receptors near the facility including the Maximally Exposed Individual (MEI, the offsite location with the highest individual risk where a person could have a residence) and sensitive receptors such as people in nursing homes and day care centers. From the GLCs and cancer inhalation unit risk factors, the individual cancer risk due to inhalation is determined. In addition, noninhalation exposure routes including soil ingestion, meat and dairy product ingestion, backyard crop ingestion, surface water ingestion, mother's milk, fish ingestion, and dermal exposure to contaminated soils are assessed. For noncancer health risk, substances are evaluated to determine if they exceed an "acceptable" or "safe" reference exposure level (REL). The ratio of the modelled GLC (or dose for noninhalation routes) to the REL is the hazard index (HI) for a single substance. For a mixture of substances that affect the same target organ, the individual HIs are summed to yield a total hazard index (THI) for that target organ. Calculation of these indices is described in the Risk Assessment Guidelines.

Risk assessments are submitted to the air districts which review them for appropriateness of the air modeling. The reports are then sent to OEHHA to review the health effects. Based on the results of the risk assessment, the District determines if there is a significant risk to the public resulting from the facility's emissions. If such a determination is made, the facility operator is required to notify those exposed of the results of the risk assessment and to implement a risk reduction plan.

RISK COMMUNICATION

The facility operator must provide notice to all exposed persons, if the air district finds that there is a "significant health risk" attributable to the emissions from the facility. The primary goal of notification under the Air Toxics "Hot Spots" Program is to inform the public of exposure to toxic substances routinely released to the air from facilities and the potential health risks associated with those exposures. Notification also establishes a mechanism to address the public's questions concerning exposure and health risk associated with a facility's emissions.

To assist local districts with notification issues, Public Notification Guidelines[3] were developed. The Guidelines discuss specific notification procedures and provide guidance on the use of notification materials and suggestions for presenting information. Generally the notification consists of letters sent to homes and businesses in the community. The letters may lead to questions that must be addressed. Many districts also require a public meeting to address the public's questions. A public meeting also allows facility and district representatives to present the risk assessment results in more detail and to discuss activities related to reducing emissions of toxic substances.

Although the law does not define significant health risk, most air districts are concerned about individual lifetime cancer risks totaled across all carcinogenic emissions above 10^{-5}. For the majority of substances evaluated under the Air Toxics Hot Spots Program, OEHHA has specified that an HI of one or less is an indicator that adverse health effects are not likely to occur, even in sensitive individuals. Thus most Districts have decided that notification would only be required if a facility exceeded an HI or a THI of at least one.

In 1992, the first 11 facilities, all in the San Francisco Bay Area, provided notification to the public under the Air Toxics "Hot Spots" Program (Dr. Pat Holmes, personal communication). These facilities included three dry cleaners, two petroleum refineries, a naval air station, a cement plant, a sugar refinery, a water treatment plant, a chemical manufacturer, and a foundry. Nine additional facilities, originally targeted for notification by the Bay Area AQMD, either reduced or planned to reduce their risk to below the district notification threshold through the installation of pollution control equipment or through process shutdowns or modifications. Among these facilities were six dry cleaners, a hospital, a bulk loading plant, and a university. For these facilities, the desire to avoid public notification served as an incentive to reduce emissions of air toxics. While OEHHA would have recommended public notification, the local air districts have final say in risk communication.

Somewhat surprisingly the largest calculated risks have not always come from large industries like oil refineries but from smaller facilities located close to or in residential areas such as dry cleaners (sources of perchloroethylene) and chrome platers (sources of hexavalent chromium). Dry cleaners often emit from a roof top vent and also have large

fugitive emissions. They are often located in one story buildings surrounded by homes and apartments which decrease air turnover. Many dry cleaners have apartments directly above them.

Similar situations exist for chrome plating and auto body finishing operations. They emit hexavalent chromium through roof top vents in residential areas creating localized, high GLCs, resulting in high calculated cancer risks to people in adjacent residences.

Many facilities are choosing to reduce emissions rather than become involved in health warnings which are considered bad publicity. This may involve changing to a process which decreases emissions or installing best available control technology (BACT). In all probability many facilities will be required to install BACT due either to California's Toxic Air Contaminant program or the 1990 federal Clean Air Act Amendments. In addition, if a company can reduce its emissions and keep them reduced, it may apply for a change in its air permit. It may then be eligible for a reduction in air pollution permit fees which are based on amounts of pollutants emitted or entitled for emission credits which it can sell to other companies.

CONTROVERSIES AND ISSUES

Since the act requires preparation of risk assessments, many controversies have arisen. Several are discussed below.

Although hundreds of chemicals have been classified as carcinogens, values for quantitative risk assessment are available for only a fraction of them. IARC considers at least 245 chemicals or mixtures to be carcinogens[4]. The USEPA essentially agrees with IARC. The USEPA has verified cancer potency values for only about 60 chemicals on its IRIS database. Thus OEHHA was faced with a list of chemicals for which unit risk numbers were either preliminary or non-existent. Several values were derived by standard procedures while others were derived using the TD50 database.

Two unresolved controversies about potency are the relative potencies of polycyclic aromatic hydrocarbons (PAHs) and the potency of crystalline silica. As an initial approach, all carcinogenic PAHs were assumed to be as carcinogenic as benzo(a)pyrene (BaP). While evidence exists that nearly all carcinogenic PAHs, except dibenz(ah)anthracene, are less carcinogenic than BaP, neither USEPA nor OEHHA has accepted a relative weighting scheme for PAH carcinogenicity. An OEHHA-generated weighting scheme is currently undergoing external review.

The screening unit risk value for respirable, crystalline silica has generated concern because of the environmental concentrations of silica near quarries and mines. IARC has identified crystalline silica as a carcinogen based on studies in rats that have shown that chronic inhalation of crystalline silica leads to lung tumors. Workers who develop silicosis may be more likely to also develop lung cancer. The rat studies were used to derive an inhalation unit risk number for silica using standard methods. Using the number, some facilities had theoretical cancer risks due to silica greater than 10^{-3}. On the other hand, hamsters have not developed lung tumors after intratracheal administration or inhalation of silica. It is

possible that the workers with silicosis develop cancer only secondary to lung cell death.

The estimation of human exposure to air toxics is also subject to controversy. Because of the developing nature of risk assessment and the variety of environmental media and transport processes considered, numerical values for many exposure parameters are not well established. Thus values are chosen which will protect public health (default values). Such values are often called conservative by some who consider them to be excessively cautious. The values are continually scrutinized and some have been altered to take into account new information.

A much more global controversy is the uncertainty involved in risk assessment. This controversy was acknowledged and addressed in the Guidelines. After risks were determined by the CAPCOA methods so that all facilities could be compared, facilities could use other assumptions and approaches to estimate risk. They were not allowed to vary the potency numbers and reference concentrations, but could change various exposure parameters. As a result of further legislation, the uncertainty in health risk assessment must be formally addressed in the Hot Spots program. In addition the Guidelines will be subject to public review and comment before formal adoption by OEHHA.

CONCLUSION

Public concern about adverse effects of air emissions from industrial facilities is relatively high. The Air Toxics Hot Spots Act provides the state with a large database to support prioritization of resources directed at reducing airborne risks. In addition the Act functions as a community right-to-know law, providing the public with information on chemical emissions into their communities. Emissions reductions have reportedly taken place because of the Act. Facilities have become more knowledgeable about their emissions and, faced with the prospect of public notification, many are reducing emissions voluntarily. In addition, newly chaptered legislation in 1993 is requiring high risk facilities to phase in emissions reductions.

REFERENCES

1. CAPCOA (California Air Pollution Control Officers Association). "Air Toxics "Hot Spots" Program Facility Prioritization Guidelines." CAPCOA, Cameron Park, CA (1990).

2. CAPCOA. "Air Toxics "Hot Spots" Program Risk Assessment Guidelines." CAPCOA, Cameron Park, CA. (1990) Updated January 1991, January 1992, and September 1993.

3. CAPCOA. "Air Toxics "Hot Spots" Program. Public Notification Guidelines." CAPCOA, Cameron Park, CA (1992).

4. International Agency for Research on Cancer (IARC). "IARC Monographs on the Evaluation of Carcinogenic Risk of Chemicals to Humans. Supplement 7." IARC, Lyon, France (1987).

UNCERTAINTIES IN THE HEALTH RISK ASSESSMENT OF FOSSIL-FUELED ELECTRIC POWER STATIONS

Lawrence B. Gratt

IWG Corp.
1940 Fifth Avenue
Suite 200
San Diego, CA 92101

INTRODUCTION

The risk assessment process as applied to fossil-fueled electrical power generating stations is analyzed to understand the impact of assumptions and data choices. The purpose of this analysis is to separate the assessment process into emissions, dispersion, exposure and dose-response phases and examine the relative changes in the uncertainty of each of these phases based on recent measurement and analysis programs.

BACKGROUND

Health risk assessment results contain significant uncertainties that are not adequately addressed in regulatory risk assessments. Previous estimates of the uncertainty of the risk estimates were very large and dominated by the dose-response phase.[1] Simplified regulatory risk estimates contain "upper bound" values that obscure the uncertainty. Risk assessments of electric power generating stations present concerns for global impact as well as human health impacts.[2] Health impacts are generally categorized into carcinogenic and non-carcinogenic categories. In general, the carcinogenic chemical emissions dominate the impacts. Review of carcinogen risk assessment guidelines resulted in recommendations[3] that included the following:

> "The risk assessment should include a best estimate based on the *totality* of the available data and the *uncertainty* in the data and its quality. This estimate should describe the likelihood that different values within the range of uncertainty represent measurable effects."

and

> "Make uncertainty explicit in every state of the risk assessment process."

Since the risk assessment of power stations has been the subject of much research and analysis over the past 15 years, the impact of improved measurements, models and assumptions can be examined within the framework of defining research needs. The contribution of various carcinogenic substances to the total cancer risk as a function of fuel (oil, coal or gas) has been investigated using regulatory risk assessment guidelines.[4]

The Electric Power Research Institute's (EPRI) PISCES Program is currently establishing a database for fossil-fuel power station hazardous air emissions based on fuel, process, and stack measurements.[5] The results of this program, along with a similar Department of Energy testing program, will allow for a needed revision of the previous database for fossil fuels[6] compiled about a decade ago. Other analyses have investigated the emissions from fossil fueled power stations, dispersion parameters, chemicals used as carcinogens, and dose-response issues[7,8] as well as the use of higher order models.[9] A cancer risk analysis based on emission factors from the initial PISCES field results, supplemented with previous literature citations subjected to quality evaluations can be compared to previous risk evaluations for US power stations with units greater than 25 MWe capacity.

FORMULATION

Health risk assessments predict the concentration of compounds emitted from a facility into the environment, and the resulting risk to human health. Risk measures are based on the individual and population-wide health effects associated with exposure. The air toxic risk, in a random variable formulation, is as follows:

$$p(r) = p(s,d,e,h) \tag{1}$$

where p(r) is the probability density function of the risk, s is the source term (toxic air emission), d is the dispersion of the emission source into the environment resulting in ambient concentrations, e is the exposure of human in the ambient air resulting in a dose to target organs that is converted to a health impact through a dose-response function using h. Using the previous definition of risk and assuming separation of variables and use of conditional probabilities, the expected value of the risk can be written as:

$$\langle r \rangle = \int_{\text{all } s,d,h,e} \int\int\int\int h\, p(s)\, p(d(s))\, p(e(d))\, p(h/e)\, ds\, dd\, dh\, de \tag{2}$$

where p(h/e) is the conditional probability of the health effect given exposure e.

Numerous assumptions are needed to obtain a simple form for calculations of point estimates of the risk. An example of a simple form used in inhalation risk computations is

$$\langle r \rangle = \sum_{\text{all } c} Q_c\, (\chi/Q)_{max}\, U_c\, MP_c \tag{3}$$

where Q_c is the emission rate of chemical c (mass per unit time), $(\chi/Q)_{max}$ is the result from the dispersion model that converts the source emission rate (mass per unit time) to the maximum concentration (mass per unit volume) over the receptor grid. U_c is the Unit Risk Factor for the individual excess lifetime cancer probability (units of LCP per concentration) and MP_c is the multipathway factor for chemical c to account for non-inhalation pathways. For many chemicals MP ≡ 1, and is of little concern. For other chemicals MP>>1 and must be taken into account when evaluating the health risk.[10] Note that Equation (3) is a very simplified approximation of Equation (2), which represents the desired form for the point estimate of the random variable of concern. The simplifying assumptions to obtain the computational form of Equation (3) used in regulatory settings use "upper bound" values which obscure the uncertainty.

The compounding use of bounding values in the regulatory approach is an attempt to compensate for large uncertainties in the risk assessment process, but may lead to cost-ineffective risk management decisions. In this analysis, potential benefits of measured data for emissions is investigated.

POWER STATION EMISSIONS

POWER STATION EMISSIONS

The first term in the right-side of Equation (3) is the emission rate for each substance (or chemical designated by the subscript c) of concern for the power station. The number of chemicals of concern continues to increase with analytical capabilities and increases the uncertainty in the risk estimate. The emission rates for this study were calculated using currently available emission factors supplemented by literature values. The coal stations studied have been divided into categories based on fuel type (e.g., bituminous), particulate control system and flue gas control system. The oil stations are divided into two categories, uncontrolled and controlled. The natural gas-fired stations have been analyzed using available emission factors and recent measurements. To simplify this analysis, stations using mixed fuels (e.g., units burning coal and oil) were classified by the majority fuel and assumed to use 100% of that fuel.

The emission rates for each chemical (Q_c) are used with the power generation requirements, P, fuel heating value, HHV, and relative control efficiencies to estimate the specific power station emissions (lb/y). This estimate is made using Equation (4),

$$Q_c(lb/y) = EF_c \cdot \frac{(1\text{-}CE)}{(1\text{-}CE_o)} \cdot \frac{(HHV_o)}{(HHV)} \cdot P \qquad (4)$$

where EF_c is the available chemical-specific emission factor for the reference fuel, CE is the station control efficiency, CE_o is the reference control efficiency, HHV is the higher heating value of the fuel, HHV_o is the reference higher heating value , and P is the total thermal energy rate (Btu/y) required to generate the annual electrical power level for year 1989. In general, the differently fueled plants have been used to satisfy different load conditions. For 602 US generating sites, the coal station (401) runs at a higher load (58%) as compared to oil (54) and gas (147) stations (38% and 33%, respectively.).

The uncertainty in the emissions factors can be analyzed based on the variance of the measurements for specific sites where measurement programs have been conducted. These measurement programs do not cover the full realm of operating and environmental conditions as well as fuel variations that may occur over a 30-year plus operational period. However, using fuel data and models, the emissions can be estimated using available data as log normally distributed with a standard deviation approximated by 2 or 3 times the sample mean. The uncertainty in the operation of control system presents a much greater potential for changes in the emission rate. If a control system is specified to operate at 99% removal efficiency but measured data show it functions at a 99.8% level, the emission rate is reduced by a factor of 5. On the other hand, if the system (99%) is turned off only 1% of the time, the emission rate just about doubles.

Key issues for the emissions calculation are the content of substance in fuel, the firing and operation of the combustion units, and the control system performance. The impact of enrichment and particle size also presents significant uncertainties that are ignored in simplified approaches. Enrichment refers to the concentration of the pollutant in emitted ash being greater than that in the bulk fuel. Some trace metals have been observed to volatize during combustion and later condense on particulates, increasing the relative mass on the smaller size particles.

MAXIMUM CONCENTRATIONS

Atmospheric dispersion was calculated using ISC2[11] with meteorology at the nearest National Weather Service station reporting at least 5 years of data reduced to STAR (STability ARmy) format with site-dependent parameters. A 20 km by 20 km Cartesian grid centered on the stack at each generating station was the analysis domain. This grid was divided into 100 4-km^2 zones with one receptor at the center of each zone. Flat terrain and urban dispersion coefficients were used for all sites. These assumed conditions have a significant effect on the predicted ambient concentrations and on the resultant cancer risks. The calculations were carried out with all dispersion coefficients set to the ISC2 "Urban" mode. Many sites would be more appropriately modeled using the "Rural" mode. The Urban results are conservative (e.g., give larger concentrations). Previous efforts[1] indicate about an order of magnitude difference between the two coefficients.

EXPOSURE AND DOSE-RESPONSE

A key assumption of the exposure portion of a screening risk assessment is that there is an individual at the location of the maximum concentration in the study area who is exposed continuously for a 70-year lifetime. The greatest uncertainty in the risk assessment is represented by the dose-response term. The uncertainty in this portion of the risk assessment overwhelms most other terms, treated in a simplistic manner by use of a unit risk factor.[12]

The chemicals to be treated in the analysis yield different risk estimates and uncertainties. The unit risk factors for EPA assessments of power plants are different from those used in California, which include additional chemicals such as nickel, lead and selenium. For coal fuel, the EPA factors show arsenic as the dominant substance. At an assumed 5% hexavalent chromium fraction of total chromium, the California factors show hexavalent chromium as the overwhelming carcinogen due to a larger unit risk factor. For oil fuel, the role of nickel is of major significance when using the California approach, whereas EPA does not currently treat nickel combustion products as carcinogens.

Alternative approaches using low-dose extrapolation models[1] indicate the very conservative nature of unit risk factors. The choice of both the data set and model is critical in the low-dose extrapolation approach. Three data sets for arsenic risks differ only by factors of from 100 for the multihit model, to 10 million for the multistage model. The relative uncertainties in using these models may be much larger, but the estimates themselves would be much lower.

RESULTS AND UNCERTAINTIES

Results of using Equation (3) for oil- and gas-fueled power stations for improved emission estimates for 1989 power plant characteristics are illustrated and summarized in Table 1. The results for oil (Figure 1) indicate the distribution is becoming "flatter" or that the uncertainty may becoming larger. The mean risk has been decreased. There is a decrease in the larger risk stations and increase in the lowest risk stations. For gas stations, the recent measurements indicate a significant decrease in the risk distribution. Even with the addition of many chemicals (e.g., arsenic, beryllium, cadmium and hexavalent chromium), the improved emission factors decrease the already low overall risk from gas-fueled stations. The results for coal follow similar trends. The distribution of risk estimates that only a small number of stations will account for the majority of the health risk. The use of bounding results for emissions results in large risk estimates that may lead to cost-ineffective decisions (i.e., control systems added that may decrease the upper bounds risk, but could increase the actual risk).

Screening level risk assessment results using Equations (3) and (4) have little relevance to quantifying the uncertainties because maximum values have been used instead of best estimates. As more chemicals (c) and pathways (MP) enter into the risk calculations, the rise in regulatory estimates has only been checked by better measurements of the emissions. Improvements in the assessment methodology using best estimate approaches throughout each phase are needed for a better understanding of the uncertainty. Previous results for arsenic indicate the choice of dose-response model introduces greater variability than does the selection of data sets. Uncertainties due to data errors and statistical variations, as well as the preparation of uncertainty in the estimation procedure, are areas needing further research. Better methodologies can be employed for exposure estimation using available data.[13]

CONCLUSIONS AND RECOMMENDATIONS

A screening risk assessment for power stations indicates that the removal efficiency and chemicals to be treated in the risk assessment methodology are important risk assessment variables for further study. Emissions are most strongly related to the control efficiency achieved for particulates. Modeling of the dose-response relationship is a key uncertainty. Only a small number of power stations presenting significant risk levels are expected, allowing each of these sites to be examined in greater detail.

Table 1. Comparison of Risk Estimates for Power Stations

Fuel	Basis for Emissions	Maximum Excess Individual Lifetime Cancer Risk		
		Average	High	Low
Oil (147 Stations)	EPA (Mead)	4.3×10^{-8}	4.0×10^{-7}	1.7×10^{-10}
	Updated EPA	1.3×10^{-8}	2.0×10^{-7}	3.5×10^{-11}
Gas (54 Stations)	EPA	8.8×10^{-7}	8.5×10^{-6}	1.7×10^{-10}
	New	5.0×10^{-7}	4.5×10^{-6}	3.3×10^{-9}

Figure 1. Distribution of Risk from 54 Oil-Fueled Stations

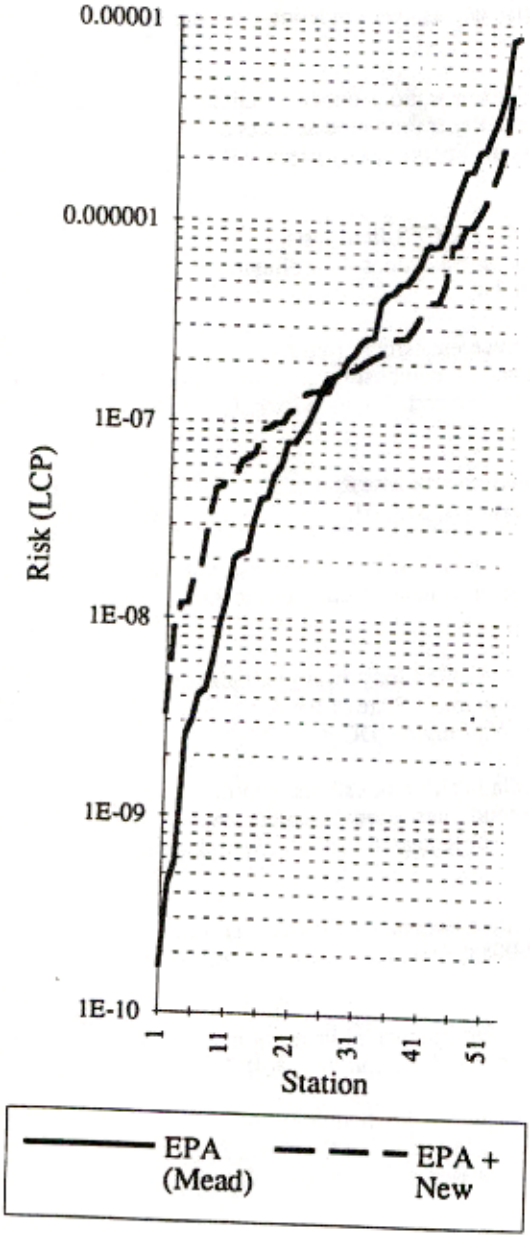
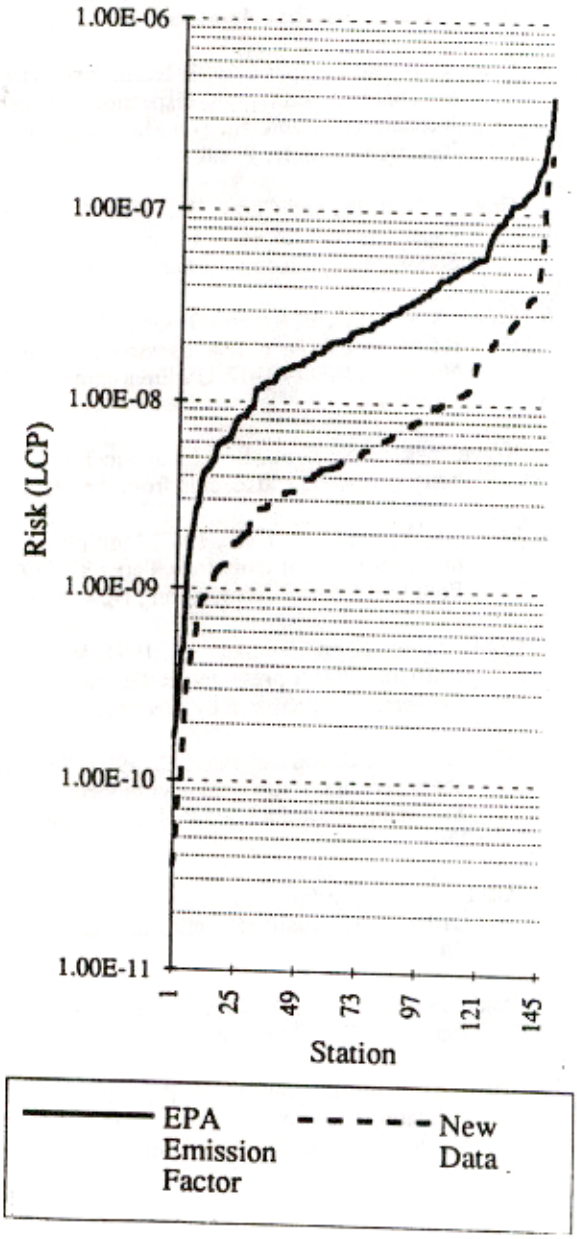


Figure 2. Distribution of Risk from 147 Gas-Fueled Stations



ACKNOWLEDGMENTS

This effort was performed under EPRI Research Project 3081-03 and under IWG Corp. provided support.

REFERENCES

1. Gratt, L. B., Levin, L. and Silvers, A., 1993, The role of arsenic emissions in power plant risk assessments: Uncertainties and research needs, Paper 93-TA-36A.01 presented at the 86th Annual Meeting of the Air & Waste Management Association, Denver, Colorado.

2. Chow, W. and Levin, L., 1993, EPRI research on hazardous air pollutants: An overview, Paper presented at Second International Conference on Managing Hazardous Air Pollutants, Sponsored by Electric Power Research Institute, Washington, DC.

3. Anderson, E., Deisler, Jr., P.F., McCallum, D, St. Hillaire, C., Spitzer, H.L., Strauss, H., Wilson, J.D., and Zimmerman, R., 1993, Key issues in carcinogen risk assessment guidelines, society for risk analysis, *Risk Analysis*, 13(4), 379.

4. Gratt, L. B. and Levin, L., 1993, Health risk assessment of utility power stations under different assumptions: Emissions, dispersion and dose-response models, Paper presented at Second International Conference on Managing Hazardous Air Pollutants, Sponsored by Electric Power Research Institute, Washington, DC.

5. Chu, P., Nott, B., and Chow, W., 1993, Results and issues from the PISCES field tests, Paper presented at Second International Conference on Managing Hazardous Air Pollutants, Sponsored by Electric Power Research Institute, Washington, DC.

6. Mead, R. C., Post, B. K., and Brooks, G. W., 1986, Summary of trace emissions from and recommendations of risk assessment methodologies for coal and oil combustion sources, Report No. 85-203-024-41-07, US Environmental Protection Agency, Research Triangle Park, North Carolina.

7. Kowalczyk, G. S., Gratt, L. B., and Ricci, P. F., 1987, An air emission risk assessment for benzo(a)pyrene and arsenic from the Mt. Tom Power Plant, *JAPCA*, 37, 361.

8. Perry, B. W. and Gratt, L. B., 1987, Multiple low-dose extrapolation models in cancer risk assessment of power plant air emissions, Paper 87-41.6 presented at the 80th Annual Meeting of the Air Pollution Control Association , New York City, New York.

9. Constantinou, E. and Seigneur, C., 1991, Multimedia health risk assessment for power plant air toxic emissions, Paper presented at the Managing Hazardous Air Pollutants: State of the Art Conference, Sponsored by Electric Power Research Institute, Washington, DC.

10. Constantinou, E. and Seigneur, C., 1993, Sensitivity of multimedia health risk estimates to the characteristics of the local environment, Paper presented at Second International Conference on Managing Hazardous Air Pollutants, Sponsored by Electric Power Research Institute, Washington, DC.

11. US EPA, 1992, *Industrial Source Complex (ISC2) Dispersion Models Volume I User Instructions*, Office of Air Quality Planning and Standards, EPA 450/4-92-008a, Research Triangle Park, North Carolina.

12. Anderson, E. L., and the Carcinogen Assessment Group of the US Environmental Protection Agency, 1983, Quantitative approaches in use to assess cancer risk, *Risk Analysis*, 3(4), 277.

13. Room, D., Kim, B., and Cohan, D., 1993, CORE project progress update: Methodology for estimating exposure to trace emissions, Paper presented at Second International Conference on Managing Hazardous Air Pollutants, Sponsored by Electric Power Research Institute, Washington, DC.

AUTOMATED RISK ASSESSMENT

FOR CALIFORNIA'S AIR TOXICS "HOT SPOTS" ACT

James H. Stuhmiller

Applied Technology & Commercial Systems
JAYCOR
San Diego, CA 92121

INTRODUCTION

California's Assembly Bill 2588 requires that facilities report emission inventories for all toxic substances. Those reports must be updated at least biennially. If the local Air Pollution Control District (APCD) determines that the release might constitute a significant risk, the facility must perform a health risk assessment that involves dispersion analysis based on local meteorology and a multipath risk assessment based on the local population density and land use. The results must be presented graphically on maps of the surrounding area and made available for public inspection. If the results of that risk assessment indicate that a section of the population is exposed to a significant risk, then the affected individuals must be notified directly by mail. Subsequent state legislation requires that the facility adopt a program to reduce the risk to acceptable levels over a period of time.

The implementation of this Act has been very difficult for the State, the Districts, and the facilities. The complexity of the prioritizing, dispersion modeling, and risk analysis has been so overwhelming that facilities have had to turn to outside consultants, at significant cost, to make the submissions. To minimize these costs, facilities do not normally make repeated analyses to determine the optimum operating solution and instead often accept a less than optimal control retrofit. The Districts are overwhelmed by the sheer magnitude of the submissions and are unable to check thoroughly the emissions data or the risk analyses. Finally, the State, which is charged with reviewing the analyses and determining if "hot spots" exist, is also overwhelmed by the size and complexity of the undertaking.

JAYCOR has developed a computer assisted system for streamlining the AB2588 inventory, screening, analysis, and reporting. STAAR (System for Tracking, Analysis, Administration, and Reporting) allows inventory data to be entered, updated, totaled, and reported. The facility can try alternative operating scenarios, control strategies, or product mix. A prioritization calculation can be made to estimate the seriousness of the emissions. If warranted, a meteorological dispersion analysis using SCREEN or ISCST can be run, with the program automatically setting up the input from the database. The dispersion effects can be determined on a grid of points, for the purposes of providing contour plots

and locating maximum exposed individuals, or at the location of "sensitive receptors", such as hospitals, schools, etc. The results of the health risk assessments are reported and areas of high risk highlighted. STAAR contains a full Geographic Information System (GIS) that allows results to be displayed on maps, coordinates determined from maps, and maps transferred to wordprocessors and drawing programs. The program allows data to be sent in electronic form from the facilities to the District and from the District to the State.

The Monterey Bay Unified Air Pollution Control District (MBUAPCD) has acquired the STAAR system and is using the program to manage their AB2588 program. STAAR allows the District to rapidly evaluate more than 1000 facilities and to perform health risk assessments from the submitted inventory data. This process saves facilities from conducting unnecessary and costly assessment and gives the District a uniform means of setting limits and reduction goals. The entire process is sped up, reducing costs all around.

For facilities that have high emissions, STAAR can be used to analyze the source of risk and evaluate various solution options. Since analyses can be done easily, the facility can arrive at a economically sound solution and the District can verify the analysis.

STAAR OVERVIEW

JAYCOR has taken a systems approach to the automation of risk assessment for air toxics. We began by working with District and industry leaders to identify the statutory requirements, as well as the practical constraints of meeting those requirements. We discovered that the effective management of data required to carry out the processes was the primary problem. The sheer complexity of organizing emissions data, checking its accuracy, translating the data into input for analysis programs, dissecting the output, and presenting the final results in the required format was overwhelming. For industry, this complexity prevents an understanding of the root problems and inhibits a systematic investigation of the most cost-effective solution. For the regulators, this complexity adds considerable cost to verify results and the lack of a computerized system prevents the overall toxic impact, which was the purpose of the legislation, from emerging. In short, a great expense is incurred by all parties to achieve only a fraction of the intended results. Based on this understanding, we identified three goals.

Goals

The first goal is to streamline the process. Without a computerized system, data keeping is duplicated and often inconsistent. The process of transferring data from one form to another, eventually as input to an analysis program, is error prone and labor intensive. The magnitude of the paper generated literally chokes the system.

The second goal is to provide industry the flexibility. Typically, a facility must use an outside consultant to conduct the risk analyses and, because of cost, those analyses are limited in number. With an automated system, facilities can explore alternatives to product mix, control strategies, or operating scenarios. With the ability to examine their emissions impact in detail they can understand cause and effect and thereby take effective action. Finally, with these environmental analyses integrated into the normal business operations, the facility can work directly with the regulatory agency to find a cost effective solution.

The third goal is to improve regulatory decisions. Without access to all of the information, regulatory decisions must be made without knowing their impact, which could lead to rules that have an unexpectedly harsh economic consequence or an unexpectedly negligible environmental improvement. An automated system allows the impacts to be studied, tradeoffs made, and consensus achieved before finalizing rules.

Functional Requirements

An examination of the risk assessment process led to formulation of the functional elements of STAAR. The principle adopted was that data be maintained in standardized form wherever possible, so that the cost of conversion is minimized and so that the data can be accessed by other applications.

For facilities and emissions data, standard Structured Query Language (SQL) databases were selected. We chose an interface that meets the emerging industry standards of compatibility, ODBC, so that STAAR can access databases of different types from within the same program.

For geographic data, required to locate facilities and receptors and to determine coordinates and elevations, we selected the USGS standard Digital Line Graph (DLG) format. Maps can be shared between STAAR and any geographic information system (GIS) and standard maps for roads, waterways, land use, etc. are available at low cost from the federal government.

For the connection to dispersion and analyses programs, we set a requirement of not modifying those programs, so that regulatory integrity can be preserved. Consequently, the input files are set up in the required format and the output files are parsed and results extracted without modifying the underlying program. As a result, calculations can always be independently checked and the input and output files archived separately from STAAR.

Since reporting is the principal product of these analyses, a versatile report writing capability must be provided. These reports should include those required by AB2588 and specialized summaries that can help guide facility and regulatory decision making. In addition, much of the information is contained graphically in maps showing impact areas, so that generation and manipulation of geographic information is required.

Finally, the system should allow data to be transmitted in electronic form between facilities and the Districts and between the Districts and the State.

Implementation

Since the system is intended to be used by staff that can vary from time to time and who may not be committed full time to risk analyses, the ease of use of the program is critical to its effectiveness. We selected MS-Windows running on an Intel-based PC as the platform with the greatest installed base and support. By using standard Windows conventions, the learning and remembering curves are short and shallow. The multi-tasking nature of the environment allows results to be shared among applications, the most important of which is that tables and graphics can be copied directly into wordprocessors for final reporting.

The software can be run over standard networks so that data can be maintained on a single server. Depending on the hardware configuration, both the data and the analysis programs can be executed on separate machines, which could be Unix workstations for speed.

DATABASE STRUCTURE

The STAAR database is patterned after California's Air Toxics Emissions Database System (ATEDS) and the US Environmental Protection Agency's AIRS database. The structure is process oriented with separate links to "stacks" (points of emission) and "devices" (equipment governed by permits). The facilities are identified with Standard Industrial Classification (SIC) numbers and the processes by Source Classification Code (SCC). Emission rates can be described by a combination of emission factors and process rates or directly by measured data.

We have extended the ATEDS data structure to meet the needs of risk analysis. First, parameters needed by analysis, but missing from the original prescription, have been added as fields. Next, description of sensitive receptors (schools, hospitals, etc.) have been included in the database so that analyses can be set up automatically. Third, tables have been added to store risk results for source-receptor combinations, so that global analyses can be made without re-running the dispersion and risk programs. Finally, speciation tables can be defined that standardize the assignment of substances emitted by a process and standardize the emission factors.

Data validation is provided at the time of entry or on the entire database. Range checking is performed based on user specified values. For quantities that must be selected from other tables, such as toxic substances and the SIC and SCC codes, the user selects from a list. The determination of UTM coordinates and elevations for sources and receptors can be made automatically from the street address, by use of the Commerce Department's TIGER files, or can be found by visually locating the point of interest on an electronic map. Conversely, the validity of a location can be checked by displaying its coordinates on an electronic street map.

STAAR uses the ODBC standard interface so that the emissions database can be in a wide variety of formats. For organizations using California's PC-ATEDS program, we use ORACLE. Other implementations of STAAR use dBase and Paradox data files.

ANALYSES

Emissions Analysis

STAAR computes all emission totals from the basic process data. In this way, no additional errors can arise by subsequent human calculations. Totals can be displayed by:

- ☐ Stack (for the purposes of dispersion analysis)
- ☐ Device (for the purposes of permit compliance)
- ☐ Facility (for the purpose of risk prioritization) and
- ☐ Multiple facilities (for the purpose of "Hot Spots" analysis).

By altering the emission factors, control efficiencies, or process rates, the consequence on these important emission quantities can be automatically determined.

Dispersion Analysis

When the user selects a facility for analysis, STAAR automatically sets up the input file to ISCST from data stored in the emissions database. Data not stored in the database, such as the meteorology data file, is assigned a default value which the user can change with a built-in ISCST input editor.

The receptor locations can be added in several ways. For the purposes of determining concentration distributions or Maximum Effected Individual (MEI), a grid of receptors in most appropriate. The program allows the user to set the location, size, and spacing of the grid in a very general way that is expressed relative to the facility so that the user does not have to be concerned with UTM coordinate values. For analyses concerned with population effects, a receptor set is generated based on the census tract data. Finally, if the impact on specific receptors is desired, they can be selected from the sensitive receptor database.

The input file is stored separately from the STAAR program. It can be archived and can be used for further analysis by ISCST without the use of STAAR.

STAAR will also set up the input deck for the SCREEN dispersion analysis, which is based on worst case meteorology. As in the case of ISCST, data is automatically

extracted from the database and the user is presented with editing screens for setting other default parameters.

Risk Analysis

AB2588 legislates that a particular multi-path risk analysis, Health Risk Assessment (HRA92), be made. These models have been solved in a program called ACE, developed under the sponsorship of the California Air Pollution Control Officers Association (CAPCOA).

The ACE program is notoriously difficult to set up correctly. Unlike ISCST, the input is in fixed field format that invites a multitude of errors. Chemical species are designated by a numbering system that follows no standard convention and changes from version to version. Furthermore, if the ISCST input and ACE input are not reconciled exactly, the risk results will be erroneous. Most of the errors that occur produce no error messages and require the user to either accept the results on faith or conduct a detailed reconstruction that is more involved than the original analysis.

STAAR sets up the ACE input file so that these errors do not occur. The ACE and ISCST inputs are reconciled as they are created. Chemical numbers are selected from a table that gives the correspondence between the name in the emissions database and the ACE values.

The output of the ACE program is parsed and the results used in subsequent analyses. When grid receptors are used, the MEI location is automatically calculated and displayed. The grid can be successively refined to locate the exact maximum. The grid results can also be converted into contour maps that can be displayed and printed. Other analyses give the total cancer burden to the population, when census receptors are used, or give facility contribution to total risk, when sensitive receptors are used.

REPORTING

STAAR generates reports needed for regulatory purposes, emissions analysis, and risk analysis. The user can design and incorporate into STAAR specialized reports of his own choice using Crystal Reports. Since the databases are maintained in standard ODBC format, they can be also accessed by a wide variety of other database programs.

STAAR produces filled in AB2588 forms that are replications of the State forms. In addition, the data can be formatted into the State specified transaction file and shipped electronically. Two organizations using STAAR can electronically exchange the complete, extended emissions database.

Maps generated by STAAR can be inserted into any document created by a Windows application. For example, a map showing risk contours superimposed on a street map can be exported to a drawing program, where labels and annotations can be made, then used in a wordprocessor to create a final document, such as required for public notification. The map can be printed in full color. For individual notification, the program can determine which sensitive receptors are within the threshold risk contour and produce a mailing list file.

Finally, reports can be generated that provide a breakdown of emissions and risk by release point or process (for control strategy analyses) or by device (for permit compliance analysis). Emission inventories can be maintained year to year so that changes can trends can be documented.

MONTEREY BAY INSTALLATION

The STAAR system has been in operation in the Monterey Bay Unified Air Pollution Control District (MBUAPCD) since February, 1993. The District now has over 1500 facilities on the system. The data was entered originally from the paper forms submitted by facilities, but at each subsequent update period, only the data that has changed needs to be modified.

MBUAPCD uses a subset of the possible analysis routines, for example, MEI as a measure of risk, rather than total cancer burden. Many of the calculations have been customized for the District needs and the user interaction has been refined based on day-to-day experience of all staff members using the program, from data entry personnel to engineers.

CONCLUSION

Toxic risk analyses are an important part of evaluating environmental conditions and deciding on corrective strategies. The complexity of the data keeping requirements, as well as dispersion and risk analyses, however, has prevented industry and regulatory organizations alike from finding the most cost effective solutions.

The STAAR system provides a complete package of database management, geographic information tools, dispersion and risk analyses, and report generating software that makes this process simple, yet powerful. Facilities can now make analyses that determine the impact of proposed process and control changes on toxic emissions and subsequent risk. Since the analyses can be made by in-house staff, the changes can be integrated into the on-going business decisions. Similarly, regulatory organizations can quickly review air toxics reports and make their own analyses of the impact of proposed rules.

A computer-assisted system, such as STAAR, of data management, analysis, and reporting can help lower the cost of complying with environmental regulations and making the actions to be taken more effective.