PROCEEDINGS OF

PSAM — II

Volume 2

(Sessions 37 - 72)

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

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.)

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)

SAND93-1235

DEVELOPMENT OF FAST-RUNNING THERMAL AND STRUCTURAL RESPONSE MODELS FOR PROBABILISTIC ANALYSES OF COMPLEX SYSTEMS*

Allan S. Benjamin and Nisa N. Brown
Special Projects Department 6411
Sandia National Laboratories
Albuquerque, NM 87150

Risk assessment is often defined as the analysis of what can go wrong in a complex system, how likely it is to occur, and what the consequences are. The more complex the system is, the more pressed the analyst becomes to ensure that he or she has considered all the credible pathways that can lead to an unsafe condition. If the analysis involves the determination of how the system responds to thermal or structural challenges, then the analyst must have the tools to evaluate these responses rapidly and reliably over a very broad range of possible scenarios.

Three areas where fast-running thermal and structural response models are particularly desirable are: (1) for assessments of potential nuclear detonation pathways for nuclear weapon systems exposed to fires and crashes; (2) for probabilistic structural analyses of civil systems exposed to dynamic loadings; and (3) for dynamic analyses of nuclear reactor systems exposed to external events. The overarching concept of the models may be similar for each of these cases, but the reasons they are needed and the manner in which they are used may be quite different.

In nuclear weapon system applications, fast-running models are needed to explore very subtle variations in the environments to which the system is exposed in order to ascertain whether any of these variations can lead to an electrical pathway from a power source to the main detonators. For such a pathway to develop, some components have to fail as a result of the environment while others must survive.

In probabilistic structural analyses, fast-running models can be used to explore the responses of the system over a wide range of material property variations to determine the effects of these uncertainties on the final state of the system. Rather than attempting to prove that the system survives all design basis accidents, the analyst attempts to demonstrate that the probability of structural failure is acceptably low.

In dynamic nuclear reactor risk assessments, fast-running models are needed for tracing the transient responses of the reactor plant over a set of accidents that can unfold in a countless number of ways, depending upon the dynamics of the external environment and the nature and timing of the human responses.

*This work was supported by the United States Department of Energy under Contract DE-AC04-76DP00789.

This paper describes two fast-running physical response algorithms, which were originally developed for the analysis of nuclear detonation pathways in nuclear weapon systems, but which can be used for other applications such as those mentioned above. The first is embodied in a computer code called TEMPRA-3D, which is an acronym for "Thermal Evaluation and Matching Program for Risk Applications." The second is contained in a computer code called STRESS-3D, which stands for "Spring-mass Transient Response Evaluation for Structural Systems." A discussion of the overall approach being taken to assess nuclear detonation risks, including the use of TEMPRA-3D and STRESS-3D, may be found in related papers.[1,2]

TEMPRA-3D is a lumped-capacitance thermal analysis code that is extremely fast-running and unconditionally stable. It contains fully integrated numerical models for many phenomena of interest in the evaluation of system responses, including thermal conduction, thermal radiation, thermal convection, chemical reactions, and material decomposition. Given inputs for the appropriate thresholds, the code is capable of calculating the timing of important events, such as component failures or the ignition of explosives. If uncertainty distributions are provided, it computes pairwise event probabilities (i.e., the probability that one event occurs before another). TEMPRA-3D achieves its speed and computational stability through the use of lumped-element modeling and semi-implicit time integration, together with full linearization and numerical coupling of the governing nonlinear equations.

TEMPRA-3D also contains a benchmarking option, in which the user may specify that certain parameters are adjustable. A special algorithm determines the values of these parameters that optimize agreement with a set of benchmarking data. The benchmarking data may include results obtained from more detailed finite-element models or data obtained from experiments. Further details of the modeling concepts employed in TEMPRA may be found elsewhere.[3]

STRESS-3D is a dynamic structural analysis code that models a system as a connection of masses and nonlinear springs. The principal functions of STRESS-3D are to calculate the dynamic responses to various types of impacts, focusing upon the stresses and strains in shell-like structures and the mean accelerations and displacements of solid components. Some of the key features of the code are: (1) explicit integration of Newton's law of motion for each mass; (2) spring forces evaluated from constitutive (stress-strain) relationships and appropriate areas; (3) characterization of strain-hardening in inelastic materials and compressive load-bearing capability of foam materials; and (4) innovative modeling of shells. The code is numerically stable regardless of mesh skewness, a feature that distinguishes it from finite-element codes. Some of the concepts employed in STRESS-3D are described elsewhere.[4]

As of this writing, the STRESS-3D code is in an exploratory state of development and has not yet been used in a risk assessment. On the other hand, TEMPRA-3D has been applied in a PRA, and the results provide evidence of the relative efficiency, accuracy, and reliability of the code compared to a detailed finite element (FE) code. The results of the comparison are shown in Figure 1 and are described below.

For this example, we discretized a reentry vehicle (R/V) and its internal components into meshes suitable for each code. The detailed FE mesh contained about 5000 finite elements, and each run utilized about 12 CPU hours on Sandia's Cray YMP computer. The long execution time was due in large part to the large number of radiation surfaces employed. The simplified TEMPRA-3D mesh contained 154 lumped elements, and each run required about 30 CPU seconds on the same platform (a factor of 1400 reduction). We ran the two models for the same five cases which are summarized in Table 1. These cases encompassed a wide variety of thermal environments. For both models, we tracked temperature responses for 11 components and structural members of interest to the PRA. We assigned each component a failure or actuation temperature threshold, recorded the time at which each exceeded its threshold, and plotted the results in Figure 1. Each point in the figure represents an event time for one of the 11 components during one of the 5 cases.

The results indicate that TEMPRA-3D is capable of providing a close simulation of detailed finite-element analyses. The standard deviation of the differences between TEMPRA-3D and the detailed FE model for the data in Figure 1 is $\pm 7.2\%$, a figure which is well within the commonly accepted accuracy requirements for PRA applications. This high degree of fidelity is attributable principally to the parameter adjustment feature of TEMPRA-3D.

Table 1. Conditions Applying to Example Application.

(a) Cases Run

Case	Fire Temperature	Fire Duration	System Configuration	Fire Orientation
1	5000 °F propellant fire	10 minute heatup	Whole R/V	Laterally engulfing
2	1850 °F fuel fire	4 minute heatup, 86 minute cooldown	Whole R/V	Laterally engulfing
3	1850 °F fuel fire	90 minute heatup	Whole R/V	Forward part engulfed, aft part insulated
4	5000 °F propellant fire	10 minute heatup	Whole R/V with 2"-dia. hole through aeroshell opposite ESD	Laterally engulfing
5	2250 °F fuel fire	90 minute heatup	Midsection without end caps	Front plane exposed, sides immersed in isothermal medium

(b) Component and Structural Members Evaluated

1. Intent strong link
2. Environmental sensing device
3. Fuse switch
4. Fireset
5. Transformer
6. Trigger circuit
7. High explosive
8. Mounting plate bolts
9. Forward flange attachment
10. Aft flange attachment
11. Thermal battery

In addition to the physically-based analysis techniques described above, we are exploring possible uses of logically based methods, such as neural networks and canonical variate analysis, as alternative approaches for simulating the thermal and mechanical responses of complex systems. These methods have been shown by a number of researchers to provide rapid and accurate simulations in certain applications.

The presentation will discuss the modeling aspects of TEMPRA-3D and STRESS-3D in greater detail, will expand upon the example results described above, and will provide additional information on the possible applications of these codes and other methods to contemporary problems in risk assessment.

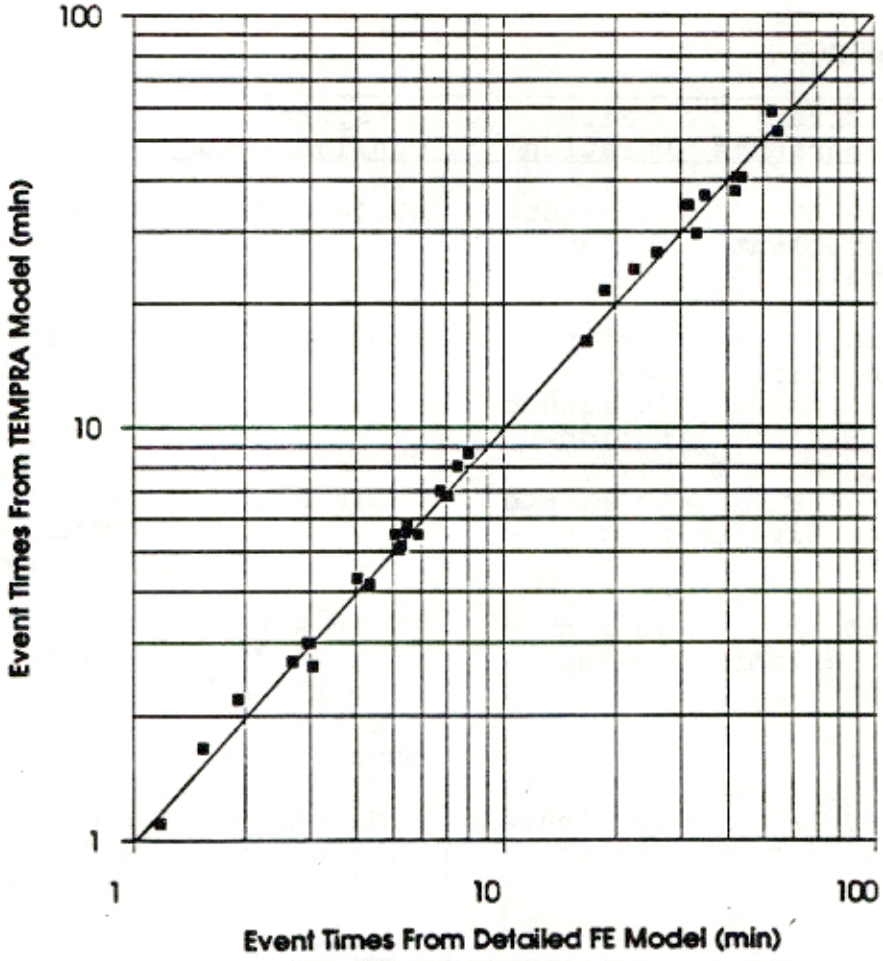


Figure 1. Comparison of TEMPRA-3D Results for Example Application with Results from Detailed Finite-Element Model.

REFERENCES

1. D. D. Carlson, "Nuclear Weapon System Risk Assessment," SAND93-1250C, This Conference, March 1994.

2. A. S. Benjamin, "Development of Smart Searching Algorithms for Vulnerability and Uncertainty Analyses in Probabilistic Risk Assessments," SAND93-1236C, This Conference, March 1994.

3. D. D. Carlson, A. S. Benjamin, R. J. Breeding, and D. M. Kunsman, "Probabilistic Risk Assessment Methods for Nuclear Weapon System Applications, Volume 2 - Methods," SAND91-0323/2, August 1991.

4. A. S. Benjamin, "Status and Observations Regarding Methodology Development for Simplified Structural Analysis," Sandia Memo, June 1992, and "Update of Status and Observations Regarding Methodology Development for Simplified Structural Analysis," Sandia Memo, March 1993.

THE IGNITION TEMPERATURE OF SOLID EXPLOSIVES EXPOSED TO A FIRE

John R. Creighton

Lawrence Livermore National Laboratory
Livermore, CA 94550

INTRODUCTION

When a system containing solid explosive is engulfed in a fire it receives a heat flux that causes the temperature of the system to rise monotonically. The temperature rise can often be approximated by a linear rise for extended periods of time. When some portion of the explosive, usually near the surface, reaches its ignition temperature it will begin to burn. If the explosive is unconfined, or can breach its confinement at low pressure, it will burn, not explode. Typically the burn front will propagate through a slab or shell at speeds on the order of a centimeter a minute. If the explosive is confined, the gas resulting from its burning will generate pressures high enough to rupture the confinement, but the peak pressure will generally be only a fraction of the pressure from a true detonation.

When a system is not engulfed in the fire, but is close enough to be heated slowly by the fire, the behavior will be different. If the explosive is heated slowly it will have a nearly uniform temperature and ignition will occur inside the explosive. This almost always causes an explosion, even when the explosive as a whole is unconfined. The reason for this behavior is not well understood but slow heating of an explosive generally results in a more violent explosion than fast heating.

These two situations are recognized by fast and slow cookoff tests used with munitions. Many munitions pass the fast cookoff test with heating rates around 2 K/min. Slow cookoff tests with heating rates around 4 K/hr generally result in an explosion. (The equations in this paper assume absolute temperatures in Kelvins, equal to Celsius + 273.16.)

Mathematical models predicting the time to explosion are usually based on the assumption that the explosive has a uniform initial temperature and that the outer surface is suddenly raised to some temperature and held there. The earliest such models were those of Semenov[1] and Frank-Kamenetskii[2]. Many numerical calculations use the same boundary conditions, as exemplified by the work of Zinn and Mader[3]. These models predict a critical temperature for explosion. Below the critical temperature heat loss exceeds the heat generated by chemical reactions *everywhere* in the explosive and no explosion occurs.

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract No. W-7405-Eng-48.

Above the critical temperature heat generation exceeds heat loss *somewhere* in the explosive. The chemical heat generation increases roughly exponentially with temperature while heat loss by conduction increases only linearly with temperature. The result is a thermal runaway that is usually associated with ignition of the explosive.

This paper analyzes a different boundary condition, a linear temporal increase of the surface temperature. The results are similar to the constant boundary temperature except that at higher heating rates the ignition temperature is higher than the critical temperature, defined above. The only other relevant calculation that we could find for this boundary condition was the work of Boddington[4]. He and his coworkers did an asymptotic analysis for a linearly increasing temperature on the boundary, assuming a single Arrhenius rate coefficient. This paper considers more realistic, multi-step, reaction schemes representing some real explosives. We used the multi-step reaction schemes of McGuire and Tarver[5] for HMX (octahydro-1,3,5,7-tetranitro-1,3,5,7-tetrazocine) and TATB (2,4,6-trinitro-1,3,5-benzentriamine). These schemes require numerical solutions. We also did calculations for a single Arrhenius rate coefficient, to compare with earlier work. The calculated ignition temperatures fit a relatively simple curve and a mathematical model explains features of the curve fit.

BASIC THEORY OF THERMAL RUNAWAY

The governing partial differential equation considers heat conduction and chemical generation of heat

$$\rho C\frac{\partial T}{\partial t}=\frac{\partial}{\partial x}\left(\lambda\frac{\partial T}{\partial x}\right)+dQ_{chem}/dt \qquad (1)$$

where r is the density , C the heat capacity per unit mass, λ the thermal conductivity of the explosive and dQ_{chem}/dt is the heat release rate due to the chemical reaction.

When the chemical heat release rate is negligible, solutions of the transient heat conduction problem can be obtained. The general solution for slab geometries is of the form $\exp\left(-x^2/4\alpha t\right)$, where the thermal diffusivity, α equals $\lambda/\rho C$. The exact form of the solution is determined by the boundary conditions, but the temperature approaches steady state with a time constant no less than $x^2/4\alpha$. Values of α from Table I give time constants on the order of 100 seconds at a depth of 1 cm. The time constant is quadratic in x so the time constant will be on the order of 400 seconds at a depth of 2 cm and 10,000 seconds at a depth of 10 cm. The behavior of cylindrical or spherical explosive systems is qualitatively similar.

If we use Arrhenius kinetics for the chemical heat release term in Eq. 1 we get

$$\rho C\frac{\partial T}{\partial t}=\lambda\nabla^2 T+\rho\Delta H_r Z[A]e^{-T_a/T} \qquad (2)$$

where ΔH_r is the heat of reaction per unit mass, $[A]$ is the mass fraction of reactant and λ is assumed to be independent of temperature. (I have used the activation temperature, T_a, in place of the traditional activation energy, E_a, equal to RT_a, to emphasize the dimensionless nature of the exponent.)

At low temperatures the chemical heat production rate is low so the system approaches a steady state where the left hand side of Eq. 2 vanishes and the conduction term cancels the chemical heat release *everywhere* in the explosive. At high temperatures the highly non-linear chemical heat release term completely overwhelms the conduction term . The rising temperature causes yet higher chemical heat release, resulting in thermal runaway. The critical temperature, T_c, is the highest boundary temperature for which a steady state can exist. Above this critical temperature the chemical heat release exceeds conduction *somewhere* in the explosive and $\partial T/\partial t$ becomes positive, increasing in magnitude as the temperature runs away

If the surface temperature is just slightly above the critical temperature the explosive will have time to reach steady state and ignition will occur near the center of a symmetric system. If the surface temperature is several degrees above the critical temperature, the center will not reach steady state before thermal runaway occurs at some location between the center and the surface. As the surface temperature is raised, thermal runaway occurs progressively closer to the boundary. Examples are found in Zinn and Mader[3].

Frank-Kamenetskii[2] discusses the critical temperature at length. We give a brief derivation. Let the surface temperature be T_s, and $T = T_s + \delta T$, where $\delta T/T_s << 1$. Substituting this in the Eq. 2 and expanding the exponent in a series yields a partial differential equation in δT.

$$\rho C\frac{\partial(\delta T)}{\partial t} = \lambda\nabla^2(\delta T) + \rho\Delta H_r Z[A]\mathrm{e}^{-T_a/T_s}\,\mathrm{e}^{T_a\delta T/T_s^2} \tag{3}$$

where typical values of T_a/T_s are between 30 and 50. For values of $T_a\delta T/T_s^2 << 1$ this equation has steady state solutions where the time derivative vanishes. If L is some characteristic thickness or radius of the piece of explosive we can make the steady state equation dimensionless by substituting $\xi = x/L$

$$\frac{\partial^2(\delta T)}{\partial\xi^2} = W(T_s)\mathrm{e}^{T_a\delta T/T_s^2} \tag{4}$$

where the dimensionless parameter

$$W(T_s) = \left(\rho\Delta H_r L^2/\lambda\right)Z[A]\mathrm{e}^{-T_a/T_s}$$

The left hand side of Eq. 4 is proportional to δT and cannot have a magnitude more than a few times δT. The minimum value of the exponential on the right hand side is 1, so solutions of Eq. 4 exist only for sufficiently small values of $W(T_s)$. Frank-Kamenetskii[2] has shown that for slab geometry there are no solutions of Eq. 4 for $W(T_s) > 0.88$. The

value of surface temperature, T_s, that yields this value of $W(T_s)$ is the critical temperature, T_c. If the explosive is a cylinder, the critical value of $W(T_s)$ is 2.0 , and it is 3.32 for a sphere. Critical temperatures exist for more complex chemical reaction mechanisms, provided the reaction rate is a monotone increasing function of the temperature.

The critical temperature is useful for safety studies because the explosive will not ignite below that temperature. However, caution should be used with calculated critical temperatures because the chemistry of explosives is complex and there are instances where actual systems containing explosives have ignited well below the calculated ignition temperature. Therefore system tests are advisable. Critical temperature is of limited use for systems engulfed in a fire. The fire temperature is generally much higher than the critical temperature so the system will eventually reach ignition temperature. In that case we would like to know how long it will take to reach ignition.

NUMERICAL SOLUTIONS FOR LINEARLY INCREASING SURFACE TEMPERATURE

Numerical solutions of the one-dimensional version of Eq. 1 were done for a slab with temperature $T_s = T_0 + \beta t$ at the surface $x = 0$ and no heat flow out of the surface at $x = L$. Three reaction schemes were used: a single Arrhenius rate coefficient as in Eq. 2 and multi-step reaction sets for HMX and TATB developed by McGuire and Tarver[5]. The chemical kinetic and thermal parameters are summarized in Table I. Calculations were done using standard finite difference and finite element methods.

Table 1. Summary of Chemical Kinetic Reaction Schemes

	λ cal/cm-s-K	C cal/gm-K	ρ gm/cm^3	Reaction	Rate	ΔH_f cal/gm
Arrhenius	0.00191	0.26	1.94	$A \longrightarrow B$	$3.5\times10^{19}\exp(-30{,}000/T)[A]$	2000
HMX	0.00123	0.24	1.90	$A \xrightarrow{1} B$	$1.4\times10^{21}\exp(-26{,}300/T)[A]$	-100
				$B \xrightarrow{2} C$	$1.9\times10^{16}\exp(-22{,}500/T)[B]$	300
				$C \xrightarrow{3} D$	$1.6\times10^{12}\exp(-17{,}500/T)[C]^2$	1200
TATB	0.00191	0.26	1.94	$A \xrightarrow{4} B$	$6.5\times10^{12}\exp(-21{,}000/T)[A]$	-50
				$A+B \xrightarrow{5} 2C$	$3.5\times10^{19}\exp(-30{,}000/T)[A][B]$	900
				$B+B \xrightarrow{6} 2C$	$1.6\times10^{15}\exp(-27{,}500/T)[B]^2$	950

$[A]$, $[B]$, $[C]$ and $[D]$ are mass fractions. Coefficients in reactions preserve mass fraction, not atoms.

Calculated ignition temperatures are shown in Fig. 1. A few relevant experimental data points[6] are shown for LX-10 (95% HMX) and LX-17 (92.5% TATB). There have been many fast and slow cookoff experiments so one would expect to find a wealth of experimental data for this boundary condition from fast and slow cookoff tests. However, when one examines this data many of the tests are for mixtures of explosives. Even if we have kinetic schemes for the individual components of the explosive it is probable that intermediate products of the two explosives interact, so we cannot simply add two reaction rates. Other cookoff tests are done with insulation between the heated surface of the

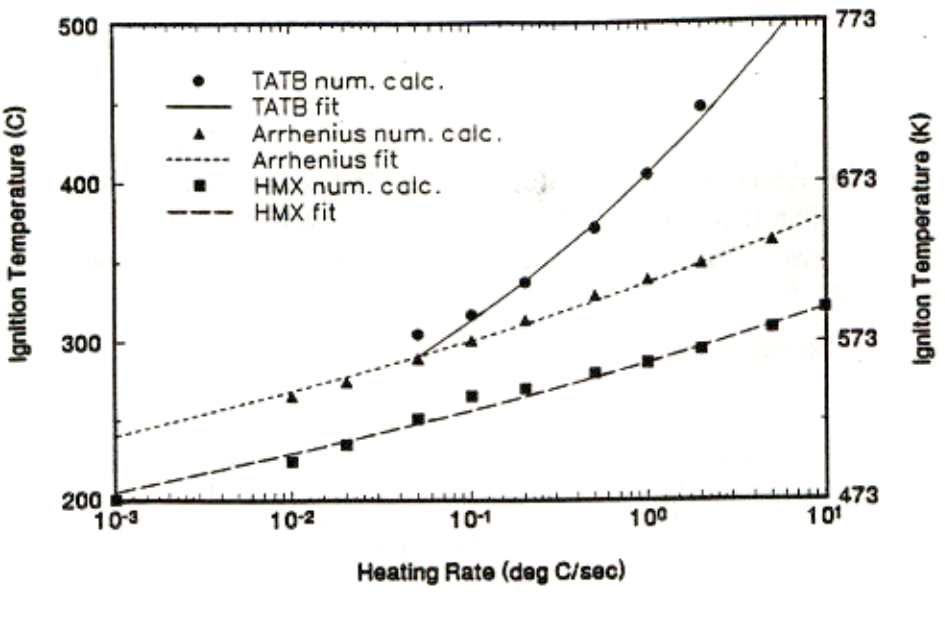


Figure 1. Numerical calculations of ignition temperature as a function of heating rate for a single Arrhenius reaction rate and multi-step models for HMX and TATB. Experimental results[6] for LX-10 (95% HMX) and LX-17 (92.5% TATB) are also shown.

munition and the explosive, so it does not match our chosen boundary condition. As a result there is surprisingly little good experimental data to compare with our numerical calculations.

A FUNCTION TO FIT THE NUMERICAL DATA

Along with the results of numerical calculations, Fig. 1 shows curve fits of the form

$$T_{ign} = \frac{T_1}{1 - b \ln \beta} \tag{5}$$

where the surface temperature is rising β K/sec. Different values of the fitting parameters, T_1 and b, are used for each kinetics model. The form of Eq. 5 was initially obtained by guessing the appropriate functional form and rejecting those that didn't fit well.

The form of Eq. 5 has a physical basis. With a linearly increasing surface temperature the steady state temperature distribution within the explosive is no longer uniform. Instead it is a parabola[7].

$$T_u = T_s - \frac{\beta L^2}{2\alpha}\left(2x/L - x^2/L^2\right) \tag{6}$$

Let $T = T_u + \delta T$, where δT is the small contribution to the total temperature due to the chemical reaction. Substituting this into Eq. 2 and expanding the exponential gives an equation analogous to Eq. 4

$$\frac{\partial^2(\delta T)}{\partial \xi^2} = W(T_s)\mathrm{e}^{-T_a\beta L^2\left(\xi - \frac{1}{2}\xi^2\right)/\left(\alpha T_s^2\right)}\mathrm{e}^{T_a\delta T/T_s^2} \tag{7}$$

At very low heating rates this has a critical temperature very close to that of Eq. 4. At higher heating rates the exponential term in the middle is less than 1 so the critical value of $W(T_s)$ must be greater than that from Eq. 4 and ignition will generally occur near the surface. Note that δT is also a function of x so Eq. 5 must be integrated to determine the functional form of δT. This has been done using several approximations[8], yielding an equation for the critical temperature with $\eta = T_a/T_s^2$ and $p = \eta L^2/\alpha$

$$T_{ign} = \frac{T_a}{\ln\left\{\frac{\eta L^2 Z \Delta H_r\, \mathrm{e}^1}{p^2 \alpha C}\right\} - \ln\left\{\frac{\beta^2}{1-(1+p\,\beta/L)e^{-p\beta}}\right\}} \tag{8}$$

This is similar in form to Eq. 5, though more complicated. It differs from Eq. 5 by asymptotically approaching the classical Frank-Kamenetskii critical temperature as it should. The time to explosion is a trivial calculation, $t_{ign} = T_{ign}/\beta$. However, one should use these calculated ignition temperatures with caution unless they have been checked by actual tests of the system being considered. The chemistry of explosives is complicated and anomalously low ignition temperatures are not infrequent in real systems.

REFERENCES

1 N. N. Semenov, *Z. phys Chem.*. 48:571 (1928).

2 David A. Frank-Kamenetskii, "Diffusion and Heat Transfer in Chemical Kinetics", Plenum Press, New York (1969).

3 John Zinn and Charles L. Mader "Thermal initiation of explosives", *J. Appl. Phys.* 31:323.

4 T. Boddington, P. Gray and S.R. Kay (1986), "Thermal explosion and times to ignition in systems with distributed temperatures. III. The influence of a steadily increasing (ramped) ambient temperature", *Proc. R. Soc. Lond. A* 405:213 (1960).

5 R.R. McGuire, and C.M. Tarver " Chemical Decomposition Models for the Thermal Explosion of Confined HMX, TATB, RDX and TNT Explosives", *Proceedings Seventh Symposium (International) on Detonation*, Naval Surface Weapons Center, Dahlgren VA., pp. 56-64 (1981). See also C.M. Tarver, R.R. McGuire, E.L. Lee, E.W. Wrenn and K.R. Brein, "The Thermal Decomposition of Explosives with Full Containment in One-Dimensional Geometries", *Seventeenth Symposium (International) on Combustion*, The Combustion Institute, Pittsburgh, PA, pp. 1407-13 (1978).

6 S.K. Chidester and Woelffer, R, LLNL, private communication (1993).

7 H.S. Carslaw and J.C. Jaeger, "Conduction of Heat in Solids", 2nd Ed., Clarendon Press, Oxford, (1959).

8 J.R. Creighton, "The Variation of the Ignition Temperature of Solid Explosives as a Function of Heating Rate", Lawrence Livermore National Lab. Report, UCRL-JC-112314 (1993).

DEVELOPMENT AND VALIDATION OF A VAPOUR CLOUD EXPLOSION BLAST MODEL

G. Opschoor, A.C. van den Berg and W.P.M. Mercx

TNO Prins Maurits Laboratory
P.O. Box 45
2280 AA Rijswijk
The Netherlands

INTRODUCTION

The presence of dangerous goods such as liquids or gaseous flammable mixtures pose an increasing risk to society as the quantities involved and the frequency of activities grow during the last decade. Vapour cloud explosions have proved to be potentially devastating. Incidents as in Flixborough and Beek have shown the need to assess the risks of vapour cloud explosions.

The explosive power of a vapour cloud can be expressed as an equivalent explosive charge whose blast characteristics are known. Up to now TNT-equivalency methods are widely used to relate the quantity of fuel available in a vapour cloud to an equivalent of TNT-charge expressing the clouds explosive power.

Gas explosion research during the last decade however, has shown a completely different picture. It shows that a fuel-air mixture is flammable, but explosive only under appropriate conditions. These boundary conditions are that the mixture must be partially confined and/or obstructed. The awareness of boundary conditions as being the primary factor for explosion severity resulted in the Multi-Energy method for vapour cloud explosion blast modelling, developed in the TNO-Prins Maurits Laboratory during the last decade.

THE MULTI-ENERGY CONCEPT

Currently it is believed that the assumption of deflagrative combustion is a conservative and sufficiently safe approach in vapour cloud explosions hazard. In general the initial stage in the process of deflagrative combustion in gas explosions is more or less laminar. Based on many vapour cloud explosions the main question is now: How can laminar combustion develop into explosive and blast generating process ? The key to this problem can be found in the phenomenon of turbulence.

Premined combustion induces expansion and causes a flow field. If the boundary conditions to this expansion flow field are such that turbulence is generated, the flame will interact with the turbulence, resulting in stronger expansion flow. A positive feed-back coupling in triggered by which the process develops more or less exponentially both in speed and overpressure.

The consequence is that the development of a gas explosion is primarily determined by the presence of a turbulent generating environment. This important conclusion determines the concept of a vapour cloud explosion which underlies the method of blast modelling. This basic concept, called the Multi-Energy concept, states that blast is generated in vapour cloud explosions only in the parts of the vapour cloud which are obstructed and/or partially confined and that the unobstructed and/or unconfined parts of the cloud hardly contribute, in contradiction to conventional methods, in which a vapour cloud is regarded as an entity.

The Blast Model

In the Multi-Energy method fuel-air charge blast is used for this purpose [1]. Figure 1 shows the peak overpressure as well as the positive phase duration of the blast wave, produced by a hemispherical fuel-air charge of radius R_0 at the earth's surface, dependent on the distance to the blast centre in a Sachs-scaled representation. This blast model is generated by numerical simulation of spherical steady flame speed gas explosions.

The blast model reflects basic features of gas explosion blast. The initial blast strength is a variable expressed as a number ranging from 1 for insignificant to 10 for detonative strength. The initial blast strength can be defined as a consistent set of blast parameters at the location of the charge radius R_0. In addition, the model gives an indication for the blast wave shape which can have considerable effects for a subsequent dynamic structural analyses of a blast-loaded structure.

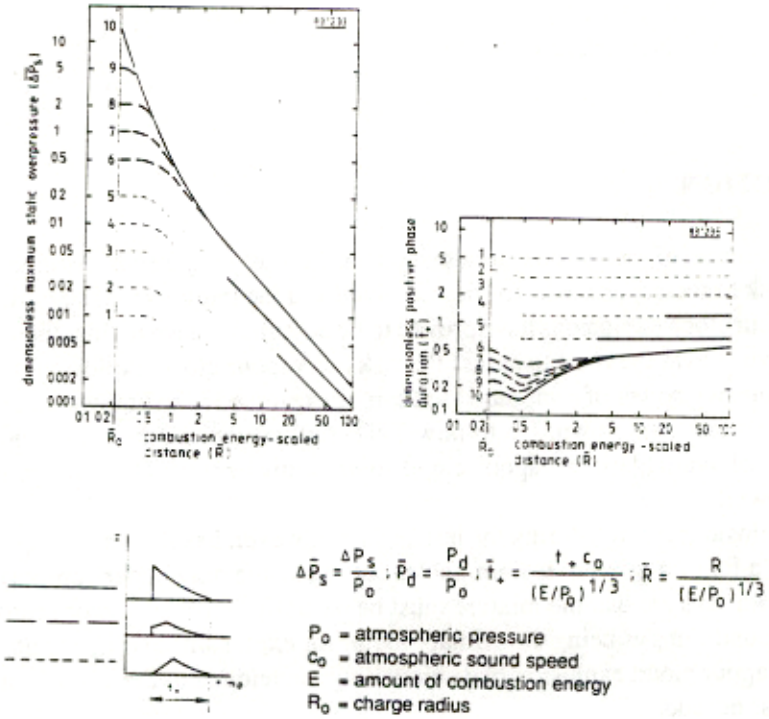


Figure 1. Hemispherical fuel-air charge blast model [1]

Uncertainties in the Multi-Energy Method (MEM)

Although the Multi-Energy method recognises the phenomena observed in reality better and should therefore be preferred to TNT-equivalency methods, there are two main aspects which hinder a clear and straight forward application.

- There is a lack of guidance to select an initial source strength (explosive power)
- In case multiple blast generating sources are present within the total vapour cloud, the question arises how they should be dealt with: separately or as one blast generating source.

Answering these questions requires fundamental knowledge of the explosion phenomena, which are gained from extensive experimental and theoretical research programs, which are still going on in the TNO/PML. Some important results will be discussed in the next chapter of this paper.

NUMERICAL SIMULATIONS

The theoretical research into vapour cloud explosions is focused on the improvement and validation of two computational fluid dynamic codes REAGAS-3D and BLAST - 3D.

The REAGAS-Code

The REAGAS-Code [2] is capable of simulating the basic mechanism of a gas explosion: the interaction between combustion, expansion and turbulence. With other words, the code can estimate the source strength (explosive power) of a vapour cloud explosion in an obstructed and/or partially confined area.

The mathematical model which implies the REAGAS-code can be summarized as follows [2]:

- The gas dynamics is modelled as a gaseous fluid which expands as a consequence of energy addition . This has been mathematically formulated in conservation equations for mass, momentum and energy.
- The energy addition is supplied by combustion which is modelled as a simple one-step conversion process of non-reacted material into combustion products. This is expressed in a conservation equation for the mixture mass fraction which a negative source term for the combustion rate.
- The combustion rate, which is fully controlled by turbulent mixing of combustion products which unreacted material is modelled by the Bray-Libby-Moss Unified Probability Function model.
- The feed-back in the interaction is closed by a k-ε model for turbulence which consists of conservation equations for the turbulent kinetic energy k and its dissipation rate ε.

An example will now be given in which the REAGAS-code is utilized. It concerns a simulation of a gas explosion in the space underneath an atmospheric storage tank. The tank is located on a pilon forest. For the simulation this pilon forest between two parallel planes is simplified into a two-dimensional obstacle environment. The obstacles are placed in 11 concentric circles according to the pilon layout. It is assumed that centrally ignition occurs. The results are presented in Figure 2.

The temperature distribution is visualised by a pattern of isotherms, one for each increase in temperature of 150 K.

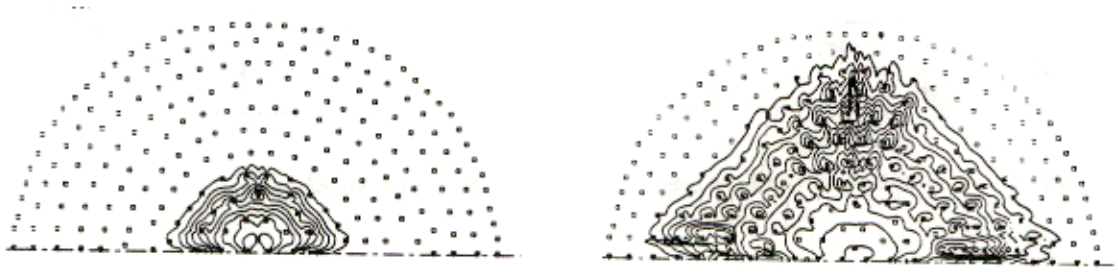


Figure 2. REAGAS simulation of a centrally ignited gas explosion developing in a concrete pilon forest underneath an atmospheric storage tank

The sequence of pictures shows a very characteristic behaviour of gas explosions: a slow start followed by a more or less exponential development in flame speed and pressure. This characteristic behaviour can be readily recognized in the overpressure transients sampled at various locations in the flow field and represented in Figure 2b. The computations sow that an overpressure of more than 40 kPa is generated during the development of this centrally ignited gas explosion. This maximum overpressure is observed more or less throughout the partially confined space.

This overpressure corresponds to a blast strength of number 6 of the MEM-charge blast model (Figure 1).

The BLAST-code

The blast waves generated by a vapour cloud explosion decay in the surrounding atmosphere and may to damage up to a considerable distance. The flow field inherent to a blast wave has a complicated structure in particular when it is influenced by the presence of irregular rigid boundaries. Often numerical simulation is the only possibility of finding the blast loadings of surrounding objects with some accuracy.

The assumption of inviscid flow-described by the Euler equations is justified for the computation of many aspects of blast. Blast-related flow fields are characterized by gas dynamic discontinuities. If conventional numerical methods are used to solve the conservation equations for mass, momentum and energy, such phenomena are completely degenerated. Special methods are required tailored to capture and preserve shock phenomena. In the BLAST-code [3] a Flux-Corrected Transport scheme is used for this purpose. By Flux-Corrected Transport, a higher order solution is obtained which is numerically diffused to an extent just sufficient for numerical stability.

To demonstrate the BLAST-code capabilities, the results of a numerical blast simulation are presented in Figure 3, which shows a blast wave of 10 kPa overpressure and 60 ms duration falling in at two buildings located close behind one another.

In Figure 3 the pressure field is represented which develops a consequence of the blast wave reflection at the configuration. At some consecutive points of time the pressure distribution is visualized by means of an isobar pattern, one isobar for each increase in pressure of 0.5 kPa. The picture gives a clear view of how the blast loading is the result of a combination of wave reflection and lateral rarefaction of reflected overpressures. In particular, they show how in between the two buildings a complicated wave pattern develops, a consequence of various reflections and wave interactions. The overpressures sampled at three different locations at each building are graphically represented in Figure 4. In the overpressure transients, the complicated wave pattern can be readily recognized.

The computation shows that the blast load at the front of the second building is considerably less than the reflected overpressure of the undisturbed blast wave endured by the front of the first building. In this way the effects of blast load reduction by sheltering effects can be quantified.

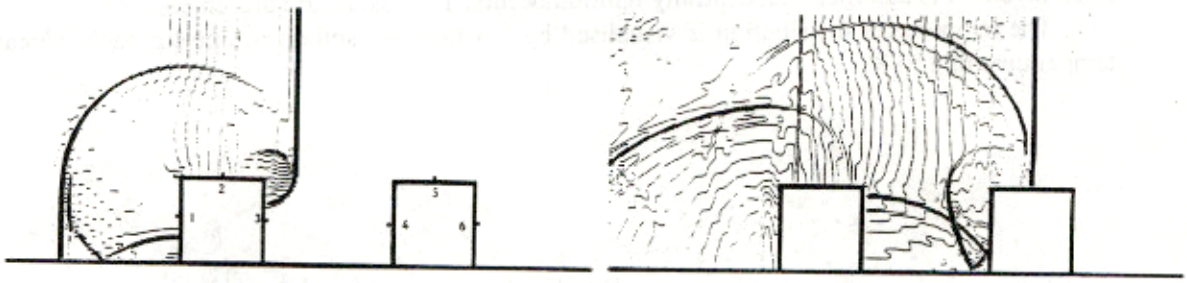


Figure 3. Blast simulation of the blast wave reflection by a complex of two buildings.

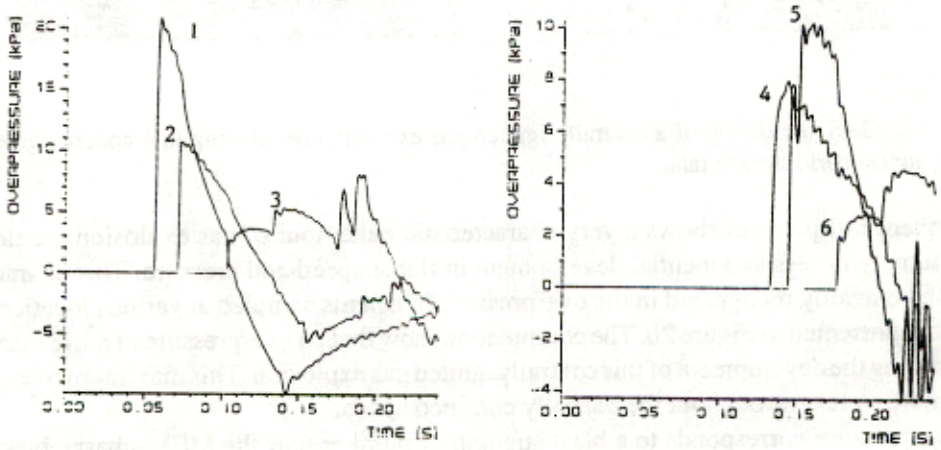


Figure 4. Overpressures sampled in various locations at the buildings.

EXPERIMENTS

The experimental research at TNO/PML was focused on the turbulence created by the flow interaction with obstacles. As in real plant situations, a wide variety of combinations of confining structures and obstacles exists. These situations had to be idealized and simplified to study efficiently the influence of the parameters involved. The emphasis was put on obstacles located between two confining surfaces, a top and a bottom plate, which is often present in on- and off-shore plants.

Here the results of two experiments will be described. The first experiment was performed on small scale (4 x 4 m) while the second was scaled up with a factor of 6.35.

In the first experiment the obstacles themselves consisted of concrete cylinders with diameters of 0.08 m. The obstacle array consisted of concentric circles of obstacles and had outer dimensions of 4x2 and 4 x 4 m with variable heights (Figure 5).

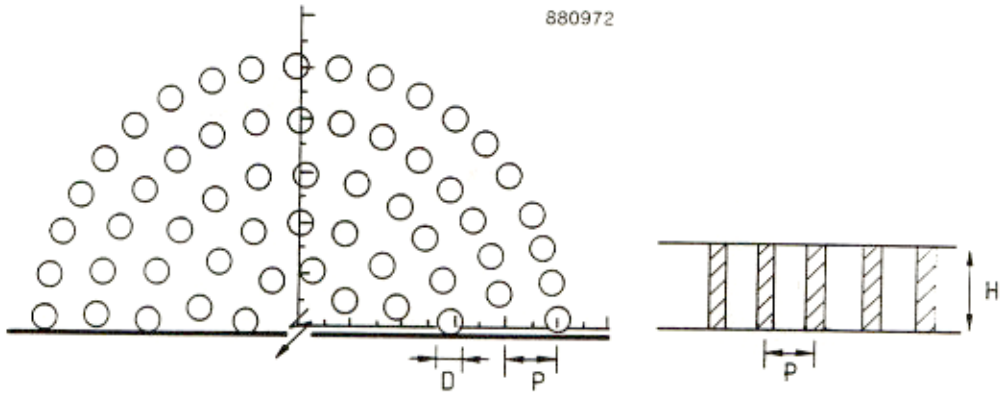


Figure 5. Obstacle configuration applied during experiments
D: obstacle diameter, H: obstacle height, P: distance between obstacle rows

Variables were [4]:

- the distance between two rows of obstacles (Pitch P);
- the ratio obstructed and unobstructed area in a cross section (Blockage Ratio BR):
- type of gas;
- a locally increased gap width between two obstacle arrays.

The last variable was to study the case in which two confined areas are present within the vapour cloud. Only the most important results will be described briefly here.

It was found that the maximum flame speeds occurred in the boundaries of the obstacle array ad that they were highest for the smallest pitch and the largest blockage ratio used (P= 1.5 D. D: obstacle diameter, BR= 0.7).

The influence of the type of gas on flame speeds and accompanying overpressures is related to the reactivity expressed in different values for the laminar flame speed: the higher the laminar flame speed, the higher the maximal flame speeds and overpressures. Further it appeared that scaling of the flame speed between various gases is possible by using the laminar flame speed as the scaling factor.

The results of the tests to simulate an explosion in one obstacle array and the ensuing explosion in a second nearby array show that the flame decelerates after leaving the first (donor) array and accelerates again after entering the second (acceptor) array.

Testing on a small scale makes an extensive study into the influence of various parameters cost effective. However, large scale experiments are necessary to validate scaling laws. It is known that explosion severity increases more than may be expected on the basis of these scaling laws, especially for vapour cloud explosions. For instance, the probability of a transition to detonation increases with increasing geometrical scale.

A test programme was set up to investigate the effect of scaling [5]. Seven tests from the previous programme were selected and scaled up with a factor of 6.35. This resulted in an obstacle with a diameter of 0.5 m and a height of 1 m. The outer dimensions of the obstacle array were 25.4 x 12.7 m. The variables were the type of gas, the pitch P and the blockage ratio BR.

The test results were influenced considerably by the partial failure of the roof during the tests.

It appeared that the simple modelling procedure for the flame speed and reactivity scaling, found for the small test results, gave unsatisfactory results. The assumption of the flame speed being the laminar flame speed until the flame speed until the flame reaches the first obstacle does not hold on a large scale. Due to the longer distance to the first obstacle, flame instabilities will occur which will increase the flame speed. Figure 6 shows a comparison between a small- and large-scale test. The premature venting through the roof is responsible for lower large-scale speeds at a longer distance.

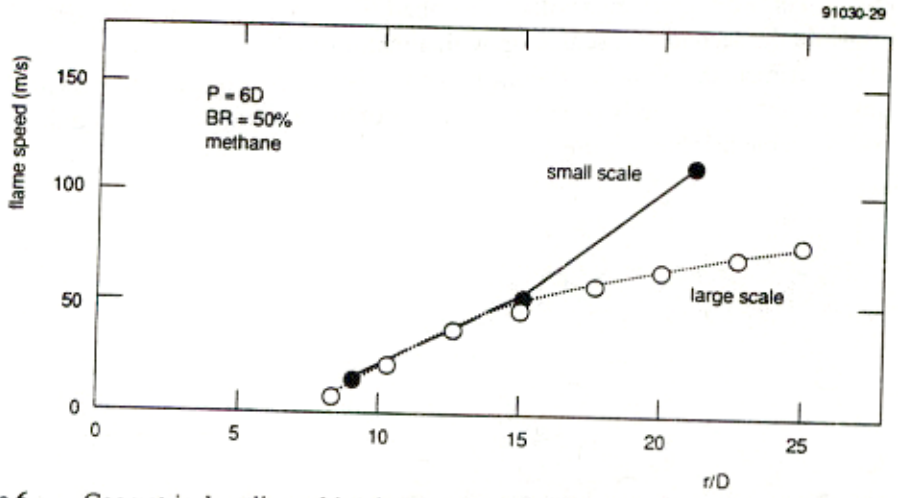


Figure 6. Geometrical scaling taking into account flame speed enhancement due to flame instabilities. r = distance to ignition. Test: methane, P = 6D, BR = 0.5.

CONCLUSIONS

Knowledge of the mechanisms of vapour cloud explosions has increased largely due to the experimental and theoretical research efforts made during the last decades. This has resulted in the development of the Multi-Energy method and the computational fluid dynamic codes such as REAGAS-3D and Blast-3D.

The Multi-Energy method constitutes an alternative for conventional TNT-equivalency methods which are unsatisfactory in some aspects.

The Multi-Energy framework is a flexible concept which makes it possible to incorporate current experimental data and advanced computational techniques. It appears that these computational techniques contribute a more and more sophisticated approach in vapour cloud explosion hazard analysis.

REFERENCES

1. A.C. van den Berg, The Multi-Energy method, a Framework for Vapour Cloud Explosion Blast Prediction, *Journal Haz. Mat.*, vol. 12, 1985.
2. A.C. van den Berg et al. "REAGAS- A Code for Numerical Simulation of Reactive Gas Dynamics in Gas Explosions," TNO-PML Report No. 1989-IN-48.
3. A.C. van den Berg. "BLAST-Code For Numerical Simulation of Blast Effects," TNO-PML internal report.
4. C.J.M. van Wingerden, Experimental Investigation into the Strength of Blast Waves Generated by Vapour Cloud Explosions in Congested Areas, *in:* "Proc. of the 6th Int. Symp. on Loss Prevention and Safety Promotion in the Process Industries," Oslo, Norway, 1988.
5. W.P.M. Mercx, Large Scale Experimental Investigation into Vapour Cloud Explosions, *in:* "Proc. 7th Int. Symp. on Loss Prevention and Safety Promotion in the Process Industries," Taormina, Italy, 1992.

POST-MORTEM RISK MODELING OF THE MEXICO CITY DISASTER

Dr. G.N. Pettitt, Mr. J.D. Harms, Dr. J.L. Woodward

DNV Technica, Inc.
355 E. Campus View Blvd, Suite 170
Columbus, OH 43235

INTRODUCTION

Computer models that simulate hazardous events are widely used in the chemical, petrochemical and related industries in order to determine hazard zones, to determine the risk from a particular incident or set of incidents, to establish an emergency response plan, etc. The validity of such analyses depends upon the accuracy of the computer models as well as upon the risk analysts' choice of modeling parameters and options. Post-mortem analysis of major accidents is an approach used to assess model accuracy and parameter choices.

We apply here post-mortem analysis of the Mexico City incident using current models and estimates of population density, fire exposure time, the fraction of available inventory burned in a fireball, etc. This exercise is as much a test of these sort of assumptions as it is of models, in this case primarily a fireball or BLEVE (boiling liquid expanding vapor explosion) model. The use of actual incidents comparing model predictions with experience usually has the advantage of not requiring scale up, but the disadvantage that the event conditions are usually poorly defined. For example, it is not known exactly how much material was involved in the Mexico City incident, and it is difficult to determine how many people were in the effect zone at the time of the incident. There is even uncertainty concerning the actual number of casualties.

BACKGROUND

The Mexico City incident occurred on November 19, 1984, when a release of LPG ignited and led to a large fire and a series of explosions that completely destroyed a PEMEX LPG storage and handling facility. At the time of the incident, inventories were variously reported at approximately 50 to 70% of capacity, or at approximately 7860 to 11,000 m^3 of LPG in six spheres and 48 bullets. The bullets were diked in groups and the tanks were diked individually. The layout of the facility at the time of the disaster is shown in Figure 1. The facility and disaster is well documented in a TNO report [1].

When the PEMEX facility was originally constructed around 1962, there were no buildings near the site. At the time of the disaster, there were about 40,000 people living in San Juan Ixhuatepec, a suburb of Mexico City, just south of the PEMEX site. Approximately 100,000 more people lived in the surrounding hills near the town. The nearest buildings were only about 130 m to the south of the storage tanks and consisted mainly of local population living in poor housing.

EVENT CHRONOLOGY

Most of the damage that occurred during the disaster resulted from several explosions during the morning. The first explosion occurred around 5:45 am. This explosion, from eyewitness accounts, was an ignited vapor cloud. This explosion did not create large overpressure but probably damaged a few nearby houses and damaged some pipes at the site. It also, most likely, started some fires in the area.

The second, and most likely the strongest explosion, occurred only 1 minute 9 seconds after the initial vapor cloud explosion. This second explosion is thought to be a BLEVE of one or both of the two 1600 m^2 (630,000 gallon) storage spheres. It is possible that one sphere contributed to the BLEVE and the second contributed to longer-lasting pool fires.

The mechanism for a possible rupture and explosion in such a short time is not clear, although high line pressures are cited in a TNO report (1). Prugh (2) summarizes historical experience with BLEVEs and lists overpressurization, mechanical damage and mechanical failure, and a vapor-space explosion in the tank as possible causes for a BLEVE in addition to the usual cause by overheating. The short time frame in this case does not allow development of high metal temperatures as suggested by instrumented large-scale tests (Appleyard, 3, Venart, et al., 4). Venart (5) has postulated a mechanism of coordinated bubble collapse that does not depend strongly on the presence of high metal temperatures.

This second explosion leveled houses close to the site and was even mistakenly reported as an earthquake. The blast wave from this explosion also shifted some of the storage cylinders from their supports which caused further LPG to be added to the fire. The instantaneous release of such a large amount of LPG during the incident most likely resulted in the material partially vaporizing in the BLEVE. It was observed that some unburned LPG spread into the populated areas. Both unburned and burning LPG flowed around and through nearby houses and ignited numerous secondary fires.

Several more explosions occurred during the next hour. The largest of these occurred at 6:54 am. This explosion was also believed to be a BLEVE of the two remaining 1600 m^3 (420,000 gallon) spheres. However by this time most of the damage had already been done by the earlier explosions.

Altogether, four 1600 m^3 (420,000 gal) spheres were completely destroyed. The two 2400 m^3 (630,000 gal) spheres were less damaged; the supporting legs weakened and tilted the spheres toward the ground; one of these larger spheres had also ruptured at the top. Of the 48 bullet tanks originally on-site, 12 had been propelled off-site, 4 had completely disintegrated, and the remaining 32 were found on-site, with only four not blown off their supports. Overpressures from the explosions likely shifted some of the tanks in the storage area, but did not cause significant damage compared to the heat and the fireballs. The maximum distance that damage occurred to stone and concrete buildings was about 300 m. Scattered damage resulting from flying fragments occurred up to 1200 m from the storage area.

The casualty list from this disaster included around 560 fatalities and 7000 injured. The majority of the damage and loss of life was probably due to the heat and ground

level fireballs that swept through the houses. Most of the fatalities occurred within 300 m of the storage area. People in the street within 300 m of the plant most likely did not survive due to direct flame contact. A large fraction of the people indoors at the time of the first two explosions within 300 m of the plant, perished, most likely while they were still sleeping.

COMPUTER MODELING

We chose to analyze a single major event, the second and probably largest explosion that occurred during the disaster since it most likely caused the most damage and loss of life. This explosion was modeled as a BLEVE using variations in several program parameters. The parameters varied are the population density, the percentage of people inside dwellings who were killed by a BLEVE, and the inventory of LPG involved in the BLEVE.

BLEVE Model

The fireball developed by a BLEVE is a short-lived transient event, described by a simple model. The effective fireball radius, R_{ef} and duration, t_{ef}, are given in terms of the mass of flammable material M, according to Moorehouse and Pritchard (6) by:

$$R_{ef} = 2.67\ M^{0.327}$$
$$t_{ef} = 0.923\ M^{0.303}$$

The emitted heat flux, F_{emit}, is given by:

$$F_{emit} = \frac{f_R M H_c}{t_{ef} A \pi R_{ef}^2}$$

where H_c is the heat of combustion. The fraction of available heat energy radiated, f_R, is given by Roberts (7) and ranges between 0.2 and 0.4. SI units apply.

The radiation dosage received by the observer, F_{dose}, depends also on a view factor, so:

$$F_{dose} = \frac{F_{emit}}{\left(\frac{R}{R_{ef}}\right)^2 + 1}$$

The effective distance to the center of a fireball, R, is related to the actual distance, R_o, by a function of the transmissivity of the atmosphere, giving, for the Mexico City conditions $R/R_o \equiv 0.66$.

Meteorological Conditions and Population Density Modeled

The ambient temperature was 7° C and winds were calm in the early morning. We used Pasquill/Gifford Stability Class E with 0.5 m/s winds to the east for the computer simulation runs.

An accurate population map for the area at the time of the disaster is unavailable. Using Figure 1, the populated area within a 300 m radius of the BLEVE is about 38,300 m^2. We assumed three alternative population densities, 1.9, 2.9 and 4.9 people/100 m^2. These densities would produce 560 fatalities if the fatality ratio for population within 300 m were 75%, 50% and 30% respectively. This same population density was also applied to the built up area outside of the 300m radius. The population was mostly indoors during the disaster, so roads were not modeled as population sources, only the building areas.

Simulation Results

Table 1 gives the BLEVE model predictions for fireball radius, duration, and emitted thermal flux for a set of assumed flammable masses, M, involved in the explosion. One eyewitness report put the fireball radius at 185 m, which would correspond to M=410 tonnes.

Figure 2, from Mudan and Croce (8), summarizes data for injury and fatality from fire exposure as a function of time of exposure and incident thermal flux. The data for the significant injury threshold are quite close to the data for the onset of fatalities to 1% of the dosed population.

For each flammable mass in Table 1 and corresponding fireball duration, t_{ef}, we obtained a threshold effect level for thermal flux from Figure 2. That is, at various fatality levels, say 25, 50 and 75%, the threshold thermal flux from Figure 2 is included in Table 1.

For each flammable mass, the BLEVE model predicts a radiation profile in radial distance. The threshold effect levels in Table 1 are points on the radiation profiles, which when overlaid over the population map indicate an incremental area and a number of people living in that area. This number of people is multiplied by the fatality fraction corresponding to the threshold effect/radial distance. Summing over all incremental areas gives the total predicted fatalities. Predicted fatalities are plotted in Figure 3 against the flammable mass, M, for each of the assumed population densities.

The simulations showed that the amount of material in the BLEVE has an approximately linear effect on fatalities. This may be an artifact of using uniform population density. That is, both the radiation levels and the area covered by the effective radiation level are related proportionally to the square root of the distance from the site center.

Figure 4 shows corrected fatality levels with respect to the flammable mass for varying population densities. The fatality levels were corrected by a factor of 0.3 to reflect the estimated degree of protection that is afforded population located indoors and shielded from the incident by buildings. From Figure 4, it is seen that this estimated degree of protection fits the observed fatality range for the estimated population density.

CONCLUSIONS

The results from the computer simulation showed that several sound assumptions can be made concerning the modeling of a BLEVE incident. In addition, for some incidents, not all of the inventory in a BLEVE-ing tank participates. Some of the inventory may rain out into a burning pool fire, or a ground level fireball phenomenon occurs.

The comparison between the historical outcome of the Mexico City disaster and computer simulations also illustrated that the role of the analyst is critical to the accuracy of the study. The analyst has to be able to decide which set of values is the optimal set for that particular location and facility. No matter how precise and accurate a group of

variables are for one facility, entirely different values may need to be used at a different facility. In this respect, the judgement and experience of the risk analyst then becomes the most important variable for the entire study.

REFERENCES

1. Pietersen, C.M., S. Cendejas Heurta, "Analysis of the LPG incident in San Juan Ixhautepec, Mexico City, 19 November 1984", TNO, The Hague, 1984.

2. Prugh, R.W., "Quantify BLEVE Hazards", Chem. Eng. Prog., p. 66-72, February 1991.

3. Appleyard, R.D., "Testing and evaluation of the EXPLOSAFE system as a method of controlling and boiling expanding vapour explosion (BLEVE), Report TP 2740, Dept. of Res. and Dev., EXPLOSAFE Div., Vulcan Industrial Packaging Ltd., 185 pages (1980).

4. Venart, J.E.S., A.C.M. Sousa, F.R. Steward and R.C. Prasad, "Experiments on the physical modelling of LPG tank cars under accident conditions", International Symposium Transport and Storage of LPG & LNG Proceedings, Vol. 1, Royal Flemish Society of Engineers, Brugge (Belgium), pp. 385-390 (1984).

5. Venart, J.E.S., "To BLEVE or not to BLEVE: An Anatomy of a Boiling Liquid Expanding Vapor Explosion".

6. Moorehouse, J. and M.F. Pritchard, "Thermal Radiation Hazards from Large Pool Fires and Fireballs - A literature Review", Symposium on the Assessment of Major Hazards, Manchester, 1982.

7. Roberts, A.F., "The Effects of Conditions Prior to Loss of Containment on Fireball Behavior", Symposium on the Assessment of Major Hazards, Manchester, 1982.

8. Mudan, K.S. and P.A. Croce, "Fire Hazard Calculations for Large Open Hydrocarbon Fires", Chapter 4 in SFPE Handbook of Fire Protection Engineering, National Fire Protection Association, Quincy, Mass, p. 2-84, 1988.

Table 1. Modeled BLEVE Parameters

Flammable Mass, M, tonnes	100	250	410	500
Fireball Radius, R_{ef}, m	115	155	183	195
BLEVE Duration, t_{ef}, sec.	30	40	46	49
Emitted Flux E_{emit}, kW/m^2	368	382	390	394
Threshold Dose for 25% fatalities F_{dose}, kW/m^2	28.2	22.4	19.4	17.8
F_{dose} for 50% fatalities	37.6	29.9	26.6	24.4
F_{dose} for 75% fatalities	44.7	35.5	30.7	28.2

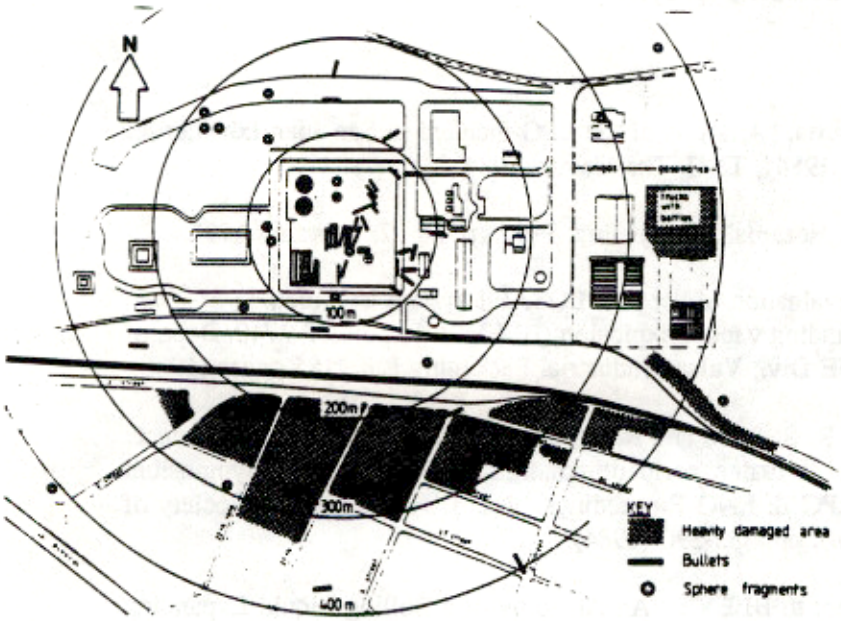


Figure 1. Reproduction of the area in which damage occurred (Reproduced from Ref. 1)

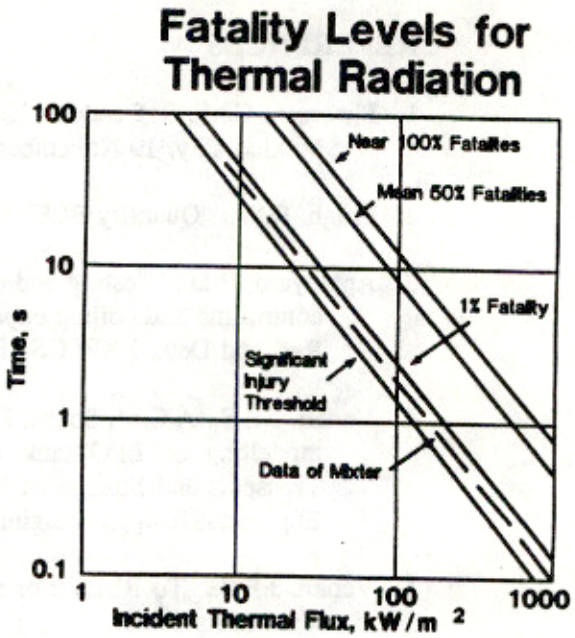


Figure 2.

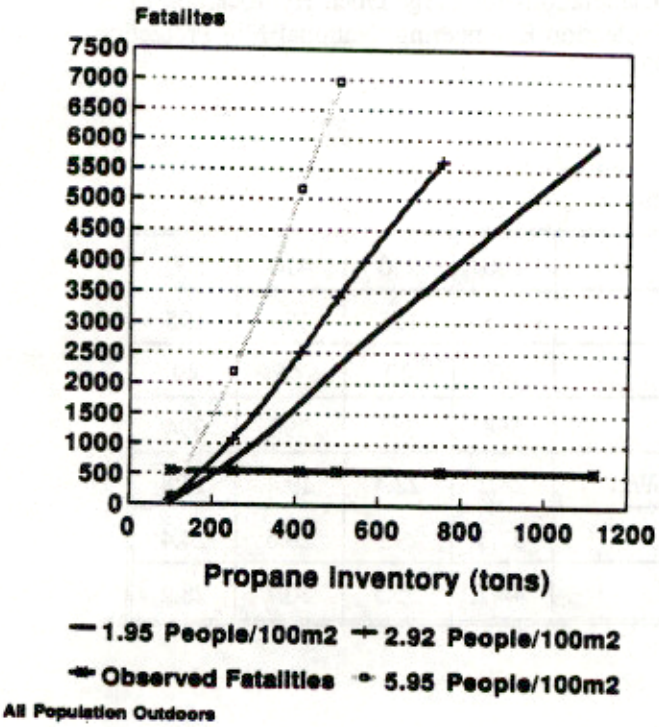


Figure 3.

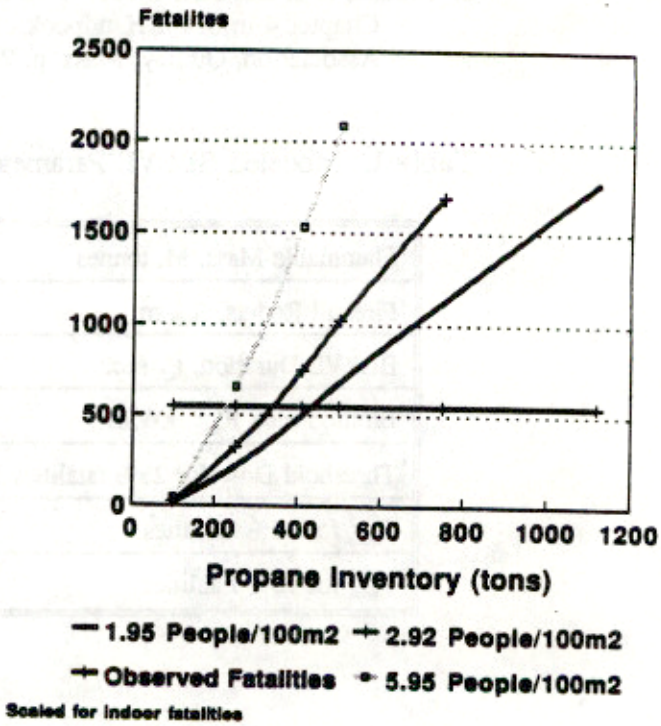


Figure 4.

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)

AN ASSESSMENT METHODOLOGY FOR SRB MISSION FAILURE PROBABILITY

Feng Hsu and Mohamad Ali Azarm

Engineering Technology Division
Department of Advanced Technology
Brookhaven National Laboratory
Upton, New York 11973

INTRODUCTION

In this paper, an assessment methodology is presented for the evaluation of mission failure probability based on Solid Rocket Booster (SRB) risk scenarios, including their relation to SRB operating specifications. This work was performed at BNL under the auspices of NASA in an effort to summarize parametric data as well as the failure-launch records of SRB. A specific SRB reliability database was developed using the internationally collected solid rocket booster data information contained in the AIAA document[1]. Due to the vital importance of SRB failures in the overall launching risk of many space vehicle systems, the main objective of this study is to develop a methodology which can be used as a procedure guide in the evaluation of SRB failure probability, and more importantly, to determine the SRB mission failure probability as a function of design parameters. In this regard, much of the effort in this study was allocated to evaluating the possible correlations among the available SRB design parameters and their underlying failure probabilities.[2]

The overall approach used to evaluate and apply SRB reliability data can be summarized as follows:

1. Identification of key data categories available for the SRB from the data resources.
2. Review of the AIAA report and careful identification of all information needed to achieve maximum retrieval of data points available from SRB failure-launch records.
3. Computerization of SRB reliability database in a format that is most convenient for the data analysis using various statistical approaches.
4. Detailed data review to identify groups of SRB parametric data based on failure frequencies observed.
5. Estimation of SRB failure probability as a function of design parameters.
6. Overall estimation of SRB failure probability using Bayesian approach.

DEVELOPMENT OF SRB RELIABILITY DATABASE

The fundamental source of SRB data used in this study was the "International Reference Guide to Space Launch Systems," documented by AIAA (hereafter referred to as the AIAA report). For this study, we have focussed our effort on the data from the AIAA report, since this data has diversified SRB parameter types, it is consistent over 10 countries worldwide, and was comparatively easier to retrieve. Future efforts may take advantage of additional data sources as they become available.

A two-step approach was used in establishing the SRB reliability database:

a. Identification of key data categories from the SRB data set: Identification of key engineering parameters was first carried out to extract only the necessary information needed for evaluating the SRB design parameters, properties, attributes, and operational characteristics. There were 14 major data variables identified. These data variables were reported consistently among all the existing SRB design. This data was considered essential to categorize SRB failures from an engineering standpoint.
The key variables identified from the AIAA report are: country ID, vehicle ID, propellant type, propellant mass, gross mass, diameter, length, average thrust, specific impulse (ISP), nominal burn time (NBT), chamber pressure, vehicle success over launch ratio (S/L), SRB failure over launch ratio (SRB/F), and failure mode.

b. Computerization of the SRB database: The data sets of SRB parameters and failure-launch records were loaded on the computer and the computerization of the database was accomplished using a relational data structure that was implemented via DBase IV software. A simple field structure was also adapted in the construction of the SRB database to ensure quick and easy retrieval of data points.

SRB DATA REVIEW AND ANALYSIS

The main objectives of the data analysis using the SRB reliability database can be described as follows:

a. summarize the SRB parametric data and failure data,
b. identify systematic variations in the data sets,
c. estimate SRB failure probability and uncertainty bounds for all categories of parametric data,
d. test for a potential relationship between the SRB physical specifications and failure probability.

SRB flight records, even though limited, are useful for statistical analysis in revealing systematic variations among engineering variables in the data sets. In the process of data review, every piece of information was carefully examined to identify and extract the names and engineering parameters of the solid rockets. Specific attention had been focussed on information about parameters used to define solid rocket types and applications. The launch-failure records at the vehicle level, stage level, as well as strap-on rockets were also completely reviewed to identify the SRB failure data.

The key data categories that were identified in the data review process as showing a clear correlation between failure events and design parameters were: thrust, diameter, length, grossmass, nominal burn time (NBT), and chamber pressure. The data review has also resulted in defining different SRB types based on design parameter ranges. Since the available SRB information contained in the AIAA report was collected from 10 different countries worldwide, the SRB types according to major engineering parameters were so diversified, and parameter ranges were so wide that a direct use of SRB data without proper classification will clearly not be useful. For instance, the solid rocket diameter in the data set ranges from 0.1 m to nearly 4.0 m and the chamber pressure ranges from 600 PSI to 1300 PSI. Therefore, it is necessary to classify (categorize) the SRB data set based on major engineering parameters into a few classes with each containing sufficient data points and manifesting homogeneity.

Using descriptive statistical methods and the associated summary statistics for each of the key parameters, the data sets can be reduced (or classified) into three or more SRB types. Among all the SRB engineering parameters established in the database, seven were identified as key variables that would reveal any possible correlations with SRB operational and risk characteristics. Statistical methods were applied to these data sets in order to identify systematic variations among engineering variables and their design reliability specifications.

POINT ESTIMATE OF SRB FAILURE PROBABILITY AS A FUNCTION OF DESIGN PARAMETERS

One of the major objectives of data analysis using the SRB parametric and failure data sets was to identify possible systematic variations of failure probability in relation to changes of SRB design parameters and engineering properties. A straight forward approach to explore possible existing phenomena between SRB failure probability and the engineering parameters was to obtain point estimates of the failure probabilities and the associated uncertainties based on each parametric category of SRB data sets. This rudimentary but straightforward investigation was an important step in the first phase of our data analysis process. The results obtained from the point estimate within each SRB data class, along with corresponding failure probability plots not only provided us with interesting comparisons, but also led us to apply more complex quantitative methods for determining the significance of relationships between SRB failures and governing design parameters.

The point estimate, mean values and associated 90% confidence bounds of failure probabilities were calculated within each of the key parametric data categories. A classical maximum likelihood estimator (MLE) based on the demand related failure model was used in the point estimate of SRB failure probabilities. Figure 1 and Figure 2 show the resulting point estimates of SRB failure probabilities and the associated uncertainty bounds for some of the key parametric data categories. It is interesting to note that among the key design parametric categories, the diameter and gross mass seem to manifest considerable positive correlations between increased parameter values and the corresponding SRB failure probabilities. However, it is equally important to understand that the limited number of data points within some of the parameter ranges resulted in large uncertainty intervals around the means.

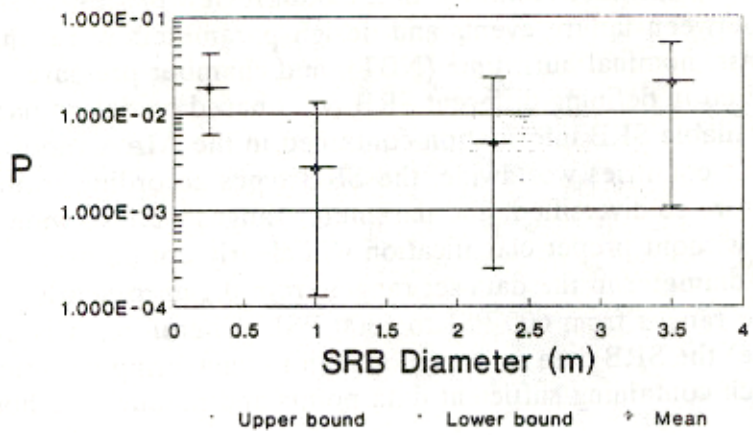


Figure 1. SRB failure probability by diameter type.

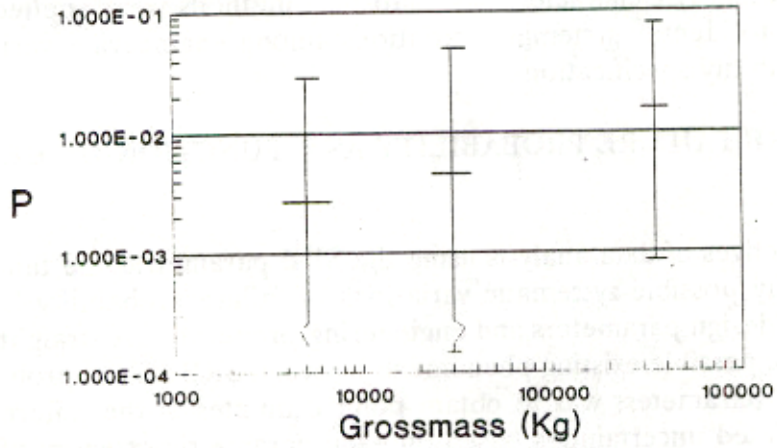


Figure 2. SRB failure probability by type of grossmass.

OVERALL ESTIMATE OF SRB FAILURE PROBABILITY

Although the point estimations of SRB probabilities, according to different parameter types were our primary focus, an overall SRB mean population failure probability estimate based on the entire data set was computed mainly for the purpose of comparison with the previous studies.[3,4] As a secondary objective we wanted to assess whether or not, in this reliability database, all the SRB failure data arise from the same homogeneous population. Therefore, some statistical test was needed to determine whether or not the SRB failure data collected by AIAA from different countries manifested homogeneity in the SRB population as a whole.

Statistical Test on Data Pooling

A chi-squared homogeneity statistical test was first performed to justify the pooling of SRB failure and launch records from different countries. Because of the sparsity of SRB failure data, a proper chi-square test could not be performed based on the SRB sample data from the nine countries as a different population. Therefore, to insure the validity of such a chi-square test, we grouped the SRB failure data into

two major populations, namely the data from the USA and all other countries combined.

It is worth noting that in the process of performing the chi-square test, 25% of the cells have expected counts < 5. This implies that such a chi-square test may not be a valid test on the underlying 2x2 table. However, to avoid such weakness in the chi-square test, a Fisher's exact test of independence in 2x2 tables was performed to verify the test results. In performing Fisher's exact test, the row and column margins (marginal frequencies) in the 2x2 table (Table 1) were considered fixed, and the exact probability of every given configuration of frequencies were evaluated, which was the hypergeometric probability of every possible table. The Fisher's exact test yields a p value of 0.714 indicating that the null hypothesis of independence between columns (SRB from the USA and others) and rows (SRB failures and launches) cannot be rejected.

Table 1. Fisher's exact test table (table of outcome by country).

	Other	USA	Totals
Failure	3	6	9
Launch	277	725	1002
Totals	280	731	1011

Fishers Exact Test	P value
(Left)	0.781
(Right)	0.475
(2-Tail)	0.714

Classical Estimation

Based upon the test results described above, the overall estimate of SRB mean population failure probability using pooled data was performed by both classical and Bayesian approaches. The classical estimation method, namely, the maximum likelihood estimate (MLE) and the confidence bounds based on the F distribution as described earlier, was used. This resulted in a mean value of 8.982E-3 with a 90% confidence interval of a lower 5th percentile at 4.701E-3 and a higher 95th percentile at 1.557E-2. The overall SRB failure probability estimated entirely based on the AIAA data source was fitted to a lognormal distribution. The estimated error factor was 1.86.

Bayesian Estimation

Considering the sparsity and limited sources of SRB failure data, the Bayesian updating approach was a useful method for a more statistically sound estimation of the overall SRB failure probability determined by incorporating the results of a previous study.

In lieu of estimating the SRB overall failure probability using the Bayesian approach, the estimate of SRB failure probability reported in Reference 4 was used as prior distribution, which was lognormally distributed with a mean of 1.1E-2 and an error factor of 2.84. BNL's Bayesian updating software code, BAYES, was developed

for the calculations needed for this study.[5-6] In this Bayesian updating process, a beta-binomial failure model was used to generate the parameters of the posterior distribution. Since the prior distribution was a single log-normal distribution, a conversion from log-normal to a beta distribution was performed to use previously estimated result as a prior for Bayesian updating. This conversion was done by using the technique of matching the mean and variance of the two distributions.

In developing the BNL Code "BAYES" and to calculate the parameters of the posterior distribution, BNL's SRB failure data evidence from the AIAA data source (i.e., k failures out of n SRB flights) was incorporated into the following updated mean E(p) and variance V(p) for the resulting posterior distribution:

$$E(p) = \frac{a+k}{a+b+n} \qquad (1)$$

$$Var(p) = \frac{(a+k)\ (b+n-k)}{(a+b+n)^2\ (a+b+n+1)} \qquad (2)$$

It can be seen that after the evidence data are observed, the classical estimator of a failure probability, k/n, is updated by using the mean of posterior distribution. However, using the BNL code "BAYES" based on the techniques described above, the updated final results of overall mean SRB population failure probability was consistent with the previous estimate, which was within a small margin of about 13% difference, with a mean value of 8.89E-3, lower 5th bound at 5.31E-3, upper 95th bound at 1.37E-2 and a log-normal error factor at 1.67. Figure 3 shows the comparison of estimated overall SRB failure probability.

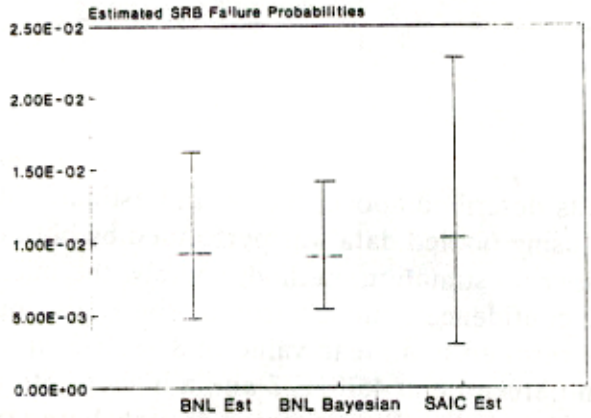


Figure 3. Comparison of overall SRB failure probability.

In order to identify correlations between failure frequency and engineering parameters, an effort was made to carefully review all the information throughout the AIAA report as well as the complete SRB database. However, some rudimentary investigation of the failure data and the parametric data indicated that some interesting relationships might exist between design parameters and the failure probability.

To test this assumption in a statistically sound manner and to determine quantitatively whether any correlation existed between the engineering variables and the failure probability, a set of straight plots of failure probability versus major engineering variables were developed. However, to quantify the magnitude of correlations and their statistical significance level, the Kruskal-Wallis non-parametric test was used to identify the underlying hypothesis. These test results and findings led to some of the conclusions that are summarized below.

SUMMARY AND CONCLUSIONS

1. Solid rocket booster mission failure probabilities were estimated in the following two ways: a) a point estimate of SRB failure probability as a function of design specifications, in which estimations were performed in accordance with key engineering parametric data categories (This parameter-driven SRB failure probability can be used for the purpose of risk and reliability evaluations at the SRB design stage), and b) the overall SRB mission failure probability using both classical and Bayesian updating estimation techniques. The statistical confirmation of overall SRB data pooling was further substantiated by a Fisher's exact test. Hence, the failure probability estimations were made by pooling failure data across all countries within the database. These estimated results showed consistency with the results from previous studies, which was within a small margin of about 13% difference.

2. Correlations between SRB mission failure probability and the engineering parameters were identified based on results from point estimates as well as non-parametric statistical tests. As a result, most major engineering parameters showed a general positive relationship with the SRB failure probability. Two out of the seven key engineering variables, i.e., diameter and gross mass, showed statistically significant correlations with the SRB mission failure probabilities. Moreover, systematic variations were found in the parametric and failure data sets using Spearman's rank correlation statistical test.

3. As a result, based on application of the SRB mission failure probability assessment methodology established in this study, a procedure guide for SRB failure probability evaluations can be provided for the purpose of design reliability estimation based on SRB specifications. Considering the findings of the relationship between failure probability and engineering parameters, a 4-step preliminary procedure guide was developed.

REFERENCES

1. "International Reference Guide to Space Launch Systems," American Institute of Aeronautics and Astronautics, Washington, D.C., 1991.

2. Special Report, The Space Shuttle: A Case of Subjective Engineering, IEEE Spectrum, June 1989.

3. Space Shuttle Integrated Risk Assessment Program (SIRA), SAIC, 1991.

4. Space Shuttle RTG Risk Assessment Report, SAIC, September 1988.

5. Azarm, M.A. and Hsu, F., ""PC-Based Tools for Reliability Estimations," BNL, June 1992.

6. Azarm, M.A. and Chu, T.L., "On Combining the Generic Failure Rate Data for Probabilistic Risk Assessment," Proc. of PSAM, pp. 1525-28, 1991.

THE DEVELOPMENT OF RISK PROFILES FOR SPACE AND MISSILE LAUNCH RANGE SAFETY DECISIONS[1]

Lloyd L. Philipson[2]

ACTA Inc.
23430 Hawthorne Blvd
Torrance, CA 90505

INTRODUCTION

Space and missile ranges in the United States characterize launch risk primarily by the expected number of casualties, or casualty expectation, E_C, that could result from launch failures. However, there has been a developing concern for specifically identifying any potential for "catastrophic" numbers of casualties given especially the increasing sizes of launch vehicles. Risk profiles that describe the probability of exceeding any possible casualty level resolve this concern. This paper briefly summarizes the methods that have been developed for deriving risk profiles for the several range hazards, and for their combination. The general risk profile derivation process is illustrated in Figure 1. The development of the profile for a given mission and also the aggregation of mission profiles, e.g., over a year, to support annual risk management are indicated. The process is specialized for analyses of the three principal launch range hazards in the following sections.

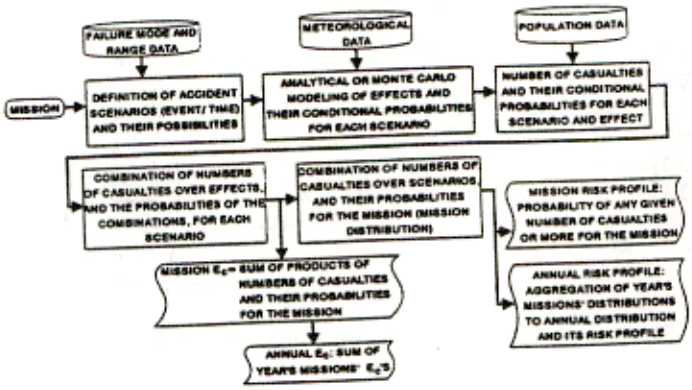


Figure 1. General risk profile derivation process.

---

[1]The investigations described in this paper were performed under the sponsorship of the U. S. Air Force 30th and 45th Space Wings, Safety Directorates, Contract No. F04703-91-C-0112, but their results are neither approved nor disapproved by the Air Force.

[2]Consultant to the U. S. Air Force Space Command, 30th and 45th Space Wings, Safety Directorates, via ACTA Incorporated, Torrance, California

THE THREE RANGE HAZARD MODELS AND THEIR RISK PROFILE DERIVATIONS

The principal hazard models at the ranges address toxic, long-range blast, and debris hazards. An essential requirement met by the new risk profile derivation procedures is that they do not perturb the primary computer programs that implement these models, but operate using input and output data of the primary programs in post-processing modes. A second requirement is that the mean value of the casualties distribution from which a risk profile derives should match as closely as possible the value of casualty expectation produced by the primary model. In two of the three hazards' risk profiles this is accomplished exactly; in one, the debris hazard, only approximately, but enhancements are under development [1 and 2].

Toxic Hazard

The Launch Area *Toxic Risk* Analysis (LATRA) program was developed to replace, with a comprehensive assessment of casualty risks, the former deterministic identification only of the areas in which the concentration or dose of a toxic effluent exceeds some acceptable standard [3 and 4]. LATRA's risk profile derivation procedures are:

1. Prompt the user to enter or modify the input data via menu options. The data files include the vehicle failure rates file, the rawinsonde meteorological profile, and the population library containing population counts or percentages by *receptor* area (population center), health category, and shelter type.
2. Initiate a *scenario* with the occurrence of a particular accident mode (conflagration, deflagration) at a particular altitude in flight, with its corresponding probability.
3. Monte Carlo relevant meteorological parameters' values to continue each scenario with a specific Monte Carlo case of these values, accounting for the correlations in them.
4. Run a dispersion model with the accident and meteorological parameters selected as inputs to develop for each given toxic effluent the resulting distribution of concentrations versus time of the toxic material of concern across the set of exposed receptors. Model the concentrations that result in the interiors of several types of structures at the receptors.
5. At each receptor and for each structure type apply an exposure-response model to each population subgroup (at present, children, aged, bronchitics; healthy adults) with a particular level of susceptibility to health effects from the toxic material, and for each considered level of severity of such health effects. Derive thereby the probability of occurrence of at least each level of severity of effect for each subgroup. Figure 2 exhibits examples of the requisite exposure-response functions that have so far been developed.

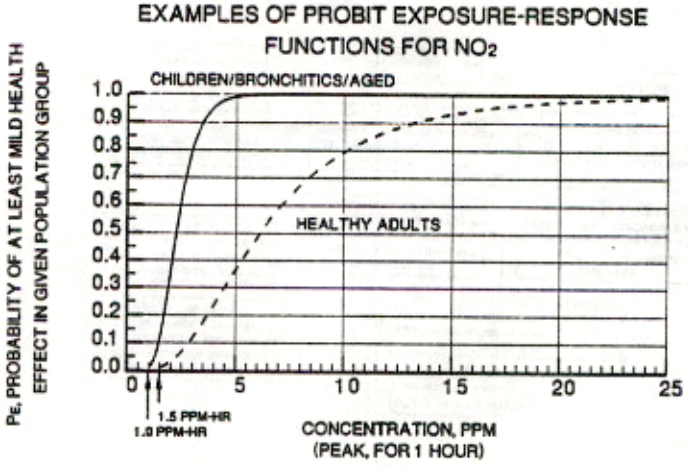


Figure 2. Examples of probit exposure-response functions for NO_2.

6. At each receptor, this probability is the parameter of a binomial distribution for the total number of individuals in the subgroup at the receptor who suffer at least that severity of effect.
7. Convolve the binomials by adding their means and variances at the receptors to obtain the mean and variance of an overall approximating normal distribution (based on the Central Limit Theorem) of the total number of all of the people suffering some severity of effect. (Alternative means for obtaining the convolutions can be applied when the population sizes and exposures are such that the normal approximation is not satisfactory.)
8. A distribution has now been derived for the number of casualties for each subgroup/severity and for

the total population for the scenario that began with a particular accident mode, vehicle altitude, and case of meteorological parameter values. Aggregate these distributions over the scenarios by discretizing them and then adding their frequencies in each discrete interval weighted by the probabilities of occurrence of the scenarios. The results are aggregated discrete distributions for the mission. The weighted sum of the means of the scenarios, i.e., the mean of each mission distribution, is the mission E_c for each subgroup/severity and overall.

9. Derive a risk profile for the mission for each subgroup/severity and for the overall population from the corresponding distributions by computing for each given number of casualties the sum of the probabilities of all numbers of casualties equal to or greater than the given number.
10. The effects of multiple toxic exposures from a given launch accident can be expressed in combined risk profiles. These are calculated by developing joint probabilities of effect from the individual toxics' probabilities of effect, assuming their independence. This assumption is probably conservative because of the high level of correlation that can be expected among the individual toxic exposures. However, it neglects any possible synergistic effects of the multiple exposures. The joint probabilities of effect are applied to the population categories and the resulting casualty distributions and risk profiles are generated as before.

The foregoing procedures have been implemented and risk profiles produced, including those for the September 25, 1992, Titan II Mars Observer launch at the Eastern Range. Examples are shown in Figure 3. These and all subsequent risk profiles should be considered illustrative only. The profiles exhibit the probability per launch of any possible number of children, aged, and bronchitics, or of healthy adults, suffering at least a mild effect from nitrogen dioxide (NO_2) and hydrogen chloride (HC_l), for one-hour exposures to time-averaged concentrations. The expected numbers of people in each subpopulation and overall who suffer an effect (i.e., at least mild) are the E_c values shown.

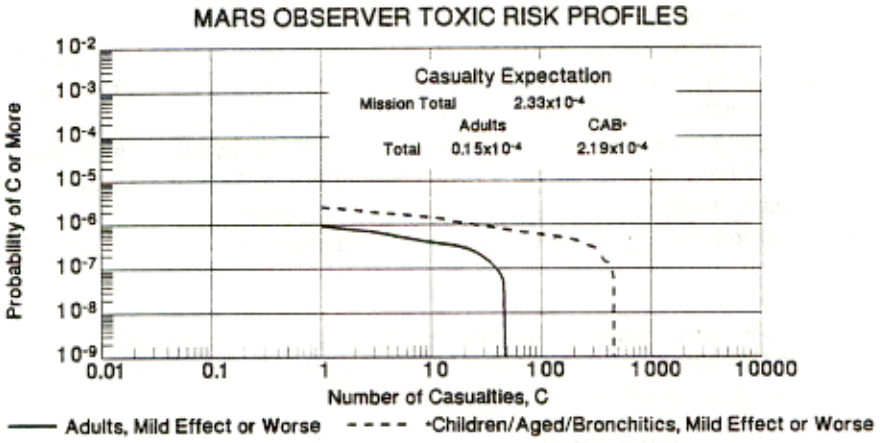


Figure 3. Mars observer toxic risk profiles.

Blast Hazard

The long-range *blast risk* from a launch is estimated with the BLASTX program [5]. The inputs to BLASTX are an estimation (that can be treated parametrically) of the potential explosive yield from a detonation occurring with a given probability in an accident on the pad or early in a launch; the predicted atmospheric conditions relevant to the propagation of the blast effects from such a detonation; the locations of the population centers that the effects may reach; the numbers of structures of various types within each population center; the numbers of windows of each of several size and strength classes in the structures; and the expected number of people in each structure during the daytime or at night, depending on when the launch is to take place.

Effects *scenarios* are defined by means of Monte Carlo sampling of the possible accident explosive yields, and atmospheric conditions. Ray-tracing is used to analyze the propagation of the blast effects for each sample. BLASTX predicts the static and dynamic overpressures on the windows in the structure of each type at each location and applies a breakage model to estimate the probability each window will break, and then computes the total expected number that will break. The overpressure prediction takes into account the possible focusing of the rays into caustics with overpressure extremes.

The sum of the expected numbers of breaking windows over the Monte Carlo samples, weighted by the samples' probabilities of occurrence and the probability of occurrence of the initial explosion and yield, is then the total expected number of breaking windows from the launch. Casualty modeling is based

on assuming that the individuals in each structure are exposed to each window in the same proportion that a window's *casualty area* is to the structure's total floor area. The casualty area is modeled so as to take into account the overpressure on the window and the room size as well as the class of the window. It is assumed that an individual in such an area will be a casualty, caused by a glass fragment, if the window breaks. Different severities are treated.

In the derivation of blast risk profiles the windows are categorized in each scenario so that each category has a common probability of breaking and a common conditional expected number of casualties given a break. Then a binomial distribution applies for the number of windows that break in each category and (from the Central Limit Theorem) an approximate normal distribution applies overall. An additional assumption generally enables the application of a Poisson approximation to the number of casualties in each scenario.

1. The main routine (BLASTX) Monte Carlo samples many possible cases, or scenarios, of atmospheric conditions in modeling the long range blast effects of a launch failure and explosion. The failure and explosive yield may be accounted for probabilistically in the scenarios, or as given conditions with a specified probability of occurrence.
2. For each case, the number of windows in each category of windows is determined. Since the windows in a category all have the same probability of breaking, and are assumed to break independently, the number of windows that, in fact, break in a category is binomially distributed. The sum over the categories of the numbers of breaking windows is then approximately normal.
3. The sum normal distribution obtained in this way for each scenario is discretized, the discrete distributions are aggregated over the scenarios, and a risk profile for the number of breaking windows is derived from the final distribution as was described for LATRA.
4. The approximate risk profile for the number of casualties caused by the breaking windows is derived as follows. In most cases of interest, the expected number of individuals in any window's casualty area, obtained before, is small. Hence it is assumed to be approximately equal to the probability that exactly one individual is in the casualty area. Since the windows in a given category have the same expected number of individuals in their casualty areas, they have the same probability of one individual. The number of casualties for the category is assumed to be binomially distributed with parameter equal to that of the number of breaking windows times this probability. A Poisson approximation generally applies for each category's casualties and so over all of the categories for a scenario.
5. The scenarios' distributions are aggregated to a final distribution and the casualty risk profile is generated as before.

Figures 4 and 5 are window breakage and total casualties profiles for the Mars Observer launch with their corresponding E_W and E_C values, respectively. Different casualty severities are assumed to be 45% Mild, 50% Significant, and 5% Fatal of the total.

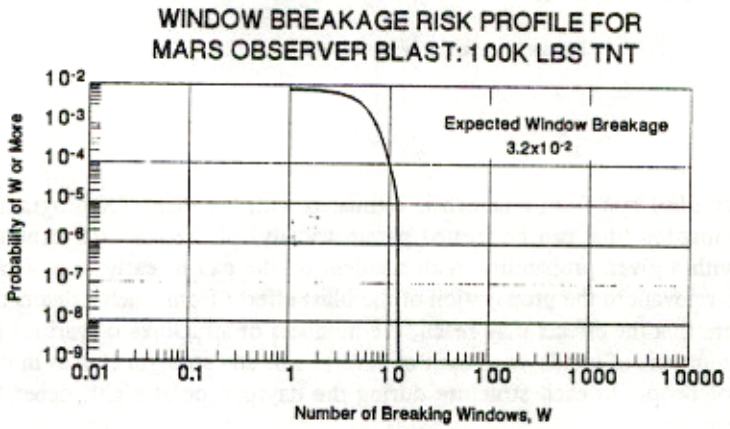


Figure 4. Window breakage risk profiles for Mars Observer blast: 100K lbs TNT.

Debris Hazard

The *debris risk* in a launch is estimated with the Launch Risk Analysis (LARA) program [6]. Its inputs essentially include the estimated probabilities of occurrence of different *failure modes* for a launch vehicle during a sequence of time intervals from launch until it is no longer hazardous to people on the ground; the counts and characteristics of the fragments of a number of *fragment groups* modeled as occurring

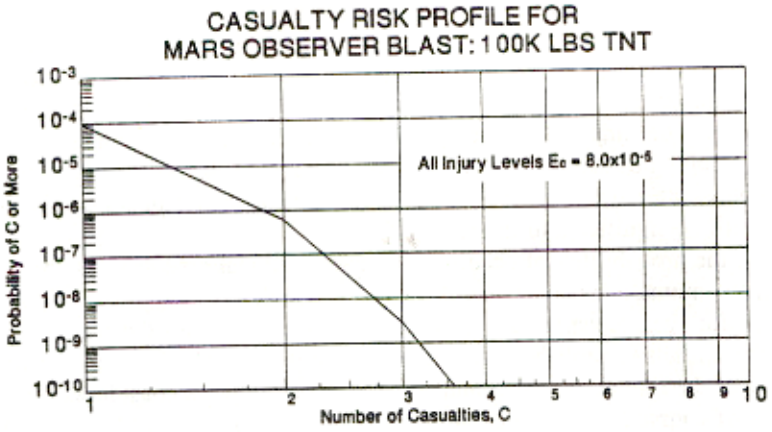


Figure 5. Casualty risk profiles for Mars Observer blast: 100K lbs TNT.

at a given time and due to a given failure mode; the wind and other atmospheric conditions versus altitude predicted for the time of launch which affect the fragments' aerodynamics; and the locations, areas, and populations of *population centers* that could be impacted by the group's fragments. The failure modes include on-trajectory thrust termination causes, and causes of malfunction turns in different directions. The vehicle may then breakup due to aerodynamic stresses or it may be destroyed by command from the ground or, for some vehicles, automatically by a self-contained destruct system. The fragment groups are defined so that the fragments in a given group have, given the predicted atmospheric conditions, the same bivariate normal probability distribution for their possible impact locations on the ground, and (taking into account whether the groups' fragments are explosive or inert) the same areas in which casualties will occur if an impact occurs within (or, for explosive fragments, sufficiently near to) a population center. The population centers (individual structures or areas containing many structures and outdoor regions) are defined so that their populations can reasonably be assumed to be uniformly distributed. The population of a center is divided into subpopulations in several levels of sheltering and so vulnerabilities to the fragments of the different groups.

LARA then computes, conditional on the occurrence of a given failure mode at a given time, or *scenario*, the probability of impact of the fragments of each group on each population center (determined by the location and area of the center in relation to the impact distribution, with some variations for explosive fragments), and the expected number of casualties at each center from the fragments of each group. The principal outputs are the compound probabilities for the launch that each center, and also at least one center overall, will be impacted by at least one fragment, and the expected number of casualties at each center and overall. The separation of casualties into significant injuries and fatalities has been established. The initial assumption is that of an equal allocation to each injury level.

Inert Debris. The development of inert debris risk profiles is fundamentally more difficult than that of toxic and blast risk profiles. While the impact locations of fragments are imperfectly but reasonably assumed in LARA to be independent, the distributions of the number of impacts of fragments on centers are *not independent*. If a fragment impacts one center, it is not available to impact any other center. A complete calculation of the number of casualties would take this into account in a correlated convolution over the centers to obtain the distribution of the total number of casualties. This is not computationally feasible given the large numbers of fragments (20 to 30 groups averaging perhaps 20 fragments each) and centers (generally several hundred).

Thus, a basically different approach has been taken to the derivation of inert debris risk profiles [1 and 2]. It extends the scenarios initiated by the occurrence of particular failure modes at particular times and the resulting generation of specified sets of fragment groups, to the causation of particular mutually exclusive partitions of the fragments on the centers (including a "miss center" to which are allocated all those fragments in a given partition that miss all population centers). These partitions are referred to as *lay-downs*.

1. For a given scenario, the combinatorial probability of each possible lay-down is calculated. The number of casualties caused by each lay-down is the sum over the population centers of the numbers of casualties caused at the centers by the lay-down's specific fragment impacts. (The possibility of multiple fragment hazard areas overlapping at a given center and thereby resulting in less than the sum of the casualties over the fragments is ignored conservatively in LARA. This is a negligible error for inert fragments.) Since the lay-downs are mutually exclusive, each one terminates a mutually exclusive

sub-scenario. In principle, it is then easy to aggregate all the sub-scenarios in all the scenarios to produce a distribution for the total number of casualties. In practice, however, the number of lay-downs, and so sub-scenarios, can be astronomical and their complete evaluation computationally infeasible. Thus, approximations based on limiting the number of lay-downs that need to be considered have been developed. The simplest involves the limitation to a total of two impacts on centers. As will be seen in an example, this has been only partially successful because, while the probabilities of individual lay-downs with more impacts are indeed very small, their number can be very large so that in total they can still be significant to the risk.

2. For each scenario, the probabilities of occurrence and (conditional expected) numbers of casualties are computed for all the mutually exclusive lay-downs considered.
3. Aggregating these for each scenario, and then over the scenarios with the scenarios' probabilities as weights, gives the casualties probability distribution for the launch, from which the risk profile is derived. Because of the limitation of the number of fragment impacts considered, the E_C derived from the risk profile is of course less than the complete value directly calculated by LARA (in which only the expected numbers of fragment impacts on centers and the corresponding expected numbers of casualties are treated). So the derived risk profile also falls short of the ideally complete one for the launch. As an interim measure, the contribution of the neglected possible impacts to the risk profile is approximated by simply scaling the calculated probabilities in the final casualties distribution by the ratio of the LARA-calculated E_C to that calculated from the distribution.

Explosive Debris. Impacts of explosive fragments can be outside population centers and still cause casualties within them, and several centers can be affected by a single impact and explosion. Consequently, the lay-down procedure employed for inert fragments is not applicable. However, there are many fewer explosive fragments than inert fragments. A Monte Carlo procedure can be employed which enables explosive debris risk profiles and also a superior computation of explosive debris E_C than is presently implemented on-line (with the restrictions this entails) in LARA. The procedure as follows:

1. For each LARA scenario (failure mode and time), Monte Carlo the LARA-generated impact location distributions for the fragments of each of the explosive fragment groups to derive a sample of the impact locations of all of the fragments.
2. Decompose each population center into a set of cells to enhance the fidelity of the computation of explosive effects at the center. (This has not been done for the computations in this paper; only entire centers are considered.)
3. For each fragment impact and its explosive yield (defined by the scenario and group), compute the distance to each cell and then, using the standard Kingery-BRL formulation, the explosion overpressure at the cell. Calculate the probability that an individual within a given category shelter exposed to this overpressure will be a casualty at a given level of severity.
4. For each cell, and each shelter category, combine the probabilities of casualty at the severity level from all the impacts in the sample. Multiply the combined probability by the population in the cell and shelter category and then add over all the cells and shelter categories to get the total (conditional expected) number of casualties for each severity level in the sample.
5. Repeat the sampling many times and derive a histogram for the frequency of each possible number of casualties at each severity in the scenario. Normalize the frequencies to probabilities by dividing by sample size.
6. Aggregate all the resulting scenarios' distributions, weighted by the scenarios' probabilities, to obtain the casualty distribution for the launch for each severity level and overall, and derive the corresponding E_C values and risk profiles as before.

Combined Debris. The total launch risk profile for all debris initially is obtained by convolving the two individual distributions for the inert and explosive debris and deriving the profile from the result. This is mechanized employing Fast Fourier transforms. Fidelity will be improved in the future by performing the convolution for each scenario before aggregating over the scenarios, to take into account the correlation of the two classes of fragments in each scenario. Figure 6 shows combined debris risk profiles for the Mars Observer launch.

Combination of Hazards

Given the casualty distribution for a given level of severity for each hazard, the convolution of the three distributions to obtain the total mission risk profile for each level of severity is straightforward. (When an individual distribution is for "*at least* a given level of severity," the distribution for ***exactly*** that level is

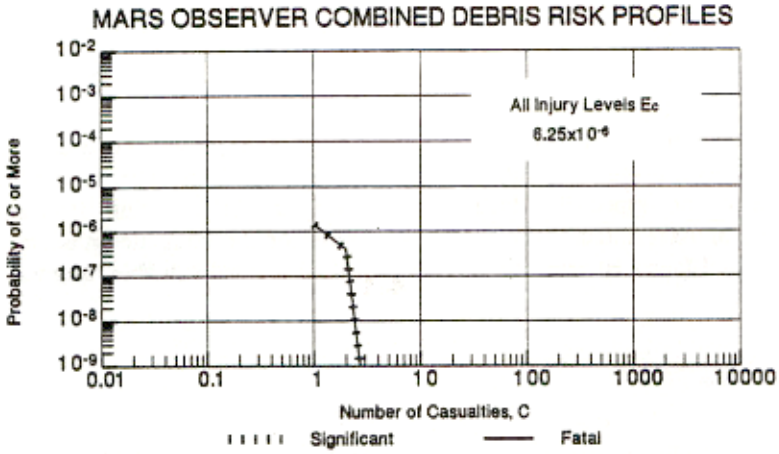


Figure 6. Mars Observer combined debris risk profiles.

derived first.) The combination is accomplished by first convolving the distributions for two of the hazards and then convolving the result with the distribution for the third hazard. As for combined debris, noted above, ultimately this will be done for each scenario, prior to aggregating over the scenarios, in order to reflect the effects of the correlation of the different hazards in a given scenario (failure mode and time). At present this is done only after the aggregation over the scenarios.

Examples of combined all-hazards risk profiles are shown in Figure 7. The profile for mild injuries is dominated by the toxic hazard; the blast hazard dominates the profiles for significant injuries and fatalities.

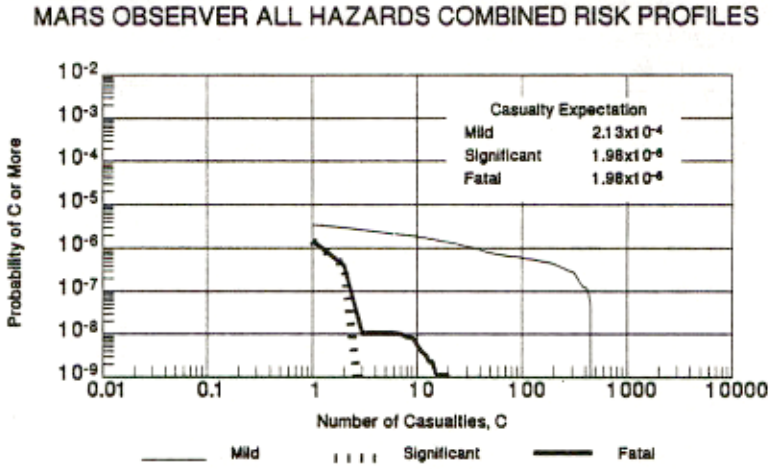


Figure 7. Mars Observer all hazards combined risk profiles.

CONCLUSIONS

Generally satisfactory procedures have been established for the derivation of risk profiles for the toxic and blast hazards and for the hazard from explosive debris in range operations. They meet the requirements of implementation as post-processing routines in relation to the primary hazard analysis programs, and of matching the value of casualty expectation produced by these programs. Procedures for combining the risks from the several hazards and deriving the associated overall mission risk profiles have also been developed and implemented. However, there remain certain needs for improvement.

The derivation of inert debris hazard risk profiles presents special difficulties. The number of lay-downs required to be evaluated to ensure a close approximation to the true risk profile is overwhelming in most cases of interest. However, procedures have been defined for the prior deletion of fragment groups and population centers which cannot contribute significantly to total risk, thereby diminishing the number of lay-downs needed to be evaluated. The smaller remaining number will permit the practical evaluation of more complete sets of lay-downs than those with only the two fragment impacts on centers so far treated.

For blast risk profiles, cases of larger numbers of exposed individuals for windows of special types need to be treated.

Lastly, to enable the combination of the risks for different levels of severity of effect, relative importance weights for the different levels need to be established through discussion and resolution with

ACKNOWLEDGEMENTS

The author wishes to express his appreciation for the support provided to him in the work described in this paper by the Safety Directorates, 30th and 45th Space Wings, Vandenberg Air Force Base and Cape Canaveral Air Force Station, especially Martin Kinna of the 30th SPW; Kevin Benn, Alan Bodner, John Piersol and Alex See of ACTA Inc., who were responsible for the computer implementations; and Jon Collins, Jerold Haber and James Hudson, also of ACTA, who provided valuable insights and reviews of the methods.

REFERENCES

[1] Haber, J.M. and L.L. Philipson, Range Safety Decision Analysis, Report No. 91-249/36-02, Prepared for USAF/45 SPW, Under Contract No. FO4703-C-0112, ACTA Inc., Torrance, CA, Sept. 1991.

[2] Haber, J.M. and L.L. Philipson, Calculation of Risk Profiles for Range Safety, Report No. 92-265/25-01, Prepared for USAF/30&45 SPW, Under Contract No. FO4703-C-0112, ACTA Inc., Torrance, CA, Sept. 1992.

[3] Haber, J.M., J.M. Hudson, L.L. Philipson and A.M See, LATRA Model Development, Report No. 92-265/17, Prepared for USAF/30&45 SPW, Under Contract No. FO4703-91-C-0112, ACTA Inc., Torrance, CA, Sept. 1992.

[4] See, A., J.M. Hudson, R. Nyman and L.L. Philipson, LATRA: Launch Area Toxic Risk Analysis Program, Report No. 93-282/36-01, Prepared for USAF/30&45 SPW, Under Contract No. FO4703-91-C-0112, ACTA Inc., Torrance, CA, Sept. 1993.

[5] Bodner, A.I., J.R. Westlake, M.R. Legg and K.B. Overbeck, Software Design Document for the BLASTX Computer Model, Report No. 92-236/06-01, Rev. 03, Prepared for USAF/30&45 SPW, Under Contract No. FO4703-91-C-0112, ACTA Inc., Torrance, CA Sept. 1992.

[6] Baeker, J.B., J.D. Collins and J.M. Haber, "Launch Risk Analysis," Journal of Spacecraft and Rockets, Vol. 14, No. 12, Dec. 1977, pp. 733-738.

RISK ASSESSMENT FRAMEWORK FOR THE CASSINI PLANETARY MISSION

Sergio B. Guarro[1] and Bruce Bream[2]

[1]The Aerospace Corporation, P.O. Box 92957, Los Angeles, CA 90009-2957
[2]NASA Lewis Research Center, 21000 Brookpark Road, Cleveland, OH 44135

Introduction and Acknowledgments

The Cassini mission is scheduled to send an unmanned spacecraft to the planet Saturn in 1997[1]. Because the spacecraft will be travelling in parts of the solar system where solar radiation is low in intensity, the electric power generation function will be entrusted to a nuclear Radioisotope Thermoelectric Generator (RTG) system, including three generators.

The presence of radioactive material on board requires the mission to undergo a thorough risk assessment and risk review process, culminating in mission approval to be granted at the presidential executive office level. Responsibilty for carrying out the mission risk assessment is shared among several Government and contractor organizations, with the NASA Lewis Research Center leading the space vehicle system portion of the assessment and the U.S. Department of Energy (DoE) reserving responsibility for the assessment of the potential consequences of a radiological release accident. This paper describes the risk assessment framework and process that is being developed to produce accident scenario accident definitions and probabilities that NASA will provide to DoE as input to the consequence assessment process. In the presentation of this framework, the authors wish to acknowledge the contributions made to the whole Cassini risk assessment effort by the representatives of other organizations, including NASA Headquarters, the Air Force Space & Missile Systems Center, the Jet Propulsion Laboratory, Martin Marietta, and General Dynamics.

Cassini PRA Framework

The progression of a typical launch vehicle accident sequence can be envisioned as being initiated at the lowest functional level by the failure of a specific mechanical part, electronic part or software subfunction. The initiating failure then propagates more or less rapidly, depending on the nature of the failure itself, up the functional hierarchy of the launch vehicle system, until it becomes manifest as a vehicle malfunction. i.e., as a serious departure from the nominal mission of the vehicle. Once a serious vehicle level malfunction occurs, and its nature is such that no recovery to a nominal mission is possible, the objective of the mission control function shifts into a safety protection and damage containment mode. The execution of these latter functions is entrusted to the Flight Termination System (FTS) design. The functionality of the FTS, which is typically composed of an automated portion and of a "man-in-the-loop" portion, consists of a malfunction detection subfunction and of a vehicle-destruct subfunction. Almost every possible type of unrecoverable vehicle malfunction results in the FTS-executed destruct of the launch vehicle and of the payload that it carries. Intentionally destructing the vehicle in flight assures that no life-threatening large pieces of hardware or large quantities of propellant fall back on earth and on populated areas.

A top-level view of the PRA modeling framework designed to best reflect the features of a typical Cassini mission accident sequence is represented in Figure 1. In this framework, three successive layers of accident sequence "pinch points" are identified above the level of initiating basic failures, namely:

- the AIC (Accident Initial Condition) layer,
- the AOC (Accident Outcome Condition) layer, and
- the RSE (RTG Sequence Endpoint) layer.

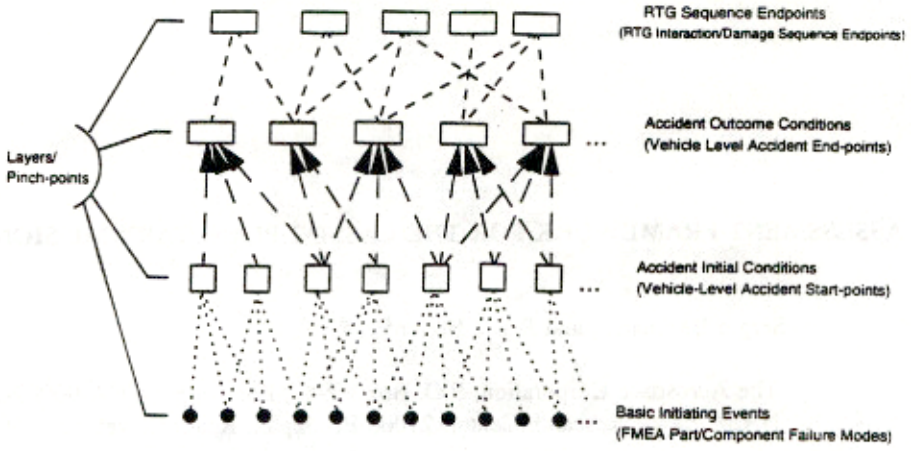


Figure 1: Top-View of Cassini PRA Models Framework

The definitions of the event types that are used as pinch points are as follows:

An AIC is the first manifestation, detectable at the launch-vehicle and/or spacecraft system level, of a serious malfunction that is intiating an RTG accident sequence.

An AOC is the first event in an RTG accident sequence which has the capability of producing a harmful effect on one of the RTGs, that is, any kind of highly energetic interaction between an RTG and the LV/Spacecraft system or the external environment.

An RSE is the final event of an RTG accident sequence, that is, the event by which the RTG receives the last potentially damaging interaction from any outside element (including LV or Spacecraft elements) and thereupon comes to rest in a state no longer subject to further damaging threats.

The pinch point layers in the PRA framework are intended to logically guide the modeling process through the steps of a typical accident progression, as defined in the brief discussion given at the beginning of the section. It should be noted that an AIC is not the lowest-level initiating cause of an accident sequence, as this role is played by the basic part-level failure events that themselves cause the AIC to occur. These events are identified in the lowest layer of the PRA framework depicted in Figure 1, under the denomination of BIEs (Basic Initiating Events). Thus, in the overall framework, BIEs will be used to identify the root-level causes of system malfunctions which, in turn, will be described by AICs. Once an AICs has been identified, analysis of the ensuing sequence possibilities will allow the identification of the different types of AOCs that may result. The AOCs will usually correspond to a highly energetic event, such as an FTS execution, or a propellant explosion, or a direct impact of the RTG with some other body or structure. A continuation of the sequence analysis beyond the AOC identification will finally determine whether other RTG-damaging interactions (or "insults," as they are often referred to) may follow the AOC itself, and by what sequence of events the RTG may come to rest and reach a stable RSE.

Details of Cassini PRA Models

Figure 2 illustrates the combination of models used in the Cassini framework and the fashion in which they are connected together to provide the desired identification and description of typical space-vehicle and RTG accident sequences. The lowest level of models is constituted of fault trees structures that show how BIEs (i.e., single failures or combination of failures of basic vehicle parts or components) can cause the failure of space-vehicle systems and the occurrence of an AIC. Because dynamic phenomenological effects are not expected to play a significant role in the propagation of failures from the basic BIE to the AIC system level, the static representation provided by fault trees is well suited for this portion of the Cassini sequence modeling. Once the fault tree models connecting AICs to the underlying BIEs are in place, the next two levels of modeling require the analyst to connect AIC events with the resulting AOC events, and the AOCs with the resulting RSEs. Because the phenomenology associated with these portions of the accident sequences is highly

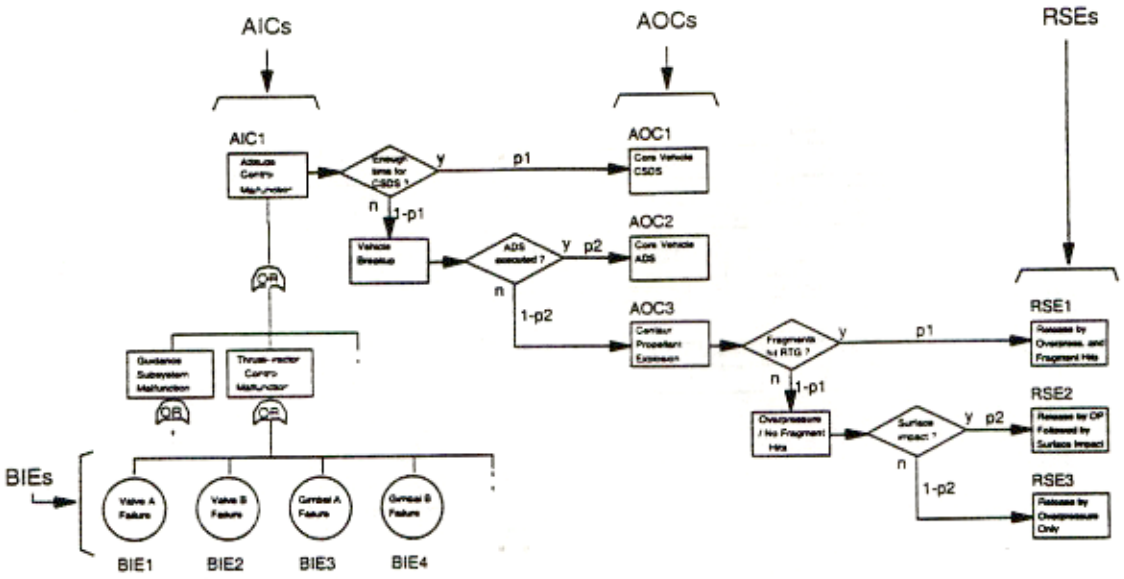


Figure 2: Integration of Cassini PRA Models

dynamic, event sequence diagrams are the specific type of modeling structures selected for this portion of the modeling. For the sake of clarity, the example represented in Figure 2 is considerably simplified, in terms of the amount of detail carried out in the models, with respect to the models that are being actually used in the Cassini PRA. Nevertheless, it is representative of the type of information that the Cassini PRA models produce and contain, and of the model logic structure that needs to be quantified in the probability assessment and analysis stage of the PRA process.

In the actual order of execution of the modeling activities, before the detailed modeling required to construct fault trees and event sequence diagrams is started, the Cassini modeling framework is set up by the construction of Master Logic Diagrams (MLDs) at the AIC and AOC event level. The MLDs provide an initial reference frame and reference set of AIC and AOC "pinch points," covering the anticipated span of possible AIC and AOC events, which is used as a guide for the derivation of the event sequence diagrams and fault trees analysis and assures that the set of AIC and AOC events that will be covered in detail in the event sequence diagram models corresponds to a "complete" set. Thus, the set of AIC events deductively defined by the AIC MLD represents all the physically possible AICs that can be identified according to the engineering knowledge of the Titan/Centaur/Cassini space vehicle that the analyst has access to. Similarly, the AOC MLD defines the spectrum of potentially damaging first interactions that can possibly take place during an accident sequence between the space vehicle system and the RTG. The deductive definition of AIC and AOC pinch points obtained via the derivation of the MLDs provides the analyst with a better assurance of completeness in the derivation of the Cassini accident scenarios than would be obtained if the identification of AOCs were left to the process of inductive accident sequence identification from AIC events onward to AOCs and RSEs. Figures 3 and 4 show the structure of the preliminary MLDs developed for the Cassini PRA

Relation of the Cassini Framework to Traditional PRA

The Cassini PRA framework is fully consistent with the established practices of the PRA methodology[2], including some of the concepts first introduced in nuclear power plant PRA by the "NUREG-1150" study[3]. Because the nature of space system accident sequences obviously differs from that of nuclear plant core-melt sequences, certain variations and adaptations had, however, to be introduced with respect to the modeling techniques adopted for the latter.

The points of analogy are easily identified. In the Cassini framework, AICs correspond to the

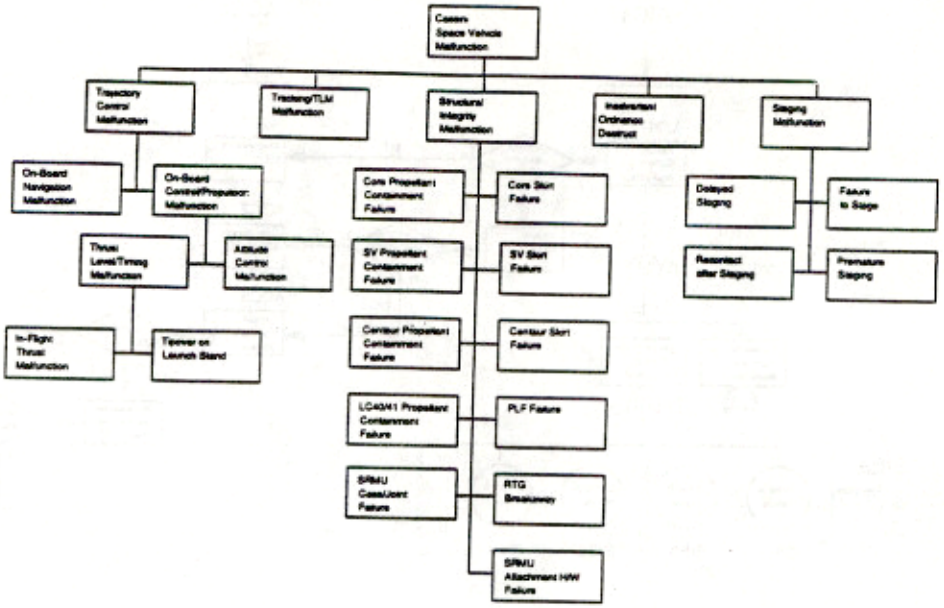


Figure 3: Cassini Accident Initial Condition (AIC) Master Logic Diagram

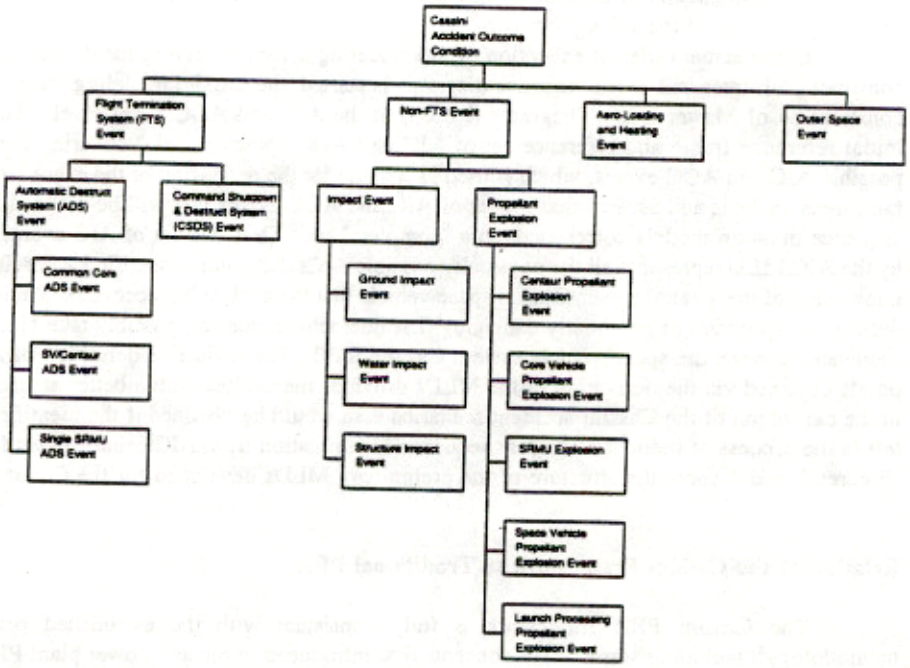


Figure 4: Cassini Accident Outcome Condition (AOC) Master Logic Diagram

"initiating events" of nuclear power plant PRAs, which are often further analized to identify their low-level underlying causes by means of fault trees, just like AICs are analyzed in the Cassini approach to relate them to the underlying BIEs. AIC-to-AOC sequences are analogous to initiating-event-to-core-melt sequences, which in nuclear plant PRAs are also modelled by means of event sequence diagrams (or their close relatives, the event trees). Finally, AOC-to-RSE sequences are the equivalent of core-melt-to-containment-failure sequences, which nuclear plant "Level 2" PRA such as NUREG-1150 also model with event sequence diagrams and/or event trees.

The main differences between the nuclear PRAs and the Cassini approach are dictated by the different nature of the accident sequences of interest. A space vehicle failure can produce a variety of outcomes. In fact the result of a system level malfunction can be, from the space vehicle point of view, a spontaneous break-up followed by an automatic self-destruct, a self-destruct commanded via radio by the mission control center, or various types of liquid tank or solid propellant explosions. Self destructs or spontaneous propellant explosions can also differ considerably among themselves, because of the physical configuration changes the vehicle itself undergoes as stages are being consumed and separated from the active portion of the vehicle. The variety of the types of AOCs that are possible explains the necessity of constructing, as we have explained in the preceding section, an AOC MLD before the actual sequences are derived, similarly to what is done for the AICs. This is unlike nuclear plant PRAs, where only one initiating event MLD (i.e., the equivalent of the Cassini AIC MLD) is usually derived. In such PRAs in fact there is no need to derive an "outcome event" MLD, since all sequences that start with an "initiating event" end into the same "outcome" pinch point, i.e. core-melt (unless of course they revert to a safe outcome not involving plant damage).

Overview of the Quantification and Bayesian Updating Process

The quantification of the Cassini PRA models, to arrive at the estimation of the expected per-mission frequency of the various accident sequences of interest, makes use of a weighted-likelihood Bayesian estimation of AIC frequencies and of a combination of conditional probability data, analysis and expert-judgment to quantify event sequence diagram split-fractions in the AIC-to-AOC and AOC-to-RSE event sequences. All event frequencies and conditional probabilities are expressed as distributions, to realistically represent the inherent uncertainty that exists with respect to their actual value.

The process adopted for the quantification of AIC event probabilities and AIC-to-AOC sequence probabilities is illustrated in Figure 5.

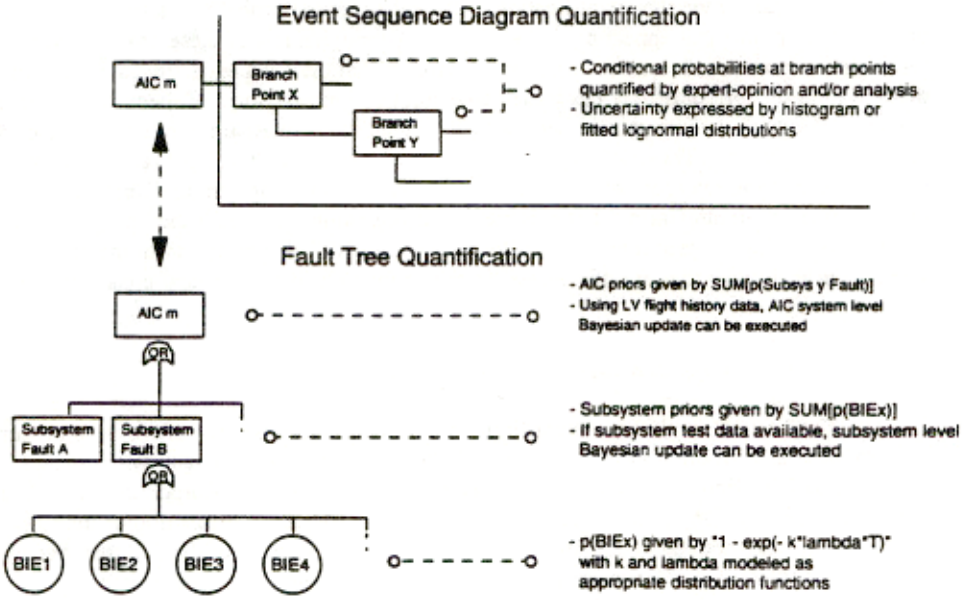


Figure 5: Cassini PRA Model Quantification Scheme

At the lowest level of the BIE-to-AIC fault tree model structures, BIE probabilities are typically expressed by exponential formulas of the type

$$(1) \quad p_{BIE} = 1 - \exp(-k\lambda t) ,$$

where t is the mission elapsed time, λ is the failure rate characterizing the failure mode(s) of the hardware represented in the BIE when operating in non-flight conditions, and k is a failure-rate-multiplying factor which, in the established reliability modeling practice of the aerospace industry, represents the negative effect of the severe flight environment (e.g., high vibration and thermal stress effects) on the mechanical and electrical parts of a space vehicle. Although not explicitly indicated in eqn. 1, k itself is a function of mission elapsed time, which can usually be represented as a series of step functions as the "environmental stress" goes up in vehicle boost phases and decreases in coast phases.

In the Cassini quantification scheme, prior state-of-knowledge distributions are constructed, mostly on the basis of FMEA (Failure Mode and Effect Analysis) generic failure data, for the k and λ terms appearing in eqn. 1. If no specific test data exists for the components or subsystems that appear in a BIE-to-AIC fault tree, Monte Carlo or Latin Hypercube techniques are used to directly obtain the prior state-of-knowledge distribution of the expected frequency of the AIC top-event for that fault tree. After this is done, a Bayesian weighted-likelihood updating process is applied to combine this prior distribution with the Titan-Centaur flight history evidence and obtain a posterior updated distribution for that frequency. If component or system level test data are available on certain elements of the vehicle, the just described process is modified and segmented as the illustration in Figure 5 indicates, to construct intermediate priors for the components or subsystems for which the test data is available. This makes possible to conduct an intermediate updating with the data existing for these components or subsystems and obtain for them "intermediate posteriors", which are then combined by Monte Carlo / Latin Hypercube operation with the priors of the other elements of the vehicle, before conducting the final AIC-level Bayesian updating operation as already has been described above.

As should be apparent from the description of the overall Cassini PRA model structures given in the preceding sections, AIC probabilities must be multiplied by AOC and RSE conditional probabilities in order to produce estimations of the frequency distributions of the AOCs themselves and of the various accident scenario categories of interest for radiological consequence estimations. The unconditional frequency (per mission) of the i-th AOC is calculated according to the formulation:

$$(2). \quad p_{AOC\,i} = \sum_{j} \left(p_{AIC\,j}\, p_{AOC\,i\,/\,AIC\,j} \right)$$

In eqn. 2, the $p_{AIC\,j}$ terms are the result of the AIC frequency estimation process just described above, whereas the $p_{AOC\,i\,/\,AIC\,j}$ terms, representing the conditional probability of a generic AOC given that a generic AIC has occurred, are the result of the quantification of the AIC-to-AOC event sequence diagram models, and as such are obtained via the quantification of the split-fraction probability terms that are associated with each of the branch points that appear on those models. Although a few of these probability values are known from reliability engineering databases (e.g., the probability that the vehicle destruct system will not function, given that the mission control officer has issued a destruct command), most of them depend on the highly dynamic phenomenological circumstances and boundary conditions that are modelled in the AIC-to-AOC event sequence diagrams. Thus, an expert elicitation process will be employed to derive state-of-knowledge probability distributions for each of the diagram branch points and these distributions will be combined via the appropriate Monte Carlo / Latin Hypercub e operations to obtain the $p_{AOC\,i\,/\,AIC\,j}$ terms of eqn. 2. A completely analogous procedure applies to the AOC-to-RSE diagrams and to the formulation of the accident scenario probabilities that are of interest for the estimation of radiological consequences by DoE.

Discussion of the Weighted Likelihood Approach

The limited number of actual flights performed in any one specific design or mission configuration is often cited as a problem in making use of flight history in risk or reliability assessment for space vehicles. The weighted likelihood approach was developed at the Aerospace Corporation specifically to address this issue and allow the use of historical data in the scenario frequency estimation of the Cassini risk assessment.

The weighted likelihood approach concept takes advantage of the fact that, even when flight data for exactly the vehicle and mission configuration of interest are not available, usually there exists recorded flight history for other types of vehicles having varying degrees of similarity with it. In the use of the Bayesian updating process for the estimation of the distribution of the expected frequency of a certain type of event (e.g., a particular accident initiating event), the likelihood function expresses the conditional probability of seeing the evidence which is being used to update the prior distribution of the event frequency parameter,

given the prior knowledge of the frequency parameter, and as a function of the possible values of the frequency parameter itself. If the evidence is fully applicable to the assessment of the parameter of interest, an appropriate form can be readily assumed for the likelihood function. For example, assume that we had the benefit of recording N flight missions exactly like Cassini (i.e., using the same Titan/Centaure/Spacecraft design and configuration, and the same mission profile), with n observed occurrences of Event X. Then the appropriate "total applicability likelihood function," L_T, for the representation of the evidence "n X-events in N trials," as a function of the per-Cassini-trial frequency of Event X, f_X, would be the binomial function, i.e.:

$$(3) \quad L_T = N! /[n! (N-n)!] \; f_X^n \; (1 - f_X)^{N-n}$$

Under normal circumstances, however, we would not have a relatively high number of trials for designs and configurations exactly like Cassini, but would have trials and outcomes for somewhat different vehicle designs and missions. Thus, to identify the appropriate form of the likelihood of such a type of evidence in relation to the Cassini Event X frequency estimation, we would be in the position of having to estimate the probability of evidence corresponding to "non-Cassini trials," based on the knowledge of the prior frequency of Event X for Cassini trials. If there were no relationship between the two types of trials, i.e., if the non-Cassini evidence had "zero applicability" to the Cassini trial frequency problem, the Cassini "zero applicability likelihood function," L_0, for the non-Cassini evidence would be simply a constant, reflecting the fact that knowledge of the Cassini Event X frequency would make no outcome of the non-Cassini trials to appear any more likely than another. The weighted likelihood approach is based on the recognition that the typical real situation under which evidence is gathered and applied is one of "partial applicability," i.e., a situation in which the evidence from designs and missions having some degree of similarity with the one of interest, is used to make predictions for the latter. Under these typical circumstances, it is assumed that the likelihood can be taken to be a weighted product of the two extreme forms -- i.e., "zero applicability" and "total applicability" -- of the likelihood function, i.e.:

$$(4) \quad L = L_T^{w} \; L_0^{1-w} = f_X^{wn} \; (1 - f_X)^{w(N-n)} \quad ,$$

where w is a fractional weight (between 0 and 1) assigned by the assessor to signify the "degree of applicability" of the non-Cassini evidence to the Cassini Event X frequency estimation problem.

In essence, the weighted likelihood approach seeks to address a difficult issue of data assessment explicitly and from a rationally justifiable perspective. Presently, for its application, the assessor is asked to use his/her engineering judgment in the assignment of the likelihood weight values (although in principle it could codified into "objective" procedures).

Status of the Assessment and Preliminary Results

In the current progress of the Cassini risk assessment activities, the MLD, fault tree and event sequence diagram models are being derived for the Safety Analysis Report (SAR) version of the assessment. An earlier and preliminary version of the assessment was executed to satisfy the mission Environmental Impact Statement (EIS) requirements[1]. In that version of the assessment only four accident scenarios, considered to be an approximate superset and summary of all possible scenarios, were considered and quantified. Because of the simplified nature of the EIS scenario assessment, it was not deemed necessary to include in it event sequence diagram models. Thus all vehicle BIEs were mapped directly into the four selected accident scenarios, which were then quantified by application of the weighted likelihood methods in a fashion closely resembling the scheme illustrated in Figure 5 for the quantification of BIE-to-AIC fault trees.

Table 1 presents the mean and key percentiles (5th, median and 95th) of the per-mission frequencies obtained for the four scenarios, as well as the corresponding values of the overall mission failure frequency. The results of the SAR cycle of the assessment are expected to produce a tighter range of uncertainty (5th to 95th percentile) for this latter parameter, because of the more detailed and complete nature of the models and associated analyses that are being developed.

References

1. "Titan IV CRAF/Cassini EIS Databook," Martin Marietta report MCR-91-2580, December 1991
2. E.S. Beckjord, M.A. Cunningham and J.A. Murphy, Probabilistic safety assessment in the United States 1972-1990, *Reliability Engineering & System Safety* 39 No. 2 (159), 1993

3. "Severe Accident Risk: An Assessment for Five US Nuclear Power Plants," USNRC report NUREG-1150, Second Draft for Peer Review, June 1989

Table 1: Cassini Risk Assessment Preliminary Results

		Frequency Distribution Values			
		5%	Median	Mean	95%
EIS Scenarios	Command Shutdown and Destruct (CSD)	1.9E-2	4.1E-2	4.5E-2	8.3E-2
	SRMU Failure to Ignite (Tipover)	2.2E-5	4.5E-4	1.4E-3	5.8E-3
	Centaur Collapse	1.9E-3	5.2E-3	7.0E-3	1.8E-2
	Reentry	9.4E-3	1.7E-2	1.7E-2	2.9E-2
	Total Mission Failure Frequency	4.2E-2	6.7E-2	7.0E-2	1.1E-1

RISKS AND ISSUES IN FIRE SAFETY ON THE SPACE STATION

Robert Friedman

Space Experiments Division
NASA Lewis Research Center
Cleveland, Ohio 44135

INTRODUCTION

A fire in the inhabited portion of a spacecraft is a greatly feared hazard, but fire protection in space operations is complicated by two factors. First, the spacecraft cabin is an enclosed volume, which limits the resources for fire fighting and the options for crew escape. Second, an orbiting spacecraft experiences a balance of forces, creating a near-zero-gravity (microgravity) environment that profoundly affects the characteristics of fire initiation, spread, and suppression.

The current Shuttle Orbiter is protected by a fire-detection and suppression system whose requirements are derived of necessity from accepted terrestrial and aircraft standards.[1] While experience has shown that Shuttle fire safety is adequate, designers recognize that improved systems to respond specifically to microgravity fire characteristics are highly desirable. Innovative technology is particularly advisable for the Space Station, a forthcoming space community with a complex configuration and long-duration orbital missions, in which the effectiveness of current fire-protection systems is unpredictable.

This paper briefly reviews the development of risk assessments to evaluate the probabilities and consequences of fire incidents in spacecraft. It further discusses the important unresolved issues and needs for improved fire safety in the Space Station, including those of material selection, spacecraft atmospheres, fire detection, fire suppression, and post-fire restoration.

RISK ASSESSMENTS FOR SPACECRAFT

Historical Development

Space systems are traditionally associated with the qualities of high reliability and safety. For missions prior to the present Shuttle, safety assessments were thorough but qualitative, based on analyses such as failure modes and effects.[2] Possible reasons for the slowness to adopt quantitative methods include the doubt that the involved calculations are the best use of scarce labor and computer resources and the fear that quantitative methods offer

the appearance of knowledge where knowledge does not exist (F. Fendell, TRW, personal communication, Nov. 1991). Recently, however, interest has arisen, counter to the earlier skepticism, in the application of limited-scope probabilistic risk assessments (PRA) to spacecraft.[3] In the past year, NASA has announced that a PRA will be conducted on the Shuttle systems to determine risk priorities and potential safety improvements.[4]

Fire Hazards and the Space Station

Previous space-field risk assessments usually had cursory treatments of fire hazards because of a belief that the probability of an internal fire is slight. Strict acceptance testing for onboard material selection ensured that very few, isolated flammable articles enter the spacecraft. In addition, experimental tests conducted under quiescent, low-gravity conditions in the Skylab space station indicated that fires spread very slowly in microgravity.[5] These assumptions are now shown to be optimistic even for the Shuttle, and they are certainly challenged by the increased fire-safety stresses anticipated in the operation of the Space Station. An initial safety review of the Space Station concept identified fire as a significant hazard among the major threats to the well-being of the station.[6] In the cited, comprehensive study, four approaches to fire-threat reduction were proposed: design to preclude (fire prevention), design to control (flammable isolation), protective devices (fire detection and suppression systems), and risk definition (minimum acceptance standards). For the risk definition, an optimization of risk, cost, and benefits established a realistic safety goal of a residual fire hazard that causes no injuries nor damage sufficient to suspend operations.

The maturity of the designs for the Space Station now warrants additional quantitative risk assessments. A study by Fuller and Halverson (cited by Kaplan[7]), though only partially completed, examined the consequences of six fire-initiation scenarios: electrical shorts/overloads, water-electrolysis unit failures, oxygen leaks, chemical reactions, payload-experiment failures, and improper crew or ground-control actions. A second independent study, still in progress, utilizes a PRA approach to calculate event probabilities and process times from initiating scenarios (wire overheating, for example) through threats (heat, smoke, and toxins) to alleviating responses (extinguishment).[8] The study is the first to include microgravity fire experiments to provide information on fire characteristics, emissions, and time constants for validation of the resulting risk assessment.

Operational Experience

Minor breakdowns in human-crew space missions that could progress into fires are by no means rare. In Shuttle missions, documented anomalies include five "incidents", at least six smoke detector false alarms, and at least five smoke detector built-in-test failures.[9] Thus, in 7969 hours of elapsed Shuttle mission time (data to October 1992), incidents have occurred on the average of once every 1600 hr of mission time. In the reported incidents, listed in Table 1, the crew saw smoke and embers in the STS-28 mission and detected odors in the other missions.[10,11] All incidents were subsequently identified as thermodegradation events caused by failures of wires or electrical components. None caused a smoke alarm to actuate. On STS-28, instrumentation did indicate a rise in smoke concentration, but the maximum concentration was below the prescribed alarm setpoint. The cited incidents never spread beyond the breakdown source, most likely a credit to the Shuttle material controls and the prompt circuit-isolating response of the crew.

One may plausibly predict the same rate of fire-precursor incidents on the Space Station. One may also predict that the crew will be able to isolate the breakdown source initially, with further control through fire-extinguisher use, if this becomes necessary. Space Station fire protection is complicated, however, by the possibility of an incident occurring in an untended period, for example, between the assembly missions. The untended station

Table 1. Shuttle Fire-Risk Experience.

Mission	Date	Incident	Result	Response
STS-6	Apr. 1983	Wires fused near material processing unit; crew detected an odor	No atmospheric contamination measured	No alarm
STS-28	Aug. 1989	Cable strain at connector to teleprinter caused insulation failure and electrical short circuit; crew detected a few embers and smoke	Smoke and particle concentration recorded	Circuit breaker did not open; no alarm
STS-35	Dec. 1990	Overheated resistor in digital display unit; crew detected an odor	No atmospheric contamination measured	No alarm
STS-40	June 1991	Refrigerator-freezer fan motor failed; crew noted an irritating odor	Atmospheric contamination identified post-flight	No alarm
STS-50	June 1992	Electronic capacitor in negative body pressure apparatus failed; crew detected an odor	No atmospheric contamination measured	No alarm

safety systems will be monitored remotely by the ground crews; and, upon an alarm, the operators will initiate the automated response cycle of electrical-power shutdown and suppressant release in the affected zone. Since this is the only option even for the probable minor, non-fire incidents, an alarm in an untended period may unnecessarily waste suppressant resources and possibly damage components.

KEY ISSUES IN SPACECRAFT FIRE SAFETY

Material Flammability Criteria

Pioneering tests conducted on the 1974 Skylab space station showed that, for typical spacecraft materials in normal gravity where vigorous, buoyancy-induced convective flows are always present, flame-spread rates are 1.5 to 10 times greater than those in quiescent, microgravity conditions.[5] The flame-spread rate in microgravity, however, has been shown to increase with forced-air flows (ventilation). For example, representative flame-spread rates for thin-paper samples determined in experiments conducted at the NASA Lewis Research Center ground-based facilities are 1.1 cm/s in normal gravity, 0.5 cm/s in quiescent microgravity conditions, and 1.0 cm/s in forced-flow microgravity.[12,13] The latter rate was attained with a 6 cm/s atmospheric flow opposed to the flame spread direction — a minimal ventilation velocity. Similarly, the limiting oxygen concentration, or the lowest atmospheric content in which flames will spread, was 16.5% in normal gravity, 21% in quiescent microgravity, and 16% in forced-flow microgravity.

As a practical necessity, materials for use in spacecraft must be qualified by normal-gravity acceptance tests. A standard NASA test for sheet materials determines the resistance to the upward spread of flame (NASA NHB 8060.1C, Upward Flammability Test). The buoyant air flow in the direction of the flame spread provides a "worst-case" environment

in normal gravity and an assumed safety factor for microgravity applications. A recent study suggests possible improvements in the standard test to aid flammability predictions,[14] but no study as yet derives correlations of normal-gravity to corresponding microgravity flammability. In addition, common articles of paper, fabric, and plastics that are clearly flammable must be accepted in spacecraft for lack of suitable substitutes. Usage agreements for these articles demand strict control of quantity, configuration, spacing, and storage. Whether these special provisions can be continuously enforced during the long-duration missions of the Space Station is a concern for safety planning.

Spacecraft Atmosphere

The atmosphere of the Shuttle Orbiter and the proposed Space Station consists of air at ordinary sea-level total pressure and oxygen concentration (21 vol%). Prior to an extravehicular activity (EVA), the atmosphere is modified by removing some of the nitrogen but not the oxygen. This change decreases the total pressure, but it also increases the oxygen concentration to a maximum of 30 vol%. The modified atmosphere permits the crew to acclimate rapidly in low-pressure space suits without the need for prolonged prebreathing times to reduce blood nitrogen levels and prevent decompression sickness.

An increased concentration of oxygen in the atmosphere can accelerate flammability considerably and promote flame spread for some materials otherwise "non-flammable" in air. A review of 766 selected materials with acceptable flame-spread resistance (in normal gravity) under air showed only 654 had acceptable fire-spread resistance under an enriched 30%-O_2 atmosphere.[15] The NASA Lewis studies cited in the previous section also noted the strong influence of atmospheric oxygen on flame-spread rates in microgravity. For example, data for thin paper show that the flame-spread rate is increased by a factor of approximately 1.7 in the EVA 30-vol%-O_2 atmosphere compared to that in air.[11,12]

In contrast to the hazards of increased-oxygen-concentration atmospheres, atmospheres with reduced-oxygen concentrations have been shown to offer both life-support and fire-protection advantages.[16] In particular, a reduced-oxygen (or excess-nitrogen) atmosphere in the untended periods of the Space Station would essentially eliminate the probability of incipient fires requiring the automatic discharge of extinguishant. A systems analysis must determine the trade-off of the costs of atmospheric nitrogen loss and replenishment prior to each crew revisit to the savings in reducing the likelihood of untended-period alarms and their wasteful consequences.

Fire Detection

The fire-detection system under consideration for the Space Station consists of photoelectric smoke detectors installed to monitor local zones. The sensors use a conventional principle based on the response to the obscuration or scattering of a light beam by smoke particles in the atmosphere flowing through a sampling duct.[17] Ground-based, smoke-chamber development tests have established an alarm setpoint of 1.5%/m light obscuration for early warning of incipient fires and smoldering. Whether this setpoint is suitable for rapid recognition of fire "signatures" in microgravity is not known. Small-scale test data do indicate that the average size and concentration of smoke particles from microgravity fires may vary considerably from those of normal-gravity fires.[18] The obvious safety factor in setting the alarm threshold at a low smoke concentration can cause more frequent false alarms from detector electronic noise or benign atmospheric pollutants (dusts). Other detection-system requirements, such as alarm-confirmation and failure-tolerance criteria, and even the zone volume specification for an optimum number and location of sensors in the station, are not yet established with any confidence.

Fire Suppression

Proposed fire suppression for the Space Station consists of a primary fixed system for remotely actuated discharge of carbon dioxide agent and a secondary system of portable carbon dioxide fire extinguishers. Storage quantities and release rates are sized to achieve a zone flooding concentration of 50 vol% CO_2, a level based on terrestrial standards and developmental-test results. The Space Station suppression system has a single-failure tolerance; *i.e.*, the primary system is backed by the portable fire extinguishers. In the untended periods, however, the only alternative upon failure of the primary suppression system is in the remotely actuated venting of the spacecraft atmosphere to space. The extinguishment of fires by venting to a sufficiently low total pressure has been demonstrated in small-scale microgravity tests.[5,11] The flow created by venting, however, was shown to stimulate the growth of the microgravity fire temporarily.[11]

Analyses suggest that the mechanisms and rates of fire suppression in low gravity may differ substantially from those in terrestrial environments.[19] Until more data are available, conservative requirements must govern the spacecraft designs. It is thus possible that the proposed Space Station suppressant concentrations may be insufficient for effective rapid extinguishment or, on the contrary, excessive and wasteful.

Post-Fire Restoration

The proposed concentrations of carbon dioxide for suppression by flooding the unsealed racks or other zones can produce toxic concentrations through leakage into the Space Station cabin atmosphere. The prompt removal of excess agent and combustion products from the spacecraft atmosphere during and after a fire is beyond the standard capabilities of the environmental-control system. Localized venting or dedicated emergency contaminant-removal systems are under study, but these methods require more development. The long-term, subtle effects of toxic and corrosive fire by-products on both the crew health and equipment performance must also be considered in post-fire management.

CONCLUDING REMARKS CONCERNING DESIGN AND RESEARCH

The Space Station is now undergoing an extensive restructuring in design and operations, although it is unlikely that the basic requirements for fire protection will change. Fire prevention, detection, and suppression provisions for current spacecraft and the Space Station are adapted from accepted practices in terrestrial fire safety. Shuttle experience indicates that current fire protection is adequate. Nevertheless, the uncertainties in the nature of fires and the effectiveness of response techniques in microgravity require that system designs be conservative with high safety factors. Quantitative risk assessments in progress to evaluate the probabilities and consequences of fire-related incidents promise results to define practical safety levels and improve system efficiency. For successful analyses, a primary need is information on the correlation of normal-gravity acceptance-test data to realistic material flammability and flame-spread rates in low gravity. The current small-scale tests in ventilated, microgravity environments are to be augmented with practical experiments on representative, thick material sections (requiring Shuttle accommodations). Other needs are data to optimize fire-detection alarm setpoints and minimum suppressant concentration and flow rates, to establish alarm confirmation and false-alarm rejection logic, to provide failure-tolerance alternatives for untended periods, and to develop post-fire cleanup techniques.

METHOD OF EXPERT JUDGMENT APPLIED TO WASTE LANDFILL PERFORMANCE

Ljiljana Rodić and Louis H.J. Goossens

Safety Science Group
Delft University of Technology
Delft, The Netherlands

INTRODUCTION

This article presents the results of formal elicitation of expert opinions by paired comparisons. The elicitation was carried out as a part of a larger project, MIRAMOS (MIlieukundig Risico-Analyse MOdel voor Stortplaatsen), which has been initiated in order to establish a risk-analysis model for solid waste landfills.

METHOD

This project has proceeded in the following stages:

1. Extensive literature search.
   It revealed that the field data on failures of engineered landfills are rather scarce, and as such do not provide a firm basis for standard statistical calculations. Therefore, the method of expert judgments has been applied (Cooke, 1991).
2. Identification of basic events for the fault-tree analysis.
   Preliminary interviews with specialists from The Netherlands were conducted to verify that the list of basic events encompassed all possible relevant points. Besides contacting researchers and designers, we also made an effort to consult with people in landfill operations whose experience is often unpublished.
3. Selection of experts.
   To select the experts as objectively as possible, we solicited referrals from professionals in the field of landfill technology and management. From approximately 340 letters sent to specialists in Europe and North America, 120 wrote back with their recommendations (35% response rate, comparable to those reported in literature, e.g. Morgan, 1984). These names were then assembled into a list of experts for the next phase of our study.
4. Discussion of general landfill issues with the experts in order to define the most relevant issues to be subsequently compared.
5. Formal elicitation of expert opinion by paired comparisons.

Each phase revealed important aspects which then determined the further course of the study. The details of the previous stages are reported by Rodić (1993a, 1993b). They mainly include general opinions offered by experts on a few fundamental landfill issues. It was necessary to address these issues before entering this phase of the project - elicitation of formal expert opinion on landfill failure modes by paired comparisons. In this paper, only the findings of the paired comparisons stage are discussed.

FAILURE OF BOTTOM LINER

The questionnaire about bottom liners consisted of two parts, one for failure which occurs in the short-term (during construction, operation and the first 30 years after closure) and one for failure which occurs in the long-term (several hundreds of years after closure). Table 1 shows the items compared for failure of the bottom liner, with the first twelve items compared for failure in the short-term and all fifteen items compared for long-term failure.

Table 1. Items (objects) compared for failure of the bottom liner

Item number	Short description
1	A choice of bad materials or an obviously inappropriate design by the design engineer.
2	Bad quality of materials delivered to and accepted at the site.
3	Installation damage.
4	Bad quality of seams and/or bad quality of clay compaction.
5	Geotechnical failure.
6	Chemical attack by unanticipated waste constituents.
7	Failure of the leachate collection and removal system (LCRS) and subsequent build-up of hydraulic head above the bottom liner.
8	A breach by the vertical gas pipes or the vertical leachate collection pipe caused by downdrag force of the settling waste.
9	Resorting to financial shortcuts during the course of construction which then partially or entirely alters the concept of the design.
10	Failure to safeguard the liner through adequate operation (tipping) activities, especially in the beginning of the operation phase.
11	Acceptance of any available site for the future landfill.
12	Numerous penetrating pipes through the bottom liner.
13	Failure of the cap liner and subsequent infiltration of rainwater into the waste bulk.
14	Subsequent land-use of the landfill site or construction in the area adjacent to the closed landfill.
15	No material can provide long-term containment.

Failure of Bottom Liner in Short-Term

The experts found that most problems stem from construction: the two highest scoring items belong to the construction phase, namely bad quality of geomembrane seams and/or bad quality of clay compaction, and damage during installation (Table 2). Although reputable geomembrane manufacturers provide their own seaming personnel and equipment (indeed, they would not sell their product if it were to be installed by others) there are still uncertainties regarding the mechanical parameters representative of seam quality as reported by Peggs (1985). The U.S. EPA organized a workshop in April 1993 to discuss these issues (EPA, 1993) with no firm conclusions about how to maintain the quality of seaming. Clay compaction is another uncertain issue as reported by Elsbury *et al.* (1990).

The next highest scoring items on the list concern design (pipes penetrating the bottom liner) and operation practices (failure to safeguard the liner).

Table 2. Expert opinions (obtained by paired comparisons) on the causes of failure of bottom liners in the short-term

item	NEL (Bradley-Terry)[1]	item	NEL
4	0.27	1	0.05
3	0.15	5	0.04
10	0.14	8	0.033
7	0.11	9	0.029
12	0.065	11	0.028
2	0.058	6	0.02

Number of experts: 16.

The general conclusion is that damage is the main cause of failure of the bottom liner in short-term rather than inadequate choice of materials, site or type of waste. With HDPE as the recommended geomembrane by almost all the regulatory guidelines (for its pronounced chemical resistance), there is a general belief that choice of material is not an issue. However, the experts still come across cases of obviously bad design, due to the emergence of numerous small design companies with less than adequate knowledge and competence.

Failure of Bottom Liners in Long-Term

An underlying assumption made by all the experts answering this questionnaire was that any failures noticed in the previous phases (short-term) had already been repaired.

Although experts agreed that there is no material which can provide long-term containment (long-term being defined as many hundreds of years), other items were ranked higher merely because they are considered to have a greater chance of occurrence before the material structure disintegrates.

Of those other items, the most frequently mentioned for long-term performance are the choice of an inadequate site for a landfill and failure of the cap liner.

It was rather difficult for the experts to decide which of the items causing the failure of the bottom liner in the short-term would also cause the failure later, for example, after 300 years. However, they clearly pointed to item no. 7 - failure of the LCRS[2]. There is a common belief, based on the field evidence, that the LCRS[2] ceases to function in a matter of decades. Theoretically, that should not lead directly to the failure of the bottom liner, but combined with all the damage during construction, build-up of leachate above the bottom liner (as a consequence of failure of the drainage system) surely provides conditions for greater leakage.

Bad design which allows pipes to penetrate the bottom liner is also cited as a serious cause of failure.

Subsequent land-use of the closed landfill site (item no. 14) is seen by some experts as a very possible cause of damage to containment. Based on their experience during the

[1] As defined by Cooke (1990).

[2] LCRS - leachate collection and removal system

last few decades, they claim that landfill records are not kept or taken into account for subsequent projects (developments around the site) after 10 years. However, most of the experts expressed their hope (rather than belief) that the recent strict regulations in this field will bring about better record-keeping and better cooperation among various governmental institutions. Particularly the experts from governmental agencies were confident about this.

LEACHATE COLLECTION AND REMOVAL SYSTEM (LCRS)

The questionnaire for the LCRS did not distinguish between short- and long-term since it is assumed that the LCRS will cease functioning within the short-term, as defined in the questionnaire. However, there is evidence that the methanogenic phase of waste degradation can last a very long time, meaning that the LCRS is also longer needed.
With this subject the experts were offered pairs of eight items shown in Table 3.

Table 3. Items compared for the failure of leachate collection and removal systems

Item number	Description
	Clogging due to failure by the design engineer:
1	the system not redundant enough - too few pipes, too small pipes, pipes not sufficiently interconnected;
2	inadequate slopes designed;
3	an inappropriate material selected for the filter and drainage layer (grain size, grain size distribution, mineralogical composition, etc.).
4	Clogging due to irregular/insufficient flushing.
5	Unpreventable clogging due to the type of waste.
6	Displacement or change in the slope of the pipes due to settling of subsoil.
7	Mechanical damage of the LCRS due to landslide of the subsoil.
8	Mechanical damage, displacement, and change in slope, during the tipping of (first meters of) the waste.

Item no. 7 posed a problem in the sense that it was not possible to imagine that the landfill would continue to function in the case of a major landslide which would significantly damage the LCRS. Therefore item no. 7 was eliminated from further analysis.

The experts were almost completely internally consistent (they had very few circular triads), although they did not always agree among themselves. The most distinctive difference in the resulting ranking order of items is between European and American experts as presented in Table 4.

Item no. 5 was by far ranked the highest by European experts. It is fairly clear from the experts' comments and the lack of literature on this topic that, in their opinion, this is the most uncertain and uncontrollable item.[3] American experts cited the failure of the design engineer in selecting appropriate materials (items no. 3) as the most prevalent reason for the failure of the LCRS.

[3] Clogging is the process of formation of a mixture of physical particles, (bio)chemical precipitates and microorganisms biomass; it can lead to a complete filling of the drainage sand layer and pipes. Clearly, these processes are very complex.

All the other items scored an order of magnitude lower. They concern the design and operation measures that can contribute to the alleviation (if not the elimination) of clogging.

Omission to flush the pipes for the purpose of cleaning the clogs (item no. 4) scores quite high. Although it may not be a remedy for clogging, field evidence shows that it helps. However, carrying out flushing in practice is difficult due to many logistical problems. Moreover, authorities seem not to monitor it adequately. Therefore, it is done irregularly and insufficiently.

Table 4. Expert opinions (obtained by paired comparisons) on the causes of failure of the LCRS

EUROPEAN EXPERTS		AMERICAN EXPERTS	
item no.	NEL (Bradley-Terry)	item no.	NEL (Bradley-Terry)
5	0.61	3	0.70
3, 4	0.10	1	0.06
6	0.07	4, 5	0.054
8	0.06	8	0.048
1	0.03	2, 6	0.03
2	0.01		
Number of experts: 7.		Number of experts: 5.	

Dutch experts found settling of the subsoil (item no. 6) important since this is present in the Dutch alluvial plane, with layers of peat and interchanging layers and patches of clay and sand, having different settling characteristics.

The items concerning the design of the drainage pipe network scored very low among continental European experts. There is a general agreement that designing according to the principles of hydraulics[4] alone cannot do away with the problem of clogging of landfill leachate drainage systems. Therefore, to reduce the chance of clogging, the system is made redundant with larger pipes, placed more densely, and better interconnected.

CONCLUSIONS

There is a common message: if any little opening in the seam, crack, tear, is left, leachate will find its way through it to the subsoil.

The definition of bottom liner failure as suggested in the questionnaire (penetration of waste constituents into the subsoil) prompted comments by some experts. Should total containment be pursued at all, knowing that all the materials currently used will ultimately leak? However, most national policies try to promote the best containment possible.

The general consensus is that there is not yet sufficient knowledge on the processes which take place within the waste bulk. However, it seems that financial resources available for such studies are scarce since interest lies more with the engineered parts of

[4] LCRS have been designed according to hydraulic principles which have traditionally been the basis for civil engineering design of drainage systems (e.g. irrigation systems). However, hydraulics does not account for the chemical and biological environment always present in LCRS.

a landfill system (barriers and drainage layer) rather than the waste itself. This is due to the commercial reality that producers of the liners and pipes are more concerned with the performance of their products over the nature of the waste.

Generally, governmental officials were not seen as knowledgeable of actual field conditions. Therefore, some of the technical guidelines are considered to be inappropriate.

Some experts warned about the general level of expertise of professionals in the field of waste landfilling. Since there is a large demand for engineered landfills, the experts were unanimous in their belief that the legislative systems allow for too many inadequately trained and insufficiently specialized professionals.

It was rather difficult for the experts to give opinions about items with which they had no direct experience. For example, the researchers had difficulty commenting on field experience during the construction phase (items 9 and 3).

The field of waste landfilling has become increasingly complex. The experts in this study have various specializations: properties of liner materials, design, construction quality control, and clogging of leachate collection and removal systems. Most of them expressed their doubts about questions they did not feel confident to answer. Also, both natural conditions (topographic, geological, geohydrological) and societal conditions (legislation, culture, mentality) differ from country to country. Therefore, all these variations among experts and their environments must be taken into consideration along with any statistical analysis of the results of formal elicitation of expert opinions by paired comparisons.

REFERENCES

Cooke, R.M. and Solomatine, D., 1990, "EXPO. Integrated System for Processing Expert Judgements. User's Manual", Faculty of Technical Mathematics and Informatics, Delft Universityt of Technology, Delft.

Cooke, R.M., 1991, "Experts in Uncertainty. Opinion and Subjective Probability in Science," Oxford University Press, New York/Oxford.

Elsbury, B.R., Daniel D.E. and Sraders G.A., 1990, Lessons learned from compacted clayliner, *J. Geotech. Eng.* 116(11):1641.

EPA, 1993, "Proceedings of the Workshop on Geomembrane Seaming. Data Acquisition and Control," Cincinnati, April 22, 1993, EPA, WAshington, D.C.

Morgan, M.G., Morris, S.C., Henrion, M., Amaral, D.A.L., and Rish, W.R., 1984, Technical Uncertainty in Quantitative Policy Analysis - A Sulfur Air Pollution Example. *Risk Analysis*, 4(3):201.

Peggs, I.E., 1985, The Effectiveness of Shear and Peel Tests in Evaluating HDPE Geomembrane Seams, *in* "Geotextiles and Geomembranes", The 2nd Canadian Symposium, Edmonton, September 23-24, 1985.

Rodić, Lj. and Goossens, L.H.J., 1993a, Formal Expert Judgement on Reliability of Landfill Liners, *in* "Geology and Confinement of Toxic Wastes", M. Arnould *et al.*, eds. Montpellier.

Rodić, Lj. and Goossens, L.H.J., 1993b, Long-term performance of landfill technology expert judgment, *in* "Sardinia '93. IV International Landfill Symposium", S. Margherita di Pula.

THE ACUTE TOXICITY OF HAZARDOUS MATERIALS AND EXPERT JUDGEMENT

Louis H.J. Goossens[1], Roger M. Cooke[2], Fred Woudenberg[3] and Pieter van der Torn[3]

1 Safety Science Group, Delft University of Technology, Delft, the Netherlands
2 Department of Stochastics, Statistics and Operations Research, Delft University of Technology, Delft, the Netherlands
3 Environmental Health Office, Municipal Health Service, Rotterdam, the Netherlands

INTRODUCTION

Probit relations play a role in predicting the expected number of fatalities as a consequence of unwanted dispersion of a gas cloud containing hazardous materials. Calculations of dispersion provide the concentrations to be expected. The probit relations provide the estimates of the number of fatalities among people exposed to the gas cloud. It is essential to such exercises that the applied probit relation represents a realistic relation between exposure dose (concentration and exposure time) and the percentage of expected fatalities.

A probit function within the frame of hazardous materials is represented as follows:

$$Pr = a + b.\ln(C^n T)$$

in which

- Pr is the probit value
- a is a constant
- b is a constant representing the slope of the probit relation
- C is the concentration of hazardous material in ppm or mg/m^3
- T is the exposure time in minutes
- n is the exponent indicating the relative influence of C to the probit value with respect to values of T.

A standard table of probit values provides the percentage of fatalities among the exposed population. For a number of hazardous materials (like chlorine, ammonia and hydrochloric acid), values of the constants a and b and the exponent n have been established in various ways given different sorts of data (for instance, animal data). For other materials the current probit relations are estimated based on LC_{50}-values, the lethal concentration at which 50 percent of the population die, sometimes sustained by the

relation of LC_{90}/LC_{10}, if at all known. In both cases, the constants a and b and the exponent n of the probit relation may have large uncertainties.
This paper describes the results of a formal expert judgement technique - developed at Delft University of Technology - that was used to obtain the dose-response relations for the acute lethal effects of five hazardous substances: acrylonitrile, ammonia, hydrogen fluoride, sulphur trioxide and azinphos-methyl. The full study has been reported by Goossens et al. (1992).

OPTIMIZATION PROCEDURE AND SEED VARIABLES

Twenty-five experts, distributed over the five substances, gave medians and 90 percent central confidence bands of the lethal dose-response relations under several conditions. Dose-response relations for each substance were calculated with parameter fitting techniques for uncertain models in two ways: with equal weights for the contributing experts and using an optimization procedure which weights the experts' assessments.

As recommended by Goossens et al. (1989) the 'Classical Model' for combining expert judgements was used. This is essentially a linear pooling or weighted averaging model, which derives its weights from classical statistical hypothesis testing, optimizing performance under a scoring rule constraint. The Classical model is extensively described in Cooke (1991).

A fundamental assumption of the 'Classical Model' is that the future performance of experts can be judged on the basis of past performance. When antecedent performance is lacking, it is generated by means of seed variables. Seed variables are variables of which the true values are known by the analyst or can be found within the time span of the study. The performance of the experts on the seed variables is taken as indicative for the performance on the variables of interest.

The seed variables must be in line with the variables of interest and require, of course, known quantitative data. As quantitative data on the lethal response of human beings to toxic chemicals are not available, the seed variables had to be selected from the "nearest" data sources. Animal experiments and low level epidemiological studies provide quantitative data which closely resemble the expected human behaviour once exposed to a large dose of a chemical substance. In the case of sulphur trioxide, animal experiments of the "nearest" toxic chemical, sulphuric acid, had to be used, as no animal experiments are reported on sulphur trioxide.

The behaviour of a toxic substance once it is inhaled by a human being has been studied. A Classification Model of Inhalation is developed with which routes and reactions of the chemical in the body can be classified. The aim is to enable the analyst to structure the contents of the seed variables. The model is represented by a number of 'dimensions':

KINETICS →	MECHANISMS →	TARGET ORGANS →	FUNCTIONAL DISTURBANCES →	HEALTH EFFECTS

The dimensions are related to:
- kinetics: (quantitative) properties concerning the rates of absorption, distribution, metabolism and elimination of the substance
- mechanisms (or dynamics): (qualitative) properties concerning the types of reaction, and the formation of metabolites, during absorption down to excretion
- target organs: the organs where the toxic impact will occur

- functional disturbances: (pathophysiogical) changes in organ-functioning as a result of the toxic impact
- health effects: clinical expression of the organ-function distributions.

Table 1 shows the distribution of the 'dimensions' of the Classification Model of Inhalation over the seed variables for the five substances. Some seed variables represent more than one 'dimension'. The 'dimensions' Kinetics and Health effects seem to be well documented in literature compared to the other three 'dimensions'.

Table 1. Distribution of 'dimensions' of the Classification Model of Inhalation over the seed variables for five chemical substances (K=kinetics, M=mechanics, TO=target organs, FD=functional disturbances, HE=health effects)

chemical substance	# of seed variables	'dimensions' K	M	TO	FD	HE
acrylonitrile	10	8	4	2	-	2
ammonia	10	3	1	3	3	3
hydrogen fluoride	9	6	-	-	-	3
sulphur trioxide	10	2	1	3	1	6
azinphos-methyl	10	6	2	1	1	5

PROPOSED PROBIT RELATIONS

For each assessed chemical substance in this study the following conclusions can be drawn with respect to the derived probit relations.

For acrylonitrile the experiment was succesful yielding a probit relation

$$Pr = -7.27 + 0.86 \ln(C^{1.3}t)$$

which leads to lower risk figures than predicted by the probit relation currently used in the Netherlands

$$Pr = -8.6 + \ln(C^{1.3}t)$$

This would impact the iso-risk-contours by dragging these approximately 20 percent closer to the source of release of acrylonitrile (for instance, an iso-risk-contour originally at 1000 meter could shift back to less than 800 meter). See Table 2.

For ammonia the experiment was also succesful: agreement on the acute lethal effects already explored in literature was sustained; the derived probit relation

$$Pr = -36.4 + 2.01 \ln(C^{2}t)$$

appears to have a steeper curve than the probit relation currently used in the Netherlands

$$Pr = -9.35 + 0.71 \ln(C^{2}t)$$

This would impact the current location of the iso-risk-contours. Higher risk-contours tend to shift away from the source, but lower risk-contours tend to shift back to the source of release. See Table 3.

Table 2. Potential change in iso-risk-contour distances in cases the currently used acrylonitrile probit relation in the Netherlands is replaced by the probit relation from this study

lethal response	iso-risk-contour in meters using current method	this study
90%	500	358
50%	1000	775
10%	1500	1257

Table 3. Potential change in iso-risk-contour distances in cases the currently used ammonia probit relation in the Netherlands is replaced by the probit relation from this study

lethal response	iso-risk-contour in meters using current method	this study
90%	500	615
50%	1000	908
10%	1500	1018

For sulphur trioxide the experiment was succesful: a probit relation could be established

$$Pr = - 2.85 + 0.68 \ln(C^2t)$$

which results in much lower response doses than is predicted by the probit relation currently used in the Netherlands

$$Pr = - 9.8 + \ln(C^2t)$$

This would impact the location of the iso-risk-contours tremendously: more than double distances (for instance, an original distance for an iso-risk-contour may shift from 500 meter to close to 1000 meter). See Table 4.

Table 4. Potential change in iso-risk-contour distances in cases the currently used sulphur trioxide probit relation in the Netherlands is replaced by the probit relation from this study

lethal response	iso-risk-contour in meters using current method	this study
90%	500	968
50%	1000	2251
10%	1500	3919

For hydrogen fluoride the experiment was not fully succesful: the nomination of experts appeared to be difficult as most of the identified experts were not available (deceased, addresses unknown). Furthermore as a result only three expert assessment were obtained, and some of these were incomplete rendering the expert data insufficient for quantifying the probit relation.

For azinphos-methyl the experiment was not succesful: experts were not sufficiently prepared for this kind of exercises which is very uncommon in the pesticide scientific community. Some seed variables appeared to be not adequately suitable. The remaining number of usable seed variables was insufficient (only six) and the number of experts was low (only three); no probit relation could be established, not even indicative.

In all cases the median assessments were used to derive the probit relations.

CONCLUSIONS

In conclusion it can be stated that the formal expert judgement procedure can lead to probit relations for ready use provided the elicitations of the experts' assessments are performed within the stringent conditions of the optimization procedure. Worldwide top experts on the toxic chemicals were elicited.

Moreover, the results of the succesful chemicals are what could be expected:

- for ammonia all experts provided median assessments within a narrow range, which is in line with the fact that the acute toxicity of ammonia is relatively well-known
- for acrylonitrile the spread in median values was large, as was indicated already in a previous exercise by the Municipal Health Service of Rotterdam (Woudenberg and van der Torn, 1991)
- for sulphur trioxide the uncertainties were large, which is in line with the fact that very little is known of the acute toxicity of sulphur trioxide.

ACKNOWLEDGEMENT

This paper reports results of the research program 'Probit relations and expert opinions' sponsored by the Ministry of Housing, Physical Planning and Environment of the Netherlands under Contract 371104-01.

REFERENCES

Cooke, R.M., "Experts in Uncertainty", Oxford University Press, New York, 1991.

Goossens, L.H.J., R.M. Cooke and J.F.J. van Steen, "Expert opinions in safety studies", TUDelft/TNO Apeldoorn, July 1989.

Goossens, L.H.J., R.M. Cooke, F. Woudenberg and P. van der Torn, "Probit functions and expert judgement: Protocol and results". TUDelft, Municipal Health Service Rotterdam, October 1992.

Woudenberg, F. and P. van der Torn, "Acrylonitrile: Quantification". Municipal Health Service Rotterdam, March 1991.

A LATENT VARIABLE MODEL IN UNCERTAINTY ANALYSIS

Adrianus M.H. Meeuwissen and Roger M. Cooke

Delft University of Technology
Faculty of Mathematics and Informatics
Mekelweg 4
2628 CD Delft
The Netherlands

INTRODUCTION

Mathematical models contain coefficients and parameters. The model predictions $\underline{Y}$ are a function of the parameters $\underline{X}$: $\underline{Y} = M(\underline{X})$. Sometimes the parameter values $\underline{x}$ of the parameters $\underline{X}$ are not known exactly. This can be modeled by assigning not a single value $\underline{x}$ to the parameters $\underline{X}$, but a (joint) probability distribution $F_{\underline{X}}$: $P(\underline{X} < \underline{x}) = F_{\underline{X}}(\underline{x})$. This distribution expresses the uncertainty of the model builder about the true value of the parameters. Assigning uncertainty distributions to the parameters implies that the output of the model $\underline{Y}$ becomes a random variable. Its distribution $F_{\underline{Y}}$ describes the uncertainty of the model builder about the outcome of the model emerging from the uncertainty in the model parameters. The distribution $F_{\underline{Y}}$ is usually calculated by Monte Carlo simulation.

We propose a latent variable model that allows for the modelling of the multivariate probability distribution $F_{\underline{X}}$ by means of bivariate probability distributions. This construction does not seriously restrict the class of multivariate probability distributions that can be modelled. Theorem 3 and Corollary 4 state that the joint distribution constructed in this way satisfies certain maximal entropy properties. A result important for the decomposition of an uncertainty analysis with dependent random variables is formulated as Theorem 5. We apply the results to fault tree uncertainty analysis modularization.

This paper is based on a previous paper by Cooke, Meeuwissen and Preyssl [1] and on the Ph.D. Thesis of Meeuwissen [9]. The techniques have been implemented in prototype software packages for the Dutch chemical corporation DSM [2] and the European Space Agency ESA [3]. The calculations of the example in this paper have been made with the computer program developed by Rene van Dorp [2].

LATENT VARIABLE MODEL

Let $\mathcal{T}$ be a graph on n nodes without cycles, i.e. $\mathcal{T}$ is a tree. Let $\underline{X} = (X_1, \ldots, X_n)$ be a vector of random variables. It is said that $\underline{X}$ shows *tree-dependence* if each of the random variables X_i can be associated with a node of $\mathcal{T}$ such that X_i, X_j are conditionally independent given their first common ancestor $(1 \leq i.j \leq n, i \neq j)$.

Given n observable random variables $\underline{X} = (X_1, \ldots, X_n)$ with joint probability distribution F, n random variables $\underline{Z} = (Z_1, \ldots, Z_n)$ and m latent random variables $\underline{\mathcal{L}} = (\mathcal{L}_1, \ldots, \mathcal{L}_m)$. We say that $(\underline{Z}, \underline{\mathcal{L}})$ with joint probability distribution G is a *latent variable model* for $\underline{X}$ if the marginal distribution of Z_i and X_i are equal $(i = 1, \ldots, n)$ and if the vector $(\underline{Z}, \underline{\mathcal{L}})$ shows tree-dependence.

We make the following remarks.

1. Notice the similarities between a tree dependence graph and an influence diagram without decision nodes [10].

2. The tree-dependence graph of a tree-dependent vector of random variables gives a sampling strategy. First sample any of the X_i, then conditional on this realisation sample its decendents, etcetera.

3. G is a composition of only bivariate probability distributions.

4. It is an open problem which class of joint probability measures F of $\underline{X}$ can be modelled by some latent variable model $(\underline{Z}, \underline{\mathcal{L}})$ with joint probability distribution G.

Consider the following application of this latent variable model. It is used to capture the main characteristic of knowledge dependence, see [9]. Let there be only one latent variable $\mathcal{L}$. Identify this latent variable with 'the model builder'. The random variables $\underline{X}$ are coupled to the latent variable with a degree depending on the 'degree of subjectivity' of the information source on which the uncertainty distribution of the parameters is assessed.

In short this means that if the model builder has an extensive statistical test at his disposal on which he can base the uncertainty distribution of a parameter, then this parameter will have an uncertainty distribution which will be independent or almost independent of $\mathcal{L}$. But if on the other hand little data are known to the model builder on a certain parameter and he has to rely upon his general knowledge and insight for the assessment of the uncertainty distribution, then this uncertainty distribution will be tightly coupled to $\mathcal{L}$. For a random variable X this coupling may be measured by the *rank correlation* $\rho_r(X, \mathcal{L})$ which equals the correlation $\rho(F_X(X), F_{\mathcal{L}}(\mathcal{L}))$ where F_X and $F_{\mathcal{L}}$ denote the distribution function of X and $\mathcal{L}$ respectively [5], [7].

Lemma 1

Given a model $Y = M(\underline{X})$ with random variables $\underline{X} = (X_1, \ldots, X_n)$ and a latent variable $\mathcal{L}$.

(i) If each of the pairs $(X_i, \mathcal{L})$, $1 \leq i \leq n$, are independent, then $(Y, \mathcal{L})$ is independent.

(ii) If M is monotone increasing and each of the rank correlations $\rho_r(X_i, \mathcal{L}) = 1$, $1 \leq i \leq n$, then $\rho_r(Y, \mathcal{L}) = 1$.

This lemma shows that the coupling between the model prediction and the latent variable can be interpreted as a degree of subjectivity of the uncertainty of the model prediction. The following theorem and its corollary show that the joint probability distribution G of a latent variable model $(\underline{Z}, \underline{\mathcal{L}})$ with given marginals and a given (tree-dependent) correlation structure have an optimal entropy property if and only if each of the composing bivariate probability distributions posseses this property.

Definition 2 (Relative Information,[6])
Let f be absolutely continuous with respect to g. The relative information $I(f|g)$ of a probability density $f(x)$ with respect to a probability density $g(x)$ equals

$$I(f|g) = \int f(x) \log \frac{f(x)}{g(x)}\, dx \ .$$

Theorem 3 (Meeuwissen and Cooke, [9])
Let $g_{X,Y}$ be the necessarily unique, [8], probability density with marginals g_X and g_Y that minimizes $I(g_{X,Y}|g_X g_Y)$ given the correlation ρ_{XY} between X and Y, and let $g_{X,Z}$ be the probability density with marginals g_X and g_Z that minimizes $I(g_{X,Z}|g_X g_Z)$ given the correlation ρ_{XZ} between X and Z. Then $g_{X,Y,Z} := g_{X,Y} g_{Z|X}$ is the probability density with marginals g_X, g_Y and g_Z that minimizes $I(g_{X,Y,Z}|g_X g_Y g_Z)$ given the correlations ρ_{XY} between X and Y and ρ_{XZ} between X and Z.

Corollary 4 *Consider the joint probability density $f_{\underline{Z},\underline{\mathcal{L}}}$ of the random variables $\underline{Z}, \underline{\mathcal{L}}$ of a generalized latent variable model with some given correlations $\rho(Z_i, \mathcal{L}_j)$ and $\rho(\mathcal{L}_k, \mathcal{L}_\ell)$ and given marginal densities. Given these correlations and marginal densities the joint density $f_{\underline{Z},\underline{\mathcal{L}}}$ has minimal relative information with respect to the product density of the marginal densities if and only if each of the bivariate densities $f_{Z_i,\mathcal{L}_j}$ and $f_{\mathcal{L}_k,\mathcal{L}_\ell}$ has the same property; i.e. if and only if each of the bivariate densities has minimal relative information with respect to the product density of its marginal densities given the correlation value for the two variables and given the two marginal densities.*

UNCERTAINTY ANALYSIS DECOMPOSITION

This section describes a mathematical approach of decomposing uncertainty analysis of larger models into the uncertainty analysis of smaller submodels. The problems that arise in taking proper account of (knowledge) dependence when modularizing uncertainty analysis are diminished by using latent variable models. Consider the following case. Let

$$\underline{Y} = M(\underline{X}) = M(S_1(\underline{X}_1), S_2(\underline{X}_2)) \ ;$$

i.e. the model $M(\underline{X})$ is a composition of the two submodels $S_1(\underline{X}_1)$ and $S_2(\underline{X}_2)$. It can be very convenient to determine first the probability distributions F_{S_1} and F_{S_2} of S_1 and S_2 seperately, by two Monte Carlo simulations. One can then treat in a second phase S_1 and S_2 as two random variables, whose (marginal) distributions now are known, to determine the distribution $F_{\underline{Y}}$ of the model prediction $\underline{Y}$. The problem that arises is that the two random variables S_1 and S_2 may be dependent.

There may be dependence between S_1 and S_2 for two reasons.
1. The parameter vectors $\underline{X}_1$ and $\underline{X}_2$ may contain common variables,
2. Some of the uncertainty distributions of $\underline{X}_1$ and $\underline{X}_2$ may be coupled to a common latent variable $\mathcal{L}$.

If either of these hold, then the joint probability density $f_{S_1,S_2} \neq f_{S_1} \cdot f_{S_2}$ and the density of Y cannot be determined from the marginal densities f_{S_1} and f_{S_2} alone.

In the following we assume that S_1 and S_2 have no common uncertain parameters. We consider the case where the uncertainty distributions reflect uncertainty from a *common* information source. We model this knowledge dependence using a latent variable model with one latent variable $\mathcal{L}$.

The main part of the investigation of many other interesting models can be reduced to the analysis of this model in the following way. Let $\tilde{\mathcal{L}}$ be the vector of common variables X_i of S_1 and S_2 together with the latent variables. The basic step in the following analysis will be the conditionalization on $\mathcal{L}$, which in the general case becomes conditionalization on $\tilde{\mathcal{L}}$. Then the same analysis will apply with minimal notational changes.

Note that smooth distributions are usually determined by their moments. When one wants to decompose the uncertainty analysis, one looses in principle the information on all cross product moments of the joint distribution of S_1 and S_2. By the latent variable structure however, the cross product moments can be written as a product of the regression function of $S_1^{k_1}|\mathcal{L}$ $(k_1 = 1, \ldots)$ and the moments of $F_{S_2,\mathcal{L}}$.

Theorem 5

$$E\{S_1^{k_1}S_2^{k_2}\} = E\{S_2^{k_2}\}E\{S_1^{k_1}|\mathcal{L}=0\} + E\{S_2^{k_2}\mathcal{L}\}\frac{\partial}{\partial\mathcal{L}}E\{S_1^{k_1}|\mathcal{L}=0\} + \frac{1}{2}E\{S_2^{k_2}\mathcal{L}^2\}\frac{\partial^2}{\partial\mathcal{L}^2}E\{S_1^{k_1}|\mathcal{L}=0\} + \ldots .$$

In order to take proper account of the dependencies, one should in the first phase, when one performs a Monte Carlo simulation of the sub-models S_1 and S_2, calculate an estimate of the two joint densities $f_{S_1,\mathcal{L}}$ and $f_{S_2,\mathcal{L}}$ instead of only an estimate of the marginal probability densities f_{S_1} and f_{S_2}. And then simulate from these joint probability densities in the second phase. The following corollary can be used to estimate these joint densities in a simple way.

Corollary 6

If the derivatives of the regression functions $E\{S_1^{k_1}|\mathcal{L}\}$ and $E\{S_2^{k_2}|\mathcal{L}\}$ vanish from order L onwards, then the cross product moments $E\{S_1^{k_1}\mathcal{L}^\ell\}$ and $E\{S_2^{k_2}\mathcal{L}^\ell\}$ with $\ell = 1, 2, \ldots, L-1$ determine the value of the cross product moment $E\{S_1^{k_1}S_2^{k_2}\}$.

Approximation for Decomposition. Theorem 5 and Corollary 6 provide a way to decompose an uncertainty analysis without loss of information or accurracy, also in case there exists knowledge dependence between S_1 and S_2.

In the first phase Monte Carlo simulations one not only estimates the marginal densities of S_1 and S_2, but also a number of cross product moments $E\{S_1^{k_1}\mathcal{L}^\ell\}$ and $E\{S_2^{k_2}\mathcal{L}^\ell\}$, $(k_1, k_2, \ell = 1, 2, \ldots)$. The number of cross product moments to be calculated is determined by the degree of 'linearity' of the regression functions of S_1 and S_2.

Then in the second phase Monte Carlo simulation one simulates from joint probability densities $f_{S_1,\mathcal{L}}$ and $f_{S_2,\mathcal{L}}$ with the given marginals and with the given cross product moments. The construction of distributions having minimal relative information under these constraints can for instance be done as in Meeuwissen and Bedford [8].

Instead of fitting the cross product moments $E\{S_i^k\mathcal{L}^\ell\}$, one can also fit the cross product moments $E\{F_{S_i}(S_i)^k\mathcal{L}^\ell\}$, i.e. the rank correlations etcetera. This modification is numerically much more stable as it eliminates the sensitivity to the tails of the probability distributions.

EXAMPLE

We illustrate the results in a fault tree uncertainty analysis example. Suppose M is a large fault tree, and S_1 and S_2 are two sub-fault trees comprising sub-systems. Let

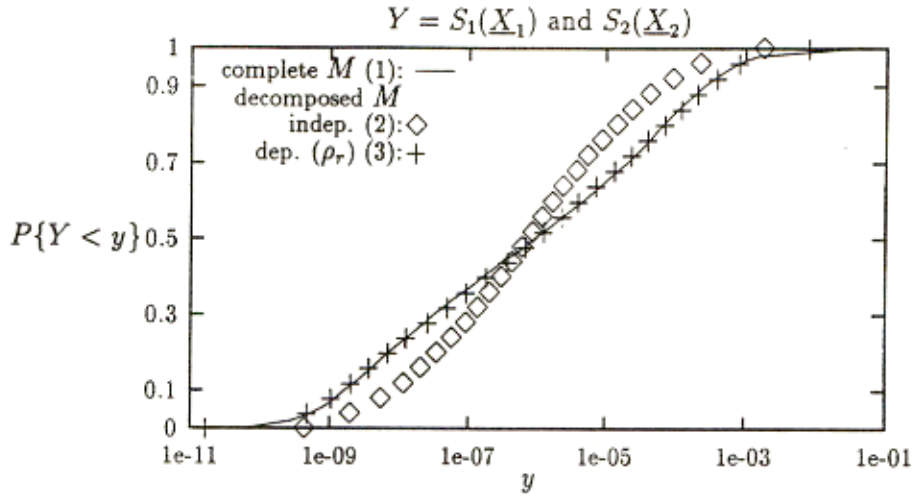


Figure 1: Failure probability distribution of two 3-out-of-4 systems (and-gate): original model (1), decomposed model disregarding dependence (2) and decomposed model fitting rank correlations $\rho_r(S_i, \mathcal{L})$ (3).

S_1 and S_2 be two 3-out-of-4 systems; i.e. S_1 consists of 4 components X_1, X_2, X_3, X_4 and fails if and only if 3 or more of these components fail. Now let the uncertainty about the failure probabilities p_i of the components X_i be identically distributed with a 5% quantile of 0.0100, a 50% quantile of 0.0548 and a 95% quantile of 0.3000.

We assume the existence of a moderate knowledge dependence and model it by assigning a rank correlation value $\rho_r(X_i, \mathcal{L})$ of 0.7 between the failure probability uncertainty distribution of each component X_i and the latent variable $\mathcal{L}$.

Now we have done three Monte Carlo simulations (sample size 10000). In the first one we have simulated the entire system with eight components. The second one was divided into two phases. In the first phase the sub-system S_1 consisting of four components has been simulated. In the second phase a small system with the two components S_1 and S_2 has been simulated. The two components were chosen to be independent and had the marginals obtained by the first phase simulation. The first phase of the third Monte Carlo simulation was identical to the second Monte Carlo simulation. In its second phase however the rank correlation between $\mathcal{L}$ and S_i had the same value as observed in the first phase simulation (0.88).

These three Monte Carlo simulations have been done for both a system "S_1 and S_2" and a system "S_1 or S_2". Results are shown in Figures 1 and 2. The correspondence between the probability distributions of the failure probabilities in the complete model and the decomposed model with fitting only the first cross-product-moment (rank-correlation) is remarkable. It is seen that for the decomposition of a fault tree model into two smaller sub-models it is sufficient to calculate in the first phase only very few (i.e. 1) cross product moments $E\{S_i^k \mathcal{L}^\ell\}$ which then can be fitted by a maximal entropy distribution in the second phase.

CONCLUDING REMARKS

In this paper we have presented a latent variable model for knowledge dependence in uncertainty analysis. We have given the important factors that play a role in the decomposition of large uncertainty analyses into smaller ones. We have applied the

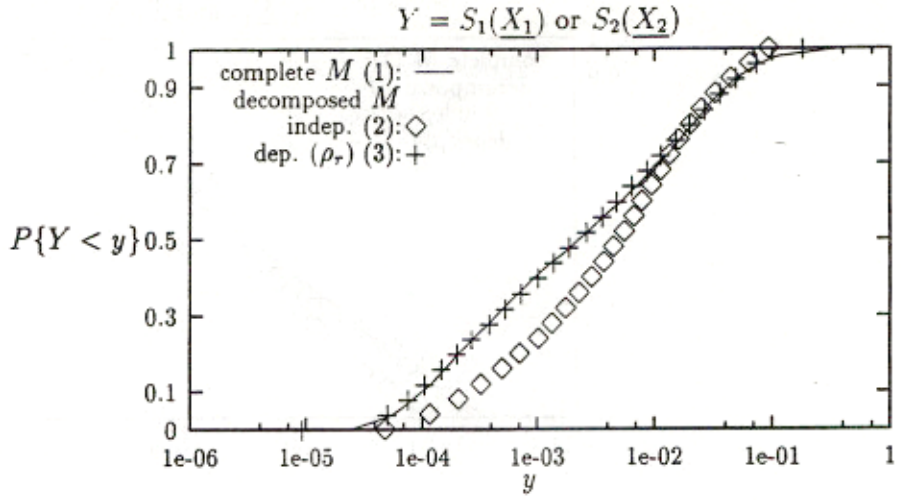


Figure 2: Failure probability distribution of two 3-out-of-4 systems (or-gate): original model (1), decomposed model disregarding dependence (2) and decomposed model fitting rank correlations $\rho_r(S_i, \mathcal{L})$ (3).

result to the case of fault tree uncertainty analysis. The decompositioning technique shows to do very well by taking into account only the first order cross product moments. The calculations were numericaly much more stable in the calculation of quantiles and rank-correlations than in the calculation of moments and ordinary cross-product moments by the heavy tails involved in these fault tree models.

REFERENCES

1. R.M. Cooke, A.M.H. Meeuwissen and C. Preyssl, Modularizing fault tree uncertainty analysis: the treatment of dependent information sources, in: Probabilistic Safety Assessment and Management, Ed. G. Apostolakis, Elsevier Science Publishing Co., New York (1991).
2. J.R. van Dorp, Dependence Modeling for Uncertainty Analysis, Thesis Delft University of Technology, The Netherlands (1991).
3. R.M. Cooke, M.S. Keane & A.M.H. Meeuwissen, User's Manual for RIAN: Computerized Risk Assessment, Estec 1233, Delft University of Technology, The Netherlands (1990).
4. P.W. Holland & P.R. Rosenbaum, Conditional Association and Unidimensionality in Monotone Latent Variable Models, The Annals of Statistics vol. 14, pp 1523–1543 (1986).
5. W.H. Kruskal, Ordinal Measures of Association, J. Amer. Stat. Assoc. vol. 53, pp. 814–861 (1958).
6. S. Kullback, Information Theory and Statistics, Wiley, Chichester (1959).
7. E.L. Lehmann, Some concepts of dependence, Ann. Math. Stat. vol. 37, pp. 1137–1153 (1963).
8. A.M.H. Meeuwissen & T. Bedford, Probability distributions with given marginals and given correlation that have maximal entropy, in: A.M.H. Meeuwissen, Dependent Random Variables in Uncertainty Analysis, Ph.D. Thesis, TU Delft, The Netherlands (1993).
9. A.M.H. Meeuwissen & R.M. Cooke, Knowledge dependence and uncertainty analysis decomposition, in: A.M.H. Meeuwissen, Dependent Random Variables in Uncertainty Analysis, Ph.D. Thesis, TU Delft, The Netherlands, 1993.
10. R.M. Oliver & J.Q. Smith (eds), Influence Diagrams, Belief Nets and Decision Analysis, Wiley, Chichester (1990).

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)

SOME REQUIREMENTS FOR DESIGNING AND MANAGING RELIABLE COMPLEX SYSTEMS

Karlene H. Roberts
University of California, Berkeley

Martha Grabowski
Rensselaer Polytechnic University

On a global basis complex organizations are increasing. Inevitably some parts of many of these organizations engage in behaviors that can lead to catastrophic error. As Perrow (1984) points out catastrophic error in one part of an organization can have a domino effect in other parts of the same organization. In fact, there is a body of research that describes both catastrophic accidents in such organizations (e.g. Shrivastava, 1986, Davidson, 1990, etc) and organizations in which attempts are constantly made to avoid such catastrophes (Roberts, 1990; Roberts, 1993).

Only infrequently do organizational writers consider systems of organizations. There are the networked organizations featured in the Miles and Snow research (Miles & Snow, 1986), interlocking boards of directorates (Burt, 1980; 1979), and socio-technical systems (Trist & Bamforth, 1951). Despite the obvious existence of systems few organizational writers think about systems of organizations in which error in one part of the system (but not necessarily in the same organization) can propagate to other parts of the system. And none have made empirical observations in such systems. Yet, it is obvious that as the number of system components increases the probability of error increases.

TYPOLOGIES OF ORGANIZATIONAL SYSTEMS ARE MISSING

Of the many problems facing managers and researchers interested in designing and managing large scale systems two stand out as candidates for initial scrutiny. The first is that there exists no typology of organizational systems. Yet, clearly various kinds of organizational systems exist. Two examples illustrate this point.

Prince William Sound at the time of the Exxon-Valdez tragedy is an example of one kind of organizational system. The accident was the result of the simultaneous coming

together of Exxon Shipping Company management policies that were not enforced, Coast Guard cutbacks in manning, training and serious attention to the possibilities of accidents in the immediately preceding years; manning shortages, lack of drills, and poor planning on the part of Alyeska (the industry's accident watchdog); piloting procedures that were less than optimal; and the non existence of the state of Alaska's own watchdog activities (National Transportation Safety Board, 1989; Davidson, 1990).

All of the organizations involved were interdependent with one another although behavior within each of them suggests that their members didn't understand this interdependence. For example, Alyeska was supposed to have available a well equipped barge in case of an accident. The barge was down for maintenance and had been for some time (Roberts & Moore, 1993). Thus, the supposed joint efforts of Alyeska and the Coast Guard in dealing with an accident could not have been carried out effectively. Just prior to the accident shift changes occurred at exactly the same time in the Coast Guard's Vessel Traffic Service (VTS) and aboard the Exxon-Valdez. Consequently, the supposed overlapping watches of the two units could not be realized in that instance. Worse yet, the Coast Guard had turned off the radar and the VTS operator had left his post for a cup of coffee. If the system had worked as it should have one might characterize it as a geographically dispersed parallel processing system.

Other kinds of organizational systems also exist and are very poorly articulated. Take for example, the Nordic Explorer oil drilling rig in the Java Sea off the Coast of Indonesia. It's owner is Ross Offshore, a Norwegian Company. The rig is managed by Patra, an Indonesian Company, and it drills for ARCO. One can imagine that the structure of the system might well be conducive to management problems. It appears to be a hierarchically stacked system of sorts.

The point is that there are probably a number of kinds of interdependent organizational systems that have never been explicated. It is probable that most existing organizational systems "grew like Topsy" following some underlying functional logic. But in an increasingly complex world it is likely that managers will be faced with the task of designing whole systems from scratch. The Alaska pipeline and its interdependent organizations is a case in point. Managers faced with the problem of designing organizational systems are probably hard pressed to do so in the absence of information about what their alternatives are.

MANAGEMENT PRIORITIES TO ENHANCE SAFE AND RELIABLE OPERATIONS

The second problem with organizational systems is that once designed managers must decide on appropriate priorities to enhance safe and reliable operations. Reliable and safe operations seem paramount to any organizational system simply because, as stated previously, the addition of components increases the probability of errors which can influence other organizations in the system in unexpected ways. While we know little about the management of systems of organizations we can extrapolate some issues that may be of prime importance from observations made in single organizations. Grabowski and Roberts (submitted for publication) point to five determinants of reliable operations in large scale systems. We now turn to them and to one additional determinant, the keeper of the "big picture."

The Keeper of the Big Picture

It is as much intuitive as anything else to know that if a system of organizations is to operate interdependently someone has to be in charge of having the "big picture." In this

case a unit must oversee this task for the collection of units. Militaries have long known this and it is embodied in the notion of the General Staff. Organizations have corporate headquarters with similar oversight functions. Often organizations survive despite the fact that no one seems to have a very well developed "big picture."

Particularly when a unit within a system of organizations has potential for doing large scale harm, attention must be devoted to the many ways in which the organizations can influence one another. This may occur through resource exchange and other forms of interdependence, communication, physical co-location, etc.

System Structure

There is a constant tension in some organizations between tight and loose coupling. Reliability enhancing organizations often engage in both almost simultaneously to address changing environmental conditions. For example, a study of two aircraft carriers (Roberts, Stout, & Halpern, 1993) illustrated the almost simultaneous use of both forms of control.

Most organizational theorists interested in organizational design, however, note that when organizations are tightly coupled (and consequently fairly centralized) they become brittle and unable to respond to changing environments (Weick, 1976; Perrow, 1984; Daft & Weick, 1984). These theorists call for loose coupling.

> As an example, Perrow makes specific reference to the marine transportation industry:
>
> The problem, it seems to me, lies in the type of system that exists. I will call it an "error inducing" system; the configuration of its many components induces errors and defeats attempts at error reduction. Discrete attempts to correct this or that will be defeated by something else; only a wholesale reconfiguration could make the parts fit together in an error-neutral or error-avoiding manner....it seems to be the combination of system components that promotes error inducement, such that improving or changing any one component will either be impossible because some others will not cooperate, or inconsequential because some others will be allowed more vigorous expression (Perrow, 1984, p.173).

What Perrow misses is the fact that system-wide, the marine transportation industry is very loosely coupled. In this system an example of tight coupling might be the laying down of specific laws about traffic separation schemes (TSS) that ships are expected to follow without variance. The fact that ships often break these laws in various ports in response to local weather and water conditions is an example of loose coupling. Sometimes this kind of loose coupling can result in serious mishap as when the Exxon-Valdez went outside of the TSS departing from Valdez Harbor. Thus, similarly to reliability enhancing single organizations, managers of complex organizational systems probably need to recognize the appropriateness of the tension between tight and loose coupling.

System Decision Making

Loosely federated or coupled systems are situations in which decision making is also uncoupled. Tightly coupled systems are milieus in which decision making can be rigid and uncritical (Janis & Mann, 1977). The literature on team decision making shows errors can occur for a number of reasons (Abelson & Levi, 1986; Slovic, Fischoff, & Lichtenstein, 1977, etc.) But, while teams afford opportunity for error they also afford opportunity for error correction.

The social psychological literature on decision making focuses primarily on how individuals make decisions in response to group characteristics. There is some literature on distributed decision making. But this literature makes an assumption that is often unmet (National Research Council, 1990), it assumes decisions are truly tied together across systems.

Yet some systems are truly disaggregated. The marine transportation industry is a good example of this. Since the days of Henry VIII, the need for some kind of connection between the port and the ship to provide local navigation knowledge has been recognized. To this end the piloting industry was established. If one considers the ship and its master as one unit of the system and its pilot as another, the notion of a pilot as a navigational aid introduces into the system an opportunity for team decision making and checks and balances across the master and pilot, each representing two different parts of the system. While in reality these people often engage in a real interchange, their system is not designed to require this. The master is always the final authority, and can take decision authority out of the hands of the pilot.

When we expand this example to think about the port in which these people operate individual decisions made aboard yachts, tugs, ferries, and other vessels are totally independent of one another or they are only loosely tied together on an exception basis by communication on VHF radios. Decisions in some other kinds of systems are more tightly tied together. It would be impossible to run an air traffic control system, for example, if handoffs from one sector to another were not integrated to some degree, particularly during periods of heavy traffic.

Similar to our point about system structure, managers must learn to recognize points in their systems in which disaggregated decisions can be tolerated, and points which require truly aggregated though geographically distributed decision making. No research exists that can inform managers about this.

System Communication

In the 1970s and more recently behavioral scientists made great strides in developing a methodology that can help answer questions about what constitutes optimal communication in organizational systems. The methodology is network analysis, which allows scholars to measure such factors as network density, reciprocity, roles, etc. It also allows the differentiation of figure and ground relationships. In 1979 and again in 1986 Charles Perrow wrote optimistically about network analysis' potential for answering many questions about inter organizational systems. He found only one study that truly moved in this direction, though it did not use formal network analysis. Warren, Rose, and Bergunder (1974) examined Lyndon Johnson's model cities program. This program was "designed to introduce new community action agencies into urban areas, to stimulate coordination among all agencies concerned with social problems and to promote innovative responses to these problems (Perrow, 1986, p. 206)." Studies of communication in organizational systems are still missing.

The importance of organizational system communication is nowhere stated more emphatically than in Karl Weick's analysis of the Tenerife air disaster in which 583 people on a Pan American 747 and a KLM 747 were killed:

> First, part of any job requirement must be the necessity for talk. Strong, silent types housed in systems with norms favoring taciturnity can stimulate unreliable performance because misunderstandings are not detected. Of the four implications for managerial practice derived by Sutton and Kahn (1987)

> in their influential stress review, three concern talk: be generous with information, acknowledge the information functions of the informal organization, do not hold back bad news too long. La Porte, Rochlin, and Roberts (e.g. La Porte and Consolini, 1989) find that reliable performance and amount of talk exchanged co-vary (Weick, 1993, p. 193).

This analysis suggests that simply encouraging lots of communication helps the system become more understandable more linear, predictable and controllable for those operating in it. Because of lack of research managers are left guessing about such communication issues as what constitutes sufficient feedback, the nature of required trust, the development of various communication roles, etc. Without good communication none of the other processes discussed here can be managed for optimal outcomes.

System Culture

Systems in which one or more units have strong safety requirements should have strong cultures. Often organizations have weak cultures or sub cultures (Cooke & Rousseau, 1988). If organizational systems are comprised of organizations with different but interlocking mandates they may have somewhat different subcultures. But if any part of the system requires attention to safety and reliable performance a common core of cultural values should exist which promotes behaviors consistent with those goals.

Little is known about the content of that common core. Schulman's description of a reliability enhancing organization is instructive to managers about cultural characteristics they might help foster.

> ...many administrative and technical features and many aspects of the organizational culture focus attention upon failure and its consequences. While these organizations run with seemingly relentless constancy and predictability, in many respects their members are running scared-always alert to the possibility of failure and its costliness, if not its worst case ramifications. The consistent, preventative preoccupation with failure seems to be a distinguishing feature of high reliability organization (Schulman, 1993, p. 36)

> ...there is an aversion to what might be termed **aggressive hubris**. The culture of the organization supports this aversion and is reflected in an "organizational personality" that predominates. Coolness and caution are repeatedly mentioned as personality traits desirable among employees or co-workers.... But the Array of differential powers throughout the plant that must be integrated requires constant adjustment and accommodation to make the system work. Integration depends upon the continual reinforcement of key values at the plant: credibility and trust (p. 45).

These statement suggest the necessity of constantly oiling and nurturing the culture of the system so that everyone in it understand its norms and their appropriate behavior with regard to those norms. Accomplishment of this goal probably requires heavy inputs from the "keeper of the big picture" as well as constant renegotiation about goals and processes within and across organizations.

Human Computer Interfaces

Tendencies to commit errors are part of the human condition. Thus attempts to design

error tolerance into large scale systems at the outset are frequent and usually focus on man machine interfaces. Thus dials supplement direct operator observation in assessing the reliability of various kinds of plant operations. The advent of computer technology offers a real possibility for knitting together systems of operation, and addressing a whole range of error-mitigating possibilities. The tools at hand are much improved over what they were only a few years ago; extensive automation, diverse and redundant safety devices, sophisticated warning, detection, and navigational systems, and increasing development of intelligent decision support systems (Reason, 1991). Finally, principles of ecological interface design, a theoretical framework extending the principles and benefits of interfaces to complex systems, have been devised to support human-computer interfaces in complex large scales systems (Vicente and Rasmussen, 1992).

While these advanced mechanical technologies are important partners in obtaining system reliability a problem with them in the past has been over reliance (e.g. Three Mile Island). Hopefully today's managers are experiencing training in the limitations to both human and mechanical contributors to reliable system performance.

CONCLUSIONS

We began this discussion by stating that two management challenges stand out as candidates for initial concern in current thinking about how to design and manage systems of organizations. One has to do with the complete lack of typologies for studying different system forms. Without such typologies it is impossible to help managers understand their alternatives system design strategies.

The second problem with organizational systems is that once designed mangers must decide on initial issues to focus on in order to enhance reliable and safe performance. The most obvious issue is attending to the importance of developing and nurturing the "keeper of the big picture." Beyond that we discussed five additional determinants of reliable operations in large scale systems discussed by Roberts and Grabowski (submitted for publication). These determinants are probably not the only important precursors to safe and effective performance. While we were able to highlight their importance here, there is no research that specifies exactly how managers should think about and pay attention to them. Our contribution is simply to highlight their importance

REFERENCES

Abelson, R.P. & Levi, A. (1986) Decision making and decision theory. In G. Lindzey & A. Aronson (Eds.) **Handbook of Social Psychology.** (3rd edition, vol. 1) Reading, Mass: Addison-Wesley, 231-310.

Burt, R.S. (1980) Cooptive corporate actor networks: A reconsideration of interlocking directorates involving American manufacturing. **Administrative Science Quarterly, 25,** 557-582.

Burt, R.S. (1979) A structural theory of interlocking corporate directorates. **Social Networks, 1,** 415-435.

Cooke, R.A., & Rousseau, D.M. (1988) Behavioral norms and expectations: A quantitative approach to the assessment of organizational culture. **Group and Organization Studies, 13,**

245-273.

Daft, R.L. & Weick, K.E. (1984) Toward a model of organizations as interpretation systems. **Academy of Management Review, 9**, 284-295.

Davidson, A. (1990)**In the Wake of the Exxon Valdez.** San Francisco: Sierra Club Books.

Grabowski, M., & Roberts, K.H. (submitted for publication) Human and organizational error in large scale systems.

Janis, I.L. & Mann, L. (1977) **Decision Making: A Psychological Analysis of Conflict, Choice, and Commitment.** New York: Free Press.

Miles, R.E. & Snow, C.C. (1986) **Network organizations: New concepts for new forms.** California Management Review, 28, **62-73.**

National Research Council (1990) **Distributed Decision Making: Report of a Workshop.** Washington, D.C.: National Academy Press.

National Transportation Safety Board (NTSB) (1990) Marine Accident Report: Grounding of the U.S. Tankship **Exxon Valdez** on Bligh Reef, Prince William Sound, near Valdez, Alaska, March 24, 1989. Report No. NTSB/Mar 90-04. Washington, D.C: National Transportation Safety Board.

Perrow, C. (1979) **Complex Organizations: A Critical Essay.** New York: Random House.

Perrow, C. (1986) **Complex Organizations: A Critical Essay.** New York: Random House (3rd edition).

Perrow, C (1984) **Normal Accidents: Living with High Risk Technologies.** New York: Basic Books.

Reason, J.T. (1991) How to promote error tolerance in complex systems in the context of ships and aircraft. Safety at Sea and in the Air - Taking Stock Together Symposium, The Nautical Institute.

Roberts, K.H. (1990) Some characteristics of high reliability organizations. **Organization Science, 1**, 160-177.

Roberts, K.H. (1993) **New Challenges to Understanding Organizations.** New York: Macmillan.

Roberts, K.H. & Moore, W. (1993) Bligh Reef dead ahead: The grounding of the Exxon Valdez. In K.H. Roberts (Ed.) **New Challenges to Understanding Organizations.** New York: Macmillan, 231-248.

Roberts, K.H., Stout, S., & Halpern, J. (1993) Decision dynamics in two high reliability military organizations. **Management Science.**

Schulman, P.R. (1992) A comparative framework for the analysis of high reliability organizations. In K.H. Roberts (Ed.) **New Challenges to Understanding Organizations.** New York: Macmillan.

Shrivastava, P (1986) **Bhopal: The Anatomy of a Crisis.** Cambridge, Mass: Ballinger.

Slovic, P., Fischoff, M., & Lichtenstein, S. (1977) Behavioral decision theory. In M. Rosenzweig & L.W. Porter (Eds.) **Annual Review of Psychology, 28,** 1-39.

Trist, E. & Bamforth, K.W. (1951) Social and psychological consequences of the long wall method of coal getting. **Human Relations, 4,** 3-28.

Vicente, K.J. & Rasmussen, J. (1992) Ecological interface design: Theoretical foundations. **IEEE Transactions on Systems, Man, and Cybernetics, 22,** 589-606. (July/August).

Warren, R., Rose, S., & Bergunder, A. (1974) **The Structure of Urban Reform.** Lexington, Mass: Lexington Books.

Weick,K.E. (1976) Educational organizations as loosely coupled systems. **Administrative Science Quarterly, 21,** 1-19.

Weick, K.E. (1993) The vulnerable system: An analysis of the Tenerife air disaster. In K.H. Roberts (Ed.) **New Challenges to Understanding Organizations.** New York: Macmillan, 173-198.

INCORPORATION OF HUMAN FACTORS INTO PROCESS HAZARD ANALYSIS

Denise B. McCafferty and Kurt A. Borows

DNV Technica, Inc.
16340 Park Ten Place, Suite 100
Houston, Texas 77084

HUMAN FACTORS AS A PART OF PROCESS SAFETY MANAGEMENT

In recent years, both industry and government have analyzed the factors relating to process accidents. There has been a shift away from attempts to reduce accidents through traditional safety approaches. The new focus is on Process Safety Management, which has moved away from concentrating on failures of individual pieces of equipment or injury statistics, and moved toward viewing a facility as an integrated whole, in which one part can directly or indirectly influence another. Incidents are no longer evaluated in isolation, but potential problems are evaluated for the possibility of initiating a chain of events and escalating into a catastrophic failure. Public concern has focused on the chemical industry, and has been heightened by recent accidents, such as Phillips Petroleum Company (Pasadena, Texas); ARCO (Channelview, Texas); Union Carbide (Bhopal, India); and Occidental Petroleum (Piper Alpha platform, North Sea). Through post-incident investigations, it has become clear that the source of failures may not solely be due to equipment failures, but may be linked to the failure of administrative, human, management, or organizational factors. As a result, these factors have been recognized as playing a significant role in Process Safety Management.

HUMAN FACTORS IN 29 CFR 1910.119, PROCESS SAFETY MANAGEMENT OF HIGHLY HAZARDOUS CHEMICALS

The Occupational Safety and Health Administration (OSHA) is an example of a regulatory agency concerned with Process Safety Management. In 1992, the newly-established 29 CFR 1910.119, the *Process Safety Management of Highly Hazardous Chemicals* came into effect. OSHA's intent was to provide regulation requiring industry to develop methods for managing process hazards. The legislation was aimed at preventing or minimizing the consequences of chemical accidents involving highly hazardous chemicals, and was particularly concerned with process releases of toxic, reactive, or flammable liquids and gases.

Since OSHA 1910.119 is a performance-based piece of legislation, OSHA has not defined a particular approach or methodology to be used for evaluating process hazards. Since many industry practitioners are already familiar with Hazard and Operability Studies (HAZOPs), many are using this technique as their Process Hazard Analysis (PHA) methodology. Regardless of the PHA approach taken, the methodology must include evaluation of applicable human factors. For many industrial companies, this requirement will be their first exposure to human factors.

Although it is required that human factors be addressed within the legislation, OSHA has not defined expectations, provided guidelines, nor suggested methodologies to accomplish this task. It is believed that OSHA's human factors concerns revolve around several factors:

- Review of operator/process and operator/equipment interface,
- Operator workload,
- Extended or unusual work schedules,
- Control and display interfaces,
- Instrumentation versus manual control of the process,
- Operator feedback, and
- Clarity of signs and codes.

WHAT IS HUMAN FACTORS?

Industry is now faced with the challenge of integrating human factors within Process Hazard Analysis. To meet this challenge, industry must define human factors and its application to the process plant environment. Human factors is concerned with the design of technical systems, where humans and equipment can interact safely and efficiently. Research has shown that humans are well-adapted to certain tasks, yet also have limitations. The current state of technology is also known, along with the technological limitations. As a result, a system can be designed to assign functions to humans, (such as data integration and pattern recognition), while assigning other functions to machines, (such as storing large amounts of unrelated data). Through conscious planning, a system can be created where humans and technology work together to meet a common purpose. Unfortunately, most facilities in existence today did not allocate functions in this manner, but were designed by assigning functions to technology; humans were expected to fill in the gaps and perform of the roles that could not be accomplished by machinery.

Process Hazard Analyses can give industry an opportunity to review the role of humans within facilities, and determine whether the assumptions made and the tasks assigned are within acceptable limits. Through the Process Hazard Analysis, a company can examine the role of humans within their complex facilities and determine if the design of the facility aids personnel in operating and maintaining the process within safe limits or, if in some areas, the actual design will cause personnel to make errors. Human factors is concerned with improving the reliability of operators in performing their tasks, by identifying situations leading to error and highlighting improvements to reduce that error. If done properly, a Process Hazard Analysis can examine a process unit and uncover existing error-producing situations.

DEFINING THE GOAL OF HUMAN FACTORS IN PROCESS HAZARD ANALYSES

An overall goal for integrating human factors analysis within Process Hazard Analyses must be set. The objective of reviewing human factors within PHAs is to identify situations, equipment, or other factors which may result in human errors, thus creating process hazards, operational upsets, or maintenance problems. Once potential errors are identified, steps can

be taken to control these errors. Since Hazard and Operability Studies (HAZOPs) are one of the most popular process hazard analysis techniques, this paper will address how consideration of human factors can occur during a HAZOP study.

THE SCOPE OF HUMAN FACTORS IN HAZOPS

To evaluate the effects of human factors and human error on plant operations and maintenance, multiple activities must take place. Those with expertise in the application of human factors technology are needed. Any combination of human factors analysis with HAZOPs will have a limited scope. A combined approach allows an evaluation of issues like equipment design, control systems, data displays, control-display relationships, alarm systems, work space requirements, and control room layouts. Other issues, such as Procedures, Safe Work Practices, Training, and Staffing will also be discussed to some degree during the PHA study, especially in relation to their role as important safeguards for containment of hazardous chemicals during process upsets. However, for a thorough review of the influence of human factors, issues such as procedures, safe work practices, training, and staffing should have separate, thorough human factors analyses.

APPROACHES TO INTEGRATING HUMAN FACTORS IN HAZOP STUDIES

There may be as many different approaches to integrating human factors within HAZOPs as there are different companies. Many companies are at a loss to determine how this integration can take place, and as a result, are doing nothing. Other companies have come to the belief that the inclusion of the term "Human Factors" within their HAZOP Guideword List is sufficient. Others have included a number of guidewords aimed at this concept. It is the contention of these authors that none of these approaches will prove sufficient for meeting the intent of OSHA 1910.119.

SUGGESTED METHOD FOR INCORPORATION OF HUMAN FACTORS INTO HAZOP STUDIES

To allow the concepts related to human factors to be integrated into HAZOP analyses and to meet the intent of OSHA 1910.119, a variety of activities should take place throughout the course of the HAZOP study. The human factors portions of the Process Hazard Analysis can be completed in three phases. Phase I involves the pre-HAZOP reviews of documentation and facilities; Phase II is the discussion of human factors during the HAZOP study; and Phase III is the human factors analysis stage.

Phase I

Performing a Human Factors Engineering (HFE) review of a unit prior to conducting the HAZOP helps maximize the HFE benefit in the HAZOP. Prior to conducting a Hazard and Operability Study, a Human Factors Specialist, the Study Leader, and applicable members of the HAZOP team, including unit operations personnel, should review documentation and spend time in the unit under study. During this time, issues such as equipment design, operator/machine interface, panel and alarm system design, and computer interfaces should be reviewed. A common approach for all of these areas of interest is to concentrate on the task requirements for the unit personnel. Defining the required tasks will establish the evaluation criteria. Task requirements of the unit personnel can be identified from a review of unit procedures, job performance aids (JPAs), and through discussions with unit operating

personnel. Training documentation, where available, will also help understand the unit tasking. The purpose of defining tasks and task requirements is to decide if personnel can successfully perform their jobs under all conditions with the equipment provided.

For design reviews, procedures and training documentation may not exist. In these cases, it would prove useful to define the concept of the role of the operator in a system. At this time, the team should also define which tasks they would expect an operator to perform and which tasks would be assigned to equipment. The design HAZOP team should be familiar with the concerns reviewed during an existing unit walkdown and perhaps initiate questions related to these concerns.

For existing units, once tasks have been defined and the available documentation reviewed, a unit walkdown should be undertaken. The unit walkdown should be conducted with an operator or foreman and include both the unit area and the unit control room. During the walkdown, observational notes should be made, and should include information about the adequacy of the layout and arrangement of the unit area equipment for operations and maintenance tasks. A review is also made of the accessibility of equipment and facilities, and will evaluate such characteristics as ingress and egress routes, stairs, ladders, and the adequacy of workspace. The unit environment should also be evaluated for such characteristics as lighting, noise, and heat.

The walkdown is also used to evaluate personnel safety issues, such as the potential for exposure to hazardous materials, slipping/falling hazards, adequate guard rails and safety shields, hazardous/toxic materials, sensors, and warning signs. Local control panels should be evaluated for instrumentation and control layout and completeness, including labeling and panel location/accessibility. Equipment labeling to aid in locating and identifying required components should also be reviewed. Walkdown observations in the control room should be used for the evaluation of the layout, arrangement, grouping, and labeling of all annunciators, instruments, controls, furnishings, and other equipment and facilities in this area. While reviewing the unit and control room interfaces, discussions should be held with personnel in the unit concerning usability and accessibility of equipment, overall safety, staffing, training, and past process safety incidents.

A review of procedures prior to the start of the HAZOP can often identify human factors concerns. The review might identify where two tasks must be completed at one time at different locations, mismatching in labeling and terminology, and steps involving inoperable equipment. A procedures review, at minimum, should include unit start-up, shutdown, and emergency procedures, as well as any unusual operating, maintenance, testing, and calibration procedures. Notations should address any areas of concern for presentation and discussion during the HAZOP study. These notes should not only include the problems, issues, and shortcomings identified, but also the strengths in the unit design.

Phase II

After the initial review conducted in the unit, the HAZOP team should be assembled for the HAZOP study. A briefing should be held with the team to introduce the goals and methods to be used for hazard identification and hazard analysis. Also at this time, a presentation must be given regarding human factors and how it relates to Process Hazard Analysis. Team members should be familiarized with the areas of human factors concern, such as human-machine interface, equipment design, accessibility/work space requirements/ physical work environment, procedures, safe work practices, training, and staffing. During the study, human factors issues identified during the initial visit to the unit should be presented to the team, discussed, and entered into the HAZOP record where appropriate. In addition, as other issues are discussed during the study, those with human factors implications should be identified as such and noted in the HAZOP record.

Phase III

The last phase of integrating human factors into Process Hazard Analysis involves documenting the human factors concerns. An important source of documentation of human factors concerns will be through identifying root causes during discussion about causes of deviations from the system intent. Whenever potentials for human errors are identified during a HAZOP study, the team should discuss how and why such an error could occur and ensure that the HAZOP record documents the source cause of such errors. Following the study, a human factors specialist should review the human factors concerns identified during the study and ensure that the suggested recommendations reduce the probability of the error or reduce the consequences of the error to acceptable levels. At this time, the human factors specialist can also conduct any additional analysis necessary to evaluate the extent of identified human factors problems.

THE LIMITATIONS OF THIS APPROACH TO HUMAN FACTORS AND HUMAN FACTORS IN HAZOPS

Introduction

There are limitations to what HFE can accomplish within the HAZOP analysis. Some of these limitations are based upon the purpose and the methodologies used, which may be thought of as *HAZOP process limitations*. Other constraints exist due to the limited participation in the HAZOP study of experienced and qualified HFE specialists. These limitations can be thought of as *HAZOP personnel limitations*.

HAZOP Technique Limitations

By definition, a HAZOP should identify and address all hazards inherent to a specific unit's processes. The HAZOP methodology is basically equipment and facility orientated and does not have, as the prime purpose, the complete analysis, identification, and evaluation of the personnel sub-systems and the identification of the causes of human error. In addition, a reasonably large number of process hazards do not involve the human-machine interface, nor do they require the intervention or interaction of personnel to implement adequate hazard control. These two characteristics of the HAZOP analysis maintain the emphasis on equipment and "hard" engineering issues and solutions, which also results in de-emphasizing the human error and human performance issues. This problem continues in spite of evidence that identified human error is the cause in approximately 60% of start-up and shutdown problems in batch reactions. While the HAZOP technique is heavily documented, the reasons behind human errors, the root cause, are often only superficially addressed.

Additionally, the HAZOP only needs to address the effective and efficient operation of the unit when there are hazards involved. Productivity of a facility, and its efficiency, are not necessarily HAZOP issues. Therefore, a large component of facility operations and the human-machine interface does not require in-depth review and analysis. Reduced production and/or the production of severely out-of-specification products, caused by inadequate instrumentation and control or by training and procedural problems, that do not result in increased hazards or undesirable releases, are not required to receive attention other than to verify that hazards do not result from the upset within the unit.

HAZOP Personnel Limitations

The HAZOP team is composed of a group of personnel that represent the required engineering and technical disciplines with an experience level needed to address the primary

hazards of the unit's processes. While HFE must be addressed during the HAZOP, HFE is not a required discipline to be represented on the HAZOP team. The HAZOP team will be placed at a disadvantage if there is a lack of representation of HFE skills and knowledge on the team. This can result in the misapplication of *training and procedures changes*, or to the misapplication of *equipment changes* to control or correct for human error potentials and human performance-related issues.

It has been found that without an HFE specialist, HAZOP teams often suggest or recommend procedures development and/or training changes to "solve" for human error problems. While such changes may reduce the probability of human error, they will seldom eliminate the error and may not reduce the consequences. Often times, to significantly reduce or eliminate human errors or the consequences of errors, equipment design changes may be required.

Conversely, other situations have been found where equipment changes cannot eliminate or significantly reduce the probability of error. In fact, some equipment changes may actually increase the probability of human error or may increase the severity of the consequence of an error. In cases such as this, a reduction in the consequences of the error may be possible. HFE specialists are more experienced in determining when a design change will work to reduce human error and how to avoid introducing new problems associated with human performance when incorporating changes. For particularly involved process concerns, it may be advisable for the HAZOP team to make a recommendation to involve a human factors professional in the design modification process.

BENEFITS OF HUMAN FACTORS IN PROCESS HAZARD ANALYSES

It is important to take into account the strengths and weaknesses of people in the design of a plant process, in order to reduce the vulnerability of the plant to human error. By reviewing the plant design during a HAZOP, potential sources of human error can be identified. Evaluations of the seriousness of errors can be made and suggestions given to reduce those errors by applying good human factors practices. Such practices may require improvements to equipment and/or working methods.

Human factors can be integrated into Process Hazard Analyses, and in particular, to HAZOP studies. The Human Factors professional has an important contribution to make in the evaluation of plant design and the interaction of this design with the "human" systems used to manage process safety. Time and effort should be allocated to ensure that human factors concerns are reviewed during Process Hazard Analyses. Reducing opportunities for human error within a facility can interrupt a chain of events or failures from escalating into a catastrophic failure. In addition, the application of human factors principles to facility design can result in safer, more efficient and productive plant operations.

REFERENCES

Department of Labor, Occupational Safety and Health Administration, 1992, Process Safety Management of Highly Hazardous Chemicals, Federal Register, 57, 36, 6403-6417.

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)

THE SAVANNAH RIVER SITE COMPONENT GENERIC DATA BASE: APPLICABLE TO A WIDE VARIETY OF FACILITIES

C. H. Blanton[1] and S. A. Eide[2]

[1]Westinghouse Savannah River Company
1991 S. Centennial Ave.
Building 1
Aiken, SC 29803

[2]Los Alamos Technical Associates
P.O. Box 51688
Idaho Falls, Idaho 83405-1688

INTRODUCTION

As part of a program to upgrade methodologies for safety analysis of Savannah River Site (SRS) nonreactor facilities, a state-of-the art component generic failure data base has been developed.[1] The data base has failure rate distributions generated from actual failure events for a wide variety of components and failure modes, such as pump failures to start and run, valve failures to open or close or spurious operations, electrical equipment failures, and others. Because of the many diverse data sources used to generate this data base, the results are potentially applicable to a wide variety of facilities: chemical processing; Department of Energy (DOE) production, reprocessing, and waste; commercial reactor; and others.

Strengths of the data base include the following:

- Comprehensive coverage of components and failure modes
- Wide variety of data sources
- Categorization (hierarchy) of sources
- Failure rates generated from actual failure events in most cases.

METHODOLOGY

A comprehensive list of components and failure modes was developed by reviewing existing data bases and data sources. Also, safety analysts from various DOE facilities provided additional items. The resulting list of components and failure modes includes approximately 500 entries. Also, several different process fluids are covered: water, chemical, compressed gases, and air (ventilation systems).

A wide range of sources was used to collect failure data and failure rate estimates for the components and failure modes identified. The sources included information on commercial nuclear reactor components, DOE reactor and nonreactor facilities, chemical processing facilities, military system components, offshore oil facilities, liquified natural gas facilities, and others. Of the approximately 50 sources used, 80% contained actual failure data and exposure hours (or demands). Major sources of actual failure data included the following:

- Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR)[2]
- DOE SRS production reactor failure data[3]
- DOE Idaho Chemical Processing Facility failure data[4]
- Offshore Reliability Data publication[5]
- Military data on nonelectronic components[6]
- Tritium collection system data.[7]

Information in References 4 and 5 was analyzed in detail to obtain failure data for the various component failure modes desired. (These references lump all failure events together; however, by reviewing the actual failures one can break down the information by failure mode.) Major sources for failure rate estimates (that do not list actual failure data) included the Center for Chemical Process Safety[8], IEEE Std. 500-1984[9], and WASH-1400.[10]

Sources were then grouped into one of three categories, based on existence and quality of failure data:

- Category 1 - Sources with actual failure data obtained from a detailed review of failure events (to ensure applicability to the failure mode being considered) and a detailed review of component populations and exposure hours (or demands). Approximately 20 such sources were identified, mostly dealing with commercial nuclear power plants or DOE reactors.
- Category 2 - Sources with actual failure data, but which have an added uncertainty in the data compared with Category 1 sources. This added uncertainty can result from a less comprehensive search for actual failures, a more approximate method for determining component populations or exposure hours (or demands), or a less clear breakdown of failures into the failure modes of interest. Approximately 20 category 2 sources were identified, covering nuclear power plants, military systems, DOE nonreactor facilities, offshore oil drilling platforms, liquified natural gas facilities, and others.
- Category 3 - Sources that list only failure rate estimates. Approximately 10 representative Category 3 sources were chosen.

All of the Category 1 and most of the Category 2 sources are independent, implying no overlap between sources with regard to facilities and periods covered. Category 3 sources are not completely independent, indicating some overlap in reference sources used to generate failure rate estimates in these sources.

Aggregation of failure data (Category 1 or 2) or failure rate estimates (Category 3)

was performed only within each category. The recommended component failure rate distribution was then obtained from the Category 1 result if available. If not available (no Category 1 data), then the Category 2 results were used. Finally, if no Category 1 or 2 data were available, then the Category 3 results were used. This hierarchy of categories was used in order to base component failure rate distributions on the best information available.

Aggregation routines used are described below. For Category 1 or 2 data, the following aggregation process was used.[2]

1. Compute R and R_2 from source data:

$$R = (\Sigma f_i)/(\Sigma T_i) \quad (1)$$

$$R_2 = [\Sigma f_i(f_i - 1)/T_i]/(\Sigma T_i) \quad (2)$$

where f_i = number of failures from source i

T_i = component exposure hours from source i.

2. Match moments to underlying normal distribution:

$$\mu = 2 \ln(R) - 0.5 \ln(R_2) \quad (3)$$

$$S^2 = \ln(R_2) - 2 \ln(R). \quad (4)$$

3. Determine mean and error factor of lognormal distribution:

$$Mn = \exp(\mu + S^2/2) \quad (5)$$

$$EF = \exp(1.645\ S) \quad (6)$$

where Mn = mean

EF = error factor (95th percentile/50th percentile).

For data involving demands rather than exposure hours, the same equations apply, but with T_i replaced with D_i (number of demands from source i).

For category 3 failure rate estimates, the following aggregation routine was used.[11]

1. Determine variance for each source:

$$S_i^2 = [(\ln EF)/1.645]^2. \quad (7)$$

2. Determine natural logarithm of median for each source:

$$\mu_i = \ln(Mn) - S_i^2/2 \quad (8)$$

where μ_i = natural logarithm of median.

3. Determine average of source variances:

$$S_{ave}^2 = (\Sigma S_i^2)/n_s \quad (9)$$

where n_s = number of sources.

4. Determine average of natural logarithms of medians:

$$\mu_{ave} = (\Sigma\ \mu_i)/n_s. \quad (10)$$

5. Determine variance of natural logarithms of medians:

$$S_\mu^2 = \Sigma(\mu_i - \mu_{ave})^2/n_s. \quad (11)$$

6. Determine parameters of underlying normal distribution:

$$\mu = \Sigma(\mu_i/S_i)/[\Sigma(1/S_i)] \quad (12)$$

$$S = \text{larger of } S_{ave} \text{ or } S_\mu \quad (13)$$

7. Determine mean and error factor of lognormal distribution:

$$Mn = \exp(\mu + S^2/2) \quad (14)$$

$$EF = \exp(1.645\ S). \quad (15)$$

RESULTS

Selected component failure rate estimates are presented in Table 1. Mean failure rates were rounded to 1, 3, or 5 times the appropriate power of 10. Also, error factors were rounded to 3, 5, 10, or 30. This rounding is reasonable for a generic data base and helps to reflect the precision of the results.

Strengths of the resulting data base include the following:

- Extensive coverage of components and failure modes (approximately 500 combinations)
- Breakdown of results by type of system and process fluid
- Wide range of sources used (commercial reactors, DOE facilities, chemical processing facilities, offshore oil drilling platforms, military systems, and others)
- Most (over 75%) failure rate distributions based on actual failure data rather than failure rate estimates
- Clear presentation of basis for each failure rate distribution, to allow for individual analysts to customize results.

ACKNOWLEDGEMENT

This work was supported by the U.S. Department of Energy under Contract Number DE-AC09-89SR18035.

REFERENCES

1. C. H. Blanton et al., *Savannah River Site Generic Data Base Development*, WSRC-TR-93-262, Savannah River Site, Aiken, SC (1993).

2. D. I. Gertman et al., *Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR)*, NUREG/CR-4639, U.S. Nuclear Regulatory Commission, Washington, D.C. (1989).

3. D. S. Cramer, *Data Base Development and Equipment Reliability for Phase 1 of the Probabilistic Risk Analysis*, DPST-87-642, Savannah River Site, Aiken, SC (1987).

4. J. N. Wilkinson et al., *Idaho Chemical Processing Plant Failure Rate Database*, WIN-330, Idaho National Engineering Laboratory, Idaho Falls, ID (1991).

5. *Offshore Reliability Data Handbook*, Offshore Reliability Data (OREDA), Norway (1984).

6. M. J. Rossi, *Nonelectronic Parts Reliability Data*, Reliability Analysis Center, NPRD-3, Rome Air Development Center, Rome, NY (1985).

7. L. C. Cadwallader and D. P. Sanchez, *Secondary Containment System Component Failure Data Analysis from 1984 to 1991*, EGG-FSP-10323, Idaho National Engineering Laboratory, Idaho Falls, ID (1992).

8. *Guidelines for Process Equipment Reliability Data With Data Tables*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY (1989).

9. *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations*, IEEE Std 500-1984, Institute of Electrical and Electronic Engineers, Inc., New York, NY (1983).

10. *Reactor Safety Study: An Assessment of Accident Risks in U. S. Commercial Nuclear Power Plants*, WASH-1400 (NUREG 75/014), U.S. Nuclear Regulatory Commission, Washington, D.C. (1975).

11. H.F. Martz and M.C. Bryson, On Combining Data for Estimating the Frequency of Low-Probability Events with Application to Sodium Valve Failure Rates, *Nuclear Science and Engineering* 13:267-280 (1983).

Table 1. Selected component failure rates.

System/Component/Failure Mode	Recommended Failure Rate Distribution (lognormal)	
	Mean	Error Factor
Water cooling/Piping/Leakage	3.0E-9/h-ft	10
/Tank/Leakage	1.0E-8/h	10
/Safety or standby valve, air-operated /Fails to open or close	1.0E-3/d	30
/Spurious operation	1.0E-6/h	5
/Pump, motor-driven/Fails to start	3.0E-3/d	5
/Fails to run	3.0E-5/h	10
Chemical processing/Safety or standby valve, air-operated /Fails to open or close	1.0E-2/d	10
/Spurious operation	3.0E-8/h	10
/Control valve, air-operated /Fails open or closed	5.0E-6/h	10
/Pump, motor-driven/Fails to start	1.0E-2/d	10
/Fails to run	5.0E-4/h	10
Compressed gas/Safety or standby valve, air-operated /Fails to open or close	3.0E-3/d	3
/Spurious operation	1.0E-6/h	10
/Control valve, air-operated /Fails open or closed	3.0E-6/h	5
/Compressor, motor-driven/Fails to start	5.0E-3/d	5
/Fails to run	5.0E-5/h	3
Ventilation/Safety or standby damper, air-operated /Fails to open or close	1.0E-2/d	5
/Spurious operation	1.0E-5/h	5
/Control damper, air-operated /Fails open or closed	1.0E-5/h	10
/Fan or blower/Fails to start	5.0E-3/d	5
/Fails to run	3.0E-5/h	3

RISK BASED REGULATION CONFIGURATION CONTROL FOR THE JAMES A. FITZPATRICK NUCLEAR POWER PLANT

C. J. Everline[1], M. G. Stamatelatos[1], and F. M. Quinn[2]

[1]SCIENTECH, Inc.
San Diego, CA
[2]SCIENTECH, Inc.
Rockville, MD

INTRODUCTION

During the operation of a nuclear power plant, one or more risk significant systems, subsystems, or trains may be unavailable (e.g., due to failure or maintenance). In this connection, a "configuration state" is defined as the status of components in a plant. During operation, plant configurations change because the status of the components changes. Risk-significant configurations (i.e., configurations with risk levels significantly higher than the baseline risk level) can occur. This study examines the benefit of identifying and controlling James A. Fitzpatrick (JAF) Nuclear Plant configurations from a risk perspective.

The objectives are to:

- Identify risk-significant configurations at JAF, using the existing JAF Individual Plant Examination (IPE) and JAF historical records.
- Quantitatively assess the benefit of strategies for plant configuration control, using a risk perspective.
- Estimate the risk reduction, using JAF historical records and the existing IPE, that could be accomplished by configuration control.

Only events evaluated in the JAF IPE are considered. This limits configurations addressed to configurations that occur during full power operation.

RISK-SIGNIFICANT CONFIGURATIONS

Several parameters can be used to measure the risk associated with plant configurations. In selecting a parameter it is important to consider the objective of the risk study. There are two objectives for developing strategies to control risk significant plant configurations. One is reducing public risk by minimizing the likelihood of core damage (an important precursor to accidents that impact public health and safety). The second objective is enhancing the chances that the JAF plant operates successfully over its remaining life. Reducing the likelihood public safety is jeopardized by a core damage accident, and enhancing the chances that JAF operations are not interrupted by a core damage accident, essentially require minimizing the probability that core damage occurs during future JAF operations.

The probability that core damage occurs during future JAF operations is a function of the: unconditional configuration occurrence frequency; mean configuration duration (i.e., the

length of time the plant remains in a configuration averaged over the number of times the configuration occurs); the conditional core damage frequency, given that the configuration occurs; and the remaining plant operating life. The product of the first two parameters (the unconditional configuration occurrence frequency and mean configuration duration) is simply the probability that the plant experiences the specific configuration.

Theoretically, the configuration occurrence probability and conditional core damage frequency can be calculated directly from the plant IPE. However, the review of JAF historical records discloses that high risk configurations occur more often than predicted by IPE data and the supposition that basic event probabilities are independent. Moreover, in reviewing historical records it is easier to identify high risk configurations that have actually occurred if conditional core damage frequencies are known. Consequently, the primary risk measure used in the JAF risk based regulation configuration control study is the conditional core damage frequency, given that the configuration occurs.

Table 1 lists the highest ranked basic events (from the IPE) for each major JAF system. This also provides a method for ranking systems. System ranking is an important configuration control consideration because plant Technical Specifications and many procedures are developed at a system, rather than a component, level. According to Table 1, the 125 Vdc electric power system is most risk significant system at JAF since a common cause failure of both batteries results in the highest conditional core damage frequency for

Table 1. Highest Ranked Basic Events in Each Major JAF System

Rank	System	Highest Ranked Basic Event
1	125 Vdc electric power	DC1-CCF-HW-BATTS
2	Emergency service water	ESW-CCF-FR-PUMPS
3	Emergency diesel generators	EDG-CCF-HW-4EDGS
4	Residual heat removal system, low pressure coolant injection mode	XHE-ASP-MC-RPTXR
5	4.16 kV electric power	AC4-XHE-MC-UVRLA
6	600 Vac electric power	AC6-SBR-DN-EP2A
7	Reactor core isolation cooling	XHE-ASL-MC-RLTXR
8	120 Vac electric power	AC1-XFR-HW-AC-A4
9	Residual heat removal service water	RSW-CCF-PF-2MDPA
10	Residual heat removal system, suppression pool cooling mode	SPC-MSW-FU-SW17A
12	115 kV	AC0-SBR-DN-10022
13	Standby liquid control	SLC-XHE-RE-XVMAN
14	High pressure coolant injection	HCI-MAI-MA-HPCIU
15	Diesel generator room ventilation	XHE-FRD-RE-FIRDP

singlet configurations (i.e., configurations comprised of a single, overtly unavailable, basic event). This is followed in order of importance by the emergency service water and emergency diesel generator systems. However, the preeminence of the 125 Vdc electric power system is evident from the observation that the conditional core damage frequency associated with basic event DC1-CCF-HW-BATTS is over a factor of 40 higher than any other value obtained in the analysis of singlet configurations.

All possible doublet configurations (i.e., configurations involving the overt unavailability of two basic events) were evaluated using the JAF master cut set equation. This evaluation also demonstrates the risk preeminence of the 125 Vdc electric power system. With one exception, all of the 256 highest ranked doublet configurations involve a major fault in this system (either loss of power to important 125 Vdc panels or a common cause failure of both batteries), all of these configurations have conditional core damage frequencies above 5.7×10^{-2} (per year), and no doublet configurations involving a common cause failure of both batteries have conditional core damage frequencies below 6.3×10^{-2} (per year). The next highest ranked doublet configuration has a conditional core damage frequency of 2.0×10^{-2} (per year). Moreover, comparing the singlet and doublet configurations discloses that the conditional core damage frequencies for the singlet configuration, DC1-CCF-HW-BATTS, and all of the doublet configurations involving this basic event are virtually identical. This means that the risk from doublet configurations involving the loss of both 125 Vdc batteries is dominated by the risk from common cause battery failure, alone. This result is physically reasonable because many JAF systems rely on 125 Vdc power for startup and operating control.

The one configuration among the 256 highest ranked doublet configurations that does not involve a major fault in the 125 Vdc electric power system is {ESW-CCF-FR-PUMPS, XHE-ASL-MC-RLTXR}. These basic events are ranked second and fourth in Table 1, and indicate the risk significance of the corresponding systems even when doublet configurations are considered.

One interesting difference between the singlet and doublet configuration rankings is the lower risk significance of the emergency diesel generators when doublet configurations are evaluated. Ignoring emergency diesel generator failure in conjunction with major faults in the 125 Vdc system (where the conditional core damage frequency is dominated by the 125 Vdc system fault), the highest risk doublet configuration involving emergency diesel generator failures is {EDG-CCF-HW-4EDGS, ESW-CCF-FR-PUMPS}. This configuration has a conditional core damage frequency of 2.6×10^{-3} (per year), only slightly higher (by a factor of ~2) than the conditional core damage frequency for the basic event, ESW-CCF-FR-PUMPS, alone. It is concluded from this observation that the emergency diesel generators are less risk significant when doublet configurations are considered because of the dependence of higher ranked support systems (e.g., the 125 Vdc electric power system and the emergency service water system).

The risk significance of the 125 Vdc electric power system was examined further by constructing a set of triplet configurations. These triplet configurations evolved by first combining the basic event, DC1-CCF-HW-BATTS, with every doublet configuration previously analyzed. Mutually exclusive configurations are eliminated by deleting any triplet that contains either the basic events, {DC1-CCF-HW-BATTS, DC1-BAT-HW-BATTA}, or {DC1-CCF-HW-BATTS, DC1-BAT-HW-BATTB}. Table 2 displays the salient results.

The two highest risk configurations in Table 2 correspond to the two highest risk doublet configurations with the basic event, DC1-CCF-HW-BATTS, added. The 12% increase in the conditional core damage frequency evident in Table 2 is not considered risk significant. Nevertheless, these two triplet configurations illustrate the importance of the 125 Vdc electric power system at JAF.

Common cause failure of the emergency service water pumps, in conjunction with miscalibration of the reactor low pressure interlocks pressure transmitters, appear third in Table 2, which indicates that basic events, ESW-CCF-FR-PUMPS and XHE-ASL-MC-RLTXR retain their risk significance even when triplet configurations are examined.

Table 2. Salient Triplet Configurations Common Cause 125 Vdc Battery Failure

Frequency (per year)	Configuration
$6.6x10^{-1}$	DC1-BDC-ST-BCB2A, DC1-BDC-ST-DC-B2, DC1-CCF-HW-BATTS
$6.6x10^{-1}$	DC1-BDC-ST-DC-A2, DC1-BDC-ST-DC-B2, DC1-CCF-HW-BATTS
$1.2x10^{-1}$	ESW-CCF-FR-PUMPS, XHE-ASL-MC-RLTXR, DC1-CCF-HW-BATTS
$1.2x10^{-1}$	DC1-BDC-ST-BCB2A, DC1-BDC-ST-BCB2B, DC1-CCF-HW-BATTS
$1.2x10^{-1}$	DC1-BDC-ST-BCB2A, DC1-CBL-HW-BATTB, DC1-CCF-HW-BATTS
$1.2x10^{-1}$	DC1-BDC-ST-BCB2B, DC1-CBL-HW-BATTA, DC1-CCF-HW-BATTS
$1.2x10^{-1}$	DC1-CBL-HW-BATTA, DC1-CBL-HW-BATTB, DC1-CCF-HW-BATTS
$1.2x10^{-1}$	DC1-BDC-ST-BCB2B, DC1-BDC-ST-DC-A2, DC1-CCF-HW-BATTS
$1.2x10^{-1}$	DC1-BDC-ST-DC-A2, DC1-CBL-HW-BATTB, DC1-CCF-HW-BATTS
$8.3x10^{-2}$	AC0-SBR-DN-10022, ESW-CCF-FR-PUMPS, DC1-CCF-HW-BATTS
$8.3x10^{-2}$	AC0-SBR-DN-10012, ESW-CCF-FR-PUMPS, DC1-CCF-HW-BATTS
$7.2x10^{-2}$	DC1-BDC-ST-BCB2A, ESW-MAI-MA-LOOPB, DC1-CCF-HW-BATTS
$7.1x10^{-2}$	DC1-CBL-HW-BATTA, ESW-MAI-MA-LOOPB, DC1-CCF-HW-BATTS

A total of 24885 triplet configurations involving basic event, DC1-CCF-HW-BATTS, were quantified. However, the lowest conditional core damage frequency obtained for these configurations is $6.3x10^{-2}$ (per year). This corresponds to the lowest conditional core damage frequency assessed for doublet configurations involving common cause battery failure, and implies that major faults in the 125 Vdc electric power system are so risk dominant at JAF that additional failures do not drastically increase risk since the highest conditional core damage frequency in Table 2 is within a factor of 9 of the maximum possible core damage frequency derived from the JAF IPE.

ANALYSIS OF HISTORICAL DATA

Representative results from the review of JAF historical data are presented in Table 3. The systems and equipment comprising the actual configurations, occurrence probabilities, and the corresponding conditional core damage frequencies comprise Table 3.

Table 3. Representative Historical Configurations

Configuration	Occurrence Probability		Core Damage Frequency (per year)
	IPE	Historical	
"A" RHR Down for Maintenance [RHR-MAI-MA-LOOPA] & "B" RHR, 10MOV-16B Failed to Open on Low Flow [LCI-MOV-CC-MV16B]	4.9×10^{-6}	3.2×10^{-3}	3.2×10^{-3}
"A" RHR Down for Maintenance [RHR-MAI-MA-LOOPA] & RCIC Turbine Speed Transducer Broken [RCI-TDP-FS-RCIPM]	1.9×10^{-6}	7.0×10^{-3}	7.0×10^{-3}
HPCI, 23MOV-14 Failed to Open [HCI-MOV-CC-HMV14] & RCIC Isolation due to Personnel Error [RCI-MAI-MA-RCICM]& "B" 125 Vdc Battery Bus Ground [DC1-BDC-ST-DC-B2]	1.4×10^{-9}	5.3×10^{-5}	5.3×10^{-5}

The lowest conditional core damage frequency in Table 3 is over a factor of 30 above the baseline frequency. This discloses that some relatively risk significant configurations did occur during the two operating cycles examined. However, none of the configurations resulted in exceedingly high conditional core damage frequencies (e.g., conditional core damage frequencies above 0.1 per year).

The risk impact of the Table 3 configurations can be placed in perspective by considering the overall core damage probability at JAF during the two operating cycles examined. If the average core damage frequency over these two cycles is equivalent to the IPE baseline, then the core damage probability during the two operating cycles is 3.5×10^{-6}. However, if it is assumed that the conditional core damage frequency for all JAF configurations is close to the IPE baseline except for the high risk historical configurations, then the core damage probability during the two operating cycles is 3.8×10^{-6}, an increase less than 10%. Since this computation does not include periods when the conditional core damage frequency is below the baseline, the overall core damage probability from high risk configurations historically experienced at the JAF Nuclear Power Plant appears negligible.

Table 3 exhibits significant disparity (involving orders of magnitude differences) between the IPE and historical occurrence probabilities for all configurations listed. Although the Table 3 data are merely representative, this disparity is exhibited by almost all risk significant historical configurations analyzed. Moreover, there appears to be a strong correlation between the disparate occurrence probabilities and activities involving unplanned maintenance and periodic testing.

Periodic testing is performed to determine whether any covert failures have occurred in standby systems. Covert failures are important in this regard because they increase component unavailability. To illustrate this contention, a component experiencing a covert failure will remain unavailable until the failure is detected during testing and repairs are completed. For components subjected to overt failures, repairs can begin as soon as the

failure occurs. Their unavailability is less because they do not have to remain in a failed state until the next test is performed.

Covert unavailability also increases the likelihood that configurations involving multiple component outages occur. If a component experiences a covert failure, repairs cannot begin until the failure is detected during testing. If another component fails before the first failure is detected, a doublet configuration involving both components exists. However, if the first component fails overtly and is repaired before the second component fails, the plant is not subjected to the doublet configuration. Consequently, the higher historical configuration occurrence probabilities cited in Table 3 are apparently due to covert failures that cannot be detected without surveillance testing. Scoping calculations indicate that covert failures can increase configuration occurrence probabilities by orders of magnitude above predictions using IPE values and the assumption of basic event independence. Hence, if covert unavailability is one to two orders of magnitude greater than overt unavailability for single components, two to four orders of magnitude differences are reasonable for doublet configuration occurrence probabilities when covert failures are involved.

CONFIGURATION CONTROL STRATEGIES

Any increase in core damage frequency causes plant risk to increase. Although existing Technical Specifications limit the amount of time a plant can remain in certain configurations, the core damage probability during this allowed outage time (AOT) is greater than the core damage probability over the same time interval when the plant is in the baseline configuration evaluated in the IPE.

More frequent testing of key front line and support systems, subsystems, and trains can reduce the higher risk caused by overt outages by increasing confidence in the availability of standby hardware. During operational testing, the hardware being tested is known to be operational. However, increased surveillance testing cannot guarantee system, subsystem, or train availability - it can only decrease the unavailability a limited amount. This amount depends on the STI and the type of test performed (e.g., a train that must be isolated during testing may be unable to respond to a transient during the surveillance test). These considerations are used to derive realistic unavailability values with which the impacts of diminished STIs are quantified.

Component unavailability at the end of a Surveillance Test Interval (STI) depends on the interval length and an exponential distribution rate constant. Since the exponential distribution rate constant is a function of the specific component and its environment, decreasing the STI can lower the probability that standby components fail on demand (i.e., their availability increases).

The conditional core damage frequency associated with a specific set of overtly unavailable components is very sensitive to increases in the availability of some plant components, and insensitive to increases in other component availabilities. Configuration control strategies are developed by first identifying those systems, subsystems, and trains that engender the greatest conditional core damage frequency reduction. Then, the impacts of diminished STIs are quantified. For those configurations and STIs that lower the core damage frequency to or below the level of the baseline IPE core damage frequency, the one most practical from an operations perspective is recommended.

Some configurations have conditional core damage frequencies than cannot be reduced below the baseline value, even if the unavailability of all other IPE basic events is zero. For these configurations control is achieved by limiting the AOT. If more frequent testing can lower the conditional core damage frequency of some configurations below the IPE baseline value, then a net reduction in overall risk (as measured by the plant core damage frequency) can still be obtained by limiting the duration of those configurations whose conditional core damage frequencies exceed the IPE baseline. The net reduction in overall risk realized is simply how much the configuration control strategies lower the plant core damage frequency below IPE baseline value.

APPLICATION OF RISK-BASED METHODS FOR INSPECTION OF NUCLEAR POWER PLANT SYSTEMS[1]

S.M. Wong,[2] W.E. Gunther,[2] J.W. Chung,[3] and W.D. Beckner[3]

[2]Brookhaven National Laboratory
Engineering Technology Division
Building 130
Upton, New York 11973

[3]U.S. Nuclear Regulatory Commission
Office of Nuclear Reactor Regulation
Washington, DC 20555

INTRODUCTION

As part of regulatory oversight requirements, the U.S. Nuclear Regulatory Commission (USNRC) staff conducts various routine and special inspection activities to assess the safety envelope in nuclear power plants. Currently, guidance in these inspections is provided by procedures in the NRC Inspection Manual and issuance of Temporary Instructions defining the objectives and scope of the audit effort. In several studies sponsored by the USNRC over the last few years, Brookhaven National Laboratory (BNL) has developed and applied methodologies for providing risk-based inspection guidance for the safety assessments of nuclear power plant systems. One methodology integrates insights from existing Probabilistic Risk Assessment (PRA) studies and Individual Plant Evaluations (IPE) with information from operating experience reviews for consideration in inspection planning for multi-disciplinary team inspections or individual inspections.

APPROACH AND METHODOLOGY

Typically, NRC inspection programs provide an audit function to assure compliance with regulatory requirements. Due to increased emphasis on safety significance, the NRC inspection process has been enhanced through the application of PRA insights.[1] The risk-based inspection process provides a framework for optimizing inspection resources and helps to focus on risk significant areas of plant design and operational practices. This methodology can also be used for generic

[1] Work performed under the auspices of the U.S. Nuclear Regulatory Commission.

application to light water reactor (LWR) plants without detailed PRA studies. As shown in Figure 1, the major elements of the methodology include:

1. definition of the system,
2. development of insights from PRAs and plant-specific IPEs on the role of the system in dominant accident sequences,
3. augmentation of risk-based input with information gleaned from operating experience reviews to select and rank components for inspection emphasis, and
4. identification of risk significant failure modes that require further inspection attention.

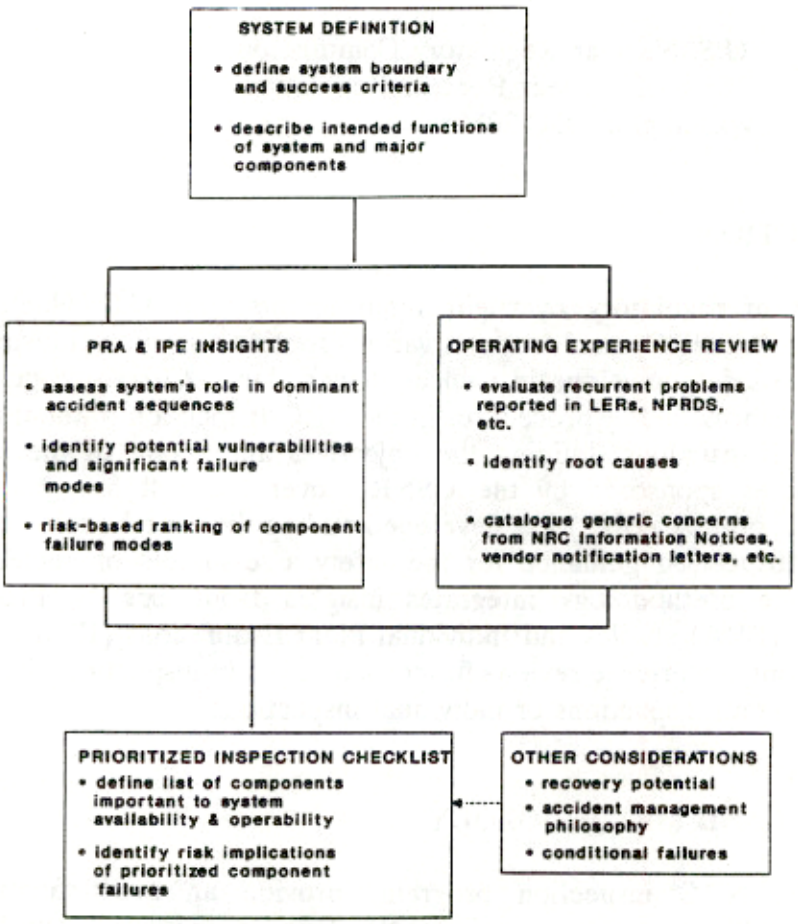


Figure 1. Risk-based methodology for optimizing inspection activities on nuclear power plant systems.

The first two elements of the process are usually well defined for safety assessments of nuclear facilities. In the case of nuclear power plants without detailed PRA studies, generic risk insights from the characterization of representative accident scenarios in both BWR and PWR plants were used to provide a risk perspective of the system's role in accident mitigation purposes.[2,3] A key element in this risk-based inspection methodology is the rationale for selection and ranking of plant components to focus the inspection effort. In this study, the rationale is based on augmenting the

risk importance of plant components with insights from operating experience review. The importance of component failures are traditionally prioritized by PRA-derived risk importance measures (e.g., Fussell-Vesely importance measure). In addition to PRA and operational considerations, the importance rankings of plant components for inspection focus are determined by including implicit considerations of recovery potential, current accident management philosophy and conditional failures to identify the less obvious, but risk significant failure modes that merit further inspection attention.

An important aspect of the risk-based inspection methodology is to determine the risk significance of inspection findings. A suitable approach in risk/reliability methodology for evaluating the relative importance of an inspection finding must include the consideration of two measures of risk significance: (i) risk implications on plant safety, and (ii) changes in system performance reliability levels due to the suspect problem. The two-pronged approach for assessing the risk significance of inspection findings is shown in Figure 2. This approach melds risk impact evaluations and system reliability calculations to determine the risk significance of each particular problem described in the inspection finding. Risk impact can be evaluated by using plant-class specific event tree models developed in the Accident Sequence Precursor (ASP) studies and input from updated databases of initiator frequencies, system/subsystem unavailabilities, and equipment failure rates. The ASP event tree models may be modified to account for the functional dependencies among support systems in order to assure completeness and consistency of the risk model. A change in system reliability level due to the existence of a particular problem can be evaluated by utilizing a fault tree model based on reconstitution of applicable generic subsystem or component train models and updated data on basic event probabilities. The insights gained from the analysis of risk significance of each particular inspection finding could then be fed back into the risk-based inspection process to focus attention on prioritized concerns in future inspections.

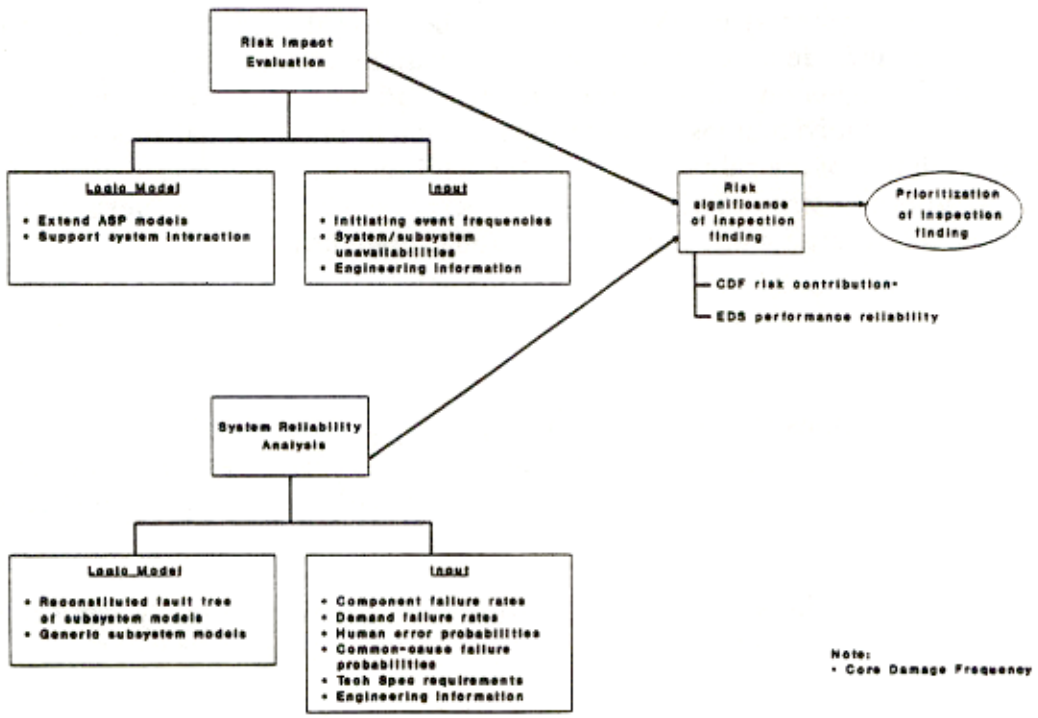


Figure 2. Risk/reliability-based approach for assessing risk significance of inspection findings.

RESULTS

Pilot tests of the risk-based inspection methodology have been demonstrated in inspection guidance provided to multi-disciplinary NRC inspection teams involved in conducting electrical distribution system functional inspections (EDSFIs) at U.S. nuclear power plants. In addition to PRA/IPE insights to identify vulnerable plant design features, risk-based guidance for EDSFIs included insights from review of Accident Precursor Study (NUREG/CR-4674) reports, EDS-related Licensee Event Reports, and electrical component failures reported in the NPRDS database to provide an overview of significant EDS events and recurrent problems. The catalogue of these risk-based insights on EDS functionality was found to be useful in prioritizing inspection activities as well as a key element in identifying risk significant inspection findings. Some of the risk significant inspection findings in EDSFIs identified by this process include:[4]

a) voltage dip problems at medium and low voltage ESF buses,
b) circuit breaker protection and coordination problems,
c) undervoltage relay setpoint errors,
d) emergency diesel generator availability problems,
e) DC power supply problems,
f) 120 V vital AC power supply problems, and
g) transformer overloading concerns.

The importance of these EDS inspection findings could be evaluated in terms of risk implications on plant safety to sort out generic issues for resolution and regulatory decision-making purposes.

Further applications of the risk-based methodology have been shown to be workable in the development of Risk-based Inspection Guides (RIGs) for inspection of high pressure injection systems (e.g., high pressure coolant injection and high pressure core spray systems) in BWR plants.[5] The current format and content of these system RIGs include a walkdown checklist of major components grouped by risk significance, and insights on risk significant failure modes from operating experience reviews to assist the individual inspector in the assessment of functional adequacy and operational readiness of the subject system. This RIG format also allows flexibility for inspectors to utilize their own field inspection experience to take a "vertical cut" assessment across programmatic and organizational boundaries.

CONCLUSIONS

On the basis of lessons learned from actual participation in EDSFIs, PRA-based operational safety and performance assessments, and HPCI/HPCS system inspections using the system RIGs, some of the key benefits of the risk-based inspection process include:

a) enhanced credibility and a rational basis for the selection of safety significant inspection items and subsequent evaluation of inspection findings,

b) optimized inspection strategies and possible reduction in inspection planning times, and

c) enhanced communication of possibly "hidden" safety concerns to plant management responsible for maintaining safe, reliable operation of a nuclear power plant.

Finally, potential applications of risk-based methods for operator licensing activities were explored to enhance the operator qualification process. A significant consideration in developing guidance for operator license reviews is the identification and prioritization of core damage scenarios for test modules in operator licensing examinations. The risk-based approach in operator licensing activities would help to improve operator quality on risk significant scenarios and thereby, result in the reduction of risks associated with human performance.

REFERENCES

1. K. Campe, J. Chung, and S. Long, "PRA Guidance in Nuclear Regulatory Commission Inspection Efforts," PSA' 89 - International Topical Meeting on Probability, Reliability, and Safety Assessment, Pittsburgh, PA, (1989).

2. R. Travis, J. Taylor, and J. Chung, "Generic Risk Insights for GE Boiling Water Reactors," NUREG/CR-5692, BNL-NUREG-52282, Brookhaven National Laboratory, Upton, NY (1991).

3. R. Travis, et al., "Generic Risk Insights for Westinghouse and CE Pressurized Water Reactors, "NUREG/CR-5637, BNL-NUREG-52260, Brookhaven National Laboratory, Upton, NY (1990).

4. S. Wong, "Risk/Reliability Methodology for Evaluation of Electrical Distribution Systems in Nuclear Power Plants," BNL Technical Report L-2065/6-23-92, Brookhaven National Laboratory, Upton, NY (1992).

5. S. Wong, A. DiBiasio, and W. Gunther, "High Pressure Coolant Injection (HPCI) System Risk-Based Inspection Guide - Browns Ferry Nuclear Power Station," NUREG/CR-6022, BNL-NUREG-52370, Brookhaven National Laboratory, Upton, NY (1993).

ASSESSMENT OF EXISTING PLANT INSTRUMENTATION FOR SEVERE ACCIDENT MANAGEMENT

Alan J. Horn, Douglas E. True

Safety and Reliability Division
ERIN Eng. and Research, Inc.
2175 N. Calif. Blvd., Suite 625
Walnut Creek, CA 94596

Seung Oh

Nuclear Power Division
Electric Power Res. Institute
3412 Hillview Avenue
Palo Alto, CA 94303

INTRODUCTION

Since the Three Mile Island-Unit 2 (TMI-2) accident in 1979, the nuclear utility industry has been studying various issues concerning the ability to successfully manage the risks associated with severe accidents. One area of this effort is the study of instrumentation and its usefulness under adverse accident conditions. Instrumentation performance during the TMI-2 accident was examined under a joint GPU, EPRI, NRC and DOE (GEND) program. During the TMI-2 accident, instruments inside the containment experienced severe environmental conditions such as high temperature steam, containment spray, hydrogen burn, and release of fission products. The summary report[1] of the examination concludes that: (1) The basic design of nuclear plant instrumentation is sound and inherently rugged, and (2) Most failures were caused by moisture intrusion which was due to faulty installation or maintenance. The lessons learned from this investigation were reflected as part of the post-TMI action plan through Reg. Guide 1.97[2]. The implementation of this post-TMI action further enhanced the instrument capability under adverse environments.

In light of TMI-2, and to further improve the safety of nuclear plants, the U.S. NRC issued SECY 88-147, "Integration Plan for Closure of Severe Accident Issues." In the plan, the enhancement of accident management capabilities is listed as an essential part of the regulatory closure of severe accident issues. This defense-in-depth approach to safety is expected to complement plant-specific risk evaluations, Individual Plant Examinations. In severe accident management, correct and successful interpretation of a plant's instrument response during severe accidents is important. There have been several studies examining instrument performance under a spectrum of potential severe accidents[3,4,5,6]. Most of these studies were performed without real plant applications and used plant equipment qualification data to evaluate the instruments' usability. This resulted in an overly pessimistic list of instruments that would be usable during a severe accident.

In this paper, we present an approach to assess nuclear plant instrumentation for use in severe accident management and the results of trial applications for two plants. The approach utilizes IPE results and plant instrumentation data. It systematically reviews the information needs and evaluates the adequacy of the instrumentation to meet the needs. In evaluating the adequacy to meet the information needs, we have used the following criteria. First, information needs should be defined as a minimum set that is necessary and sufficient to support decisions following severe accident management guidance. Second, the required accuracy of the measurement is less stringent than would be needed for normal plant operation. Third, non-safety related instrumentation can be used as a diverse means of meeting the information needs. By applying this approach, one can document the systematic evaluation of plant instrumentation for a plant-specific severe accident management plan.

METHODOLOGY

The objective of this assessment is to systematically evaluate and draw conclusions about the adequacy of existing instruments for severe accident management. The approach that we developed consists of three phases: The identification of severe accident management information needs; the determination of severe accident environmental and process conditions; and the evaluation of instruments to meet the information needs under adverse conditions.

Severe accident management information needs consist of the information necessary for plant operators and support personnel to determine the status of the plant, to determine the effectiveness of mitigating actions, and to determine the potential consequences of the accident.

Severe accident environmental and process conditions are obtained from severe accident computer code analyses and IPEs. The results of analyses of several severe accident scenarios are used in order to obtain the extent of severe conditions which plant instrumentation may experience.

The evaluation of instruments to provide the required information needs then consists of identifying instruments that can provide the basic need and comparing the existing instrument's design capability for range suitability and environmental survivability. In assuming the adequacy of instrumentation for accident management and decision making, it is important to evaluate the survivability of the instruments in the context in which they will be needed. For example, it is necessary to determine what is actually needed, not just what is nice to know; to determine when it is needed, since it may not be necessary at all times during the course of a severe accident; and to determine if there are potential alternative methods to obtain the information such as using indirect parameters or portable instruments.

Phase 1: Identification of Severe Accident Information Needs

The initial step in identifying instruments for severe accident management is to establish a minimum set of information needs. In this regard, the focus is on the information necessary for the operators and TSC staff to manage severe accidents. Some past studies have focused on general information needs, driven by a phenomenological understanding of severe accidents[3,4,5,6]. In this context, it was generally assumed that more information is better. We have focused on the information needs necessary to support severe accident management guidance (SAMG) implementation. This methodology tries to find the minimum set of information needed for accident management. This can best be achieved by reveiwing plant-specific

SAMG. In the absence of plant-specific SAMG, a reasonable approach consists of identifying information needs from existing resources. Three primary inputs are considered in this step.

1). Emergency Operating Procedures
2). Severe Accident Management Strategy Options
3). Core and Containment State Assessment

Emergency operating procedure guidelines have been developed by NSSS owners' groups to recover from accidents and to prevent the progression to severe accident conditions. These have been used to develop plant-specific emergency operating procedures (EOPs). It should be noted that many of the severe accident management actions being considered by owners' groups are currently identified in EOPs as accident mitigation measures. Because of the continuity between the operator actions used in the pre-severe accident and severe accident phases of an accident, and the gradual phenomenological changes associated with this transition, this method takes into account the pre-severe accident criteria (i.e., EOP criteria) in determining information needs. This is reasonable and desirable since existing instrumentation will likely be used by operators for determining plant status and assessing the need to invoke SAMG.

Severe accident management strategy options have not been developed yet, but during a severe accident, it is envisioned that the control room operators and TSC staff will examine and apply strategies that are provided through plant-specific SAMG. The "information need" is for the initiation and assessment of the effectiveness of each strategy. Since plant-specific strategies are not yet available, this method utilizes the Candidate High Level Actions identified in the Accident Management Guidance Technical Basis Report[7] (TBR). The TBR was developed to provide a consistent technical basis for the SAMG development and is currently being used as one of the main references by utility owners' groups in developing SAMG specific to each NSSS design.

Core and containment states need to be assessed to determine the plant status since the plant status will influence the choice of possible actions and when to implement those actions. This information need is addressed through a review of the TBR and development of core and containment status "trees". The trees are developed by analysis of plant conditions that determine when a particular state exists. For example, a branch of one of these trees may show the core is badly damaged by indications of low water level in the reactor vessel, high core temperatures, and low reactor pressure. These trees can be used to provide general insights into the types of information that might be used in SAMG to determine plant status.

The results of Phase 1 is a list of information needs. An additional step at this point is to identify a plant parameter, or parameters, that can provide each information need.

Phase 2: Identification of Severe Accident Environmental and Process Conditions

Having established the information needs and parameters, the second phase is to determine the quantitative information for each parameter (its expected range) and the environmental conditions that each instrument will encounter.

Process parameter ranges and time sequences have been modeled by the Modular Accident Analysis Program (MAAP) for most U.S. utilities as part of their Individual Plant Examinations (IPEs). To evaluate the range of the expected parameter values, several representative accidents are chosen and analyzed. The general criteria used

in the selection are as follows:

1). Relative Contribution to Core Damage Frequency - More likely accident classes (based on IPE results) should be selected as the initial screen because they represent the dominant expected conditions. Then, from those accident classes, plant damage states are selected based on the additional criteria.

2). RCS/Containment Conditions - A spectrum of conditions (e.g., high/low RCS pressure, containment cooled/not cooled, etc.) are desired to represent a variety of potential conditions.

3). Phenomenological Assumptions - Key phenomenological assumptions (e.g, debris dispersal/direct containment heating) are varied to evaluate their impact.

4). Conservative Mitigation/Operator Actions - Recoveries considered in the accident sequences evaluated as part of IPEs are not considered. This results in more severe environmental conditions and enables evaluation of long term accident progression.

For each accident, five time phases are defined: 1) pre-core damage, 2) during core damage, 3) at vessel failure, 4) from vessel failure to containment failure, and 5) post-containment failure. For each of these severe accident/time phase combinations, the parameters will have an expected range that can be identified using MAAP predictions.

A limitation is placed on this process by MAAP because MAAP does not have variables that specifically relate to all of the information needs. In these cases, where the information need does not have a corresponding MAAP variable, engineering judgement is used to evaluate its process conditions. In other cases, the nodalization of the MAAP containment model is such that the specific location of a component could only be treated as being represented by the bulk average environmental conditions of the MAAP node. In order to ensure that this assumption is reasonable, a review of each instrument loop is made to compare component locations, including the various loop components, with areas of potentially severe local conditions (i.e., near the reactor cavity/instrument tunnel inlet (PWR), near the pedestal door (BWR), etc.).

The MAAP code also provides the environmental conditions during the severe accidents. It is recognized that MAAP was not designed with this in mind, but it nevertheless provides a reasonable envelope of values for area temperatures and pressures. Humidity is generally assumed to be at 100% and radiation dose will be individually evaluated. This information is used in Phase 3 for the evaluation of instrument survivability for the time phase being reviewed.

Phase 3: Evaluation of Instruments to Meet the Information Needs

With the information needs, associated parameters, required parameter range, and maximum environmental conditions during each accident time phase, the next step is the identification and screening process of candidate instrumentation. Phase 3 consists of identifying instruments to provide needed parameters, comparing instrument design capability to the expected conditions, and determining the suitability of the instruments. In order for an instrument to be suitable and survivable, all of the components supporting the instrument must function. Those instruments that are found to be not suitable are analyzed to determine whether alternatives exist for measuring the information needs. In cases where no alternative exists, an effort is made to identify alternative approaches that can infer the information. In addition, some instruments are not required for the entire duration of the accident. Therefore,

if they fail after they are no longer needed then it is not necessary to find alternatives or other means of determining a particular information need.

A variety of plant sources are generally available to identify instruments to fit the information need parameters including P&IDs, instrument lists, functional loop diagrams, EQ lists, instrument data sheets, and Reg. Guide 1.97 lists.

The final task is to compare the identified instrumentation ranges and environmental qualification with the expected severe accident conditions for each accident class and time phase. Ideally, each information need will have a combination of instrumented parameters that will collectively satisfy the need under the applicable accident class/time phase combinations. If the instrumentation satisfies the needs, then it is determined to be "OK". If satisfactory instrumentation is not identified in this initial review several contingencies are available:

1). The required parameter range may be re-examined based on a review of the emergency procedures, core/containment assessment, and CHLA implementation information needs. That is, a parameter that covers the entire range generated by MAAP may not be necessary for successful severe accident management.

2). Instrument manufacturer data may be reviewed to determine if extending the instrument range or environmental capability is possible.

3). Instrument interpretation aids can be developed for diagnosing and interpreting failed or degraded instruments[8].

4). Calculational aids can be developed as needed to augment instrument utility to allow the use of indirect parameters.

In addition, some instruments may be "OK" even though they are not explicitly suitable or survivable. This is because the information needed is not an exact number, but "on the order of", or "about", or "rising/falling", and that degradation of the instrument accuracy may not be a concern.

TRIAL APPLICATION

This methodology was applied to two trial applications, one PWR (4-loop, Westinghouse design) and one BWR (BWR-5, Mark II). Information needs were identified using existing emergency operating procedures and information from the TBR, and parameter ranges and environmental conditions were determined by MAAP. The scenarios for the MAAP runs were chosen to provide harsh conditions that would challenge the existing instrumentation. Instrumentation was identified that would provide the information needs and then was assessed to determine its suitability and survivability.

Results of the assessment indicate that existing plant instrumentation can provide the information needs where required during the various phases of severe accidents or alternatives are available to either directly or indirectly measure the required parameters. Not all of the plant instrumentation will work during all of the phases of a severe accident, but it was found that some of the information needs are not required for all of the phases. For example, one of the PWR RCS pressure transmitters will probably fail late in many accident scenarios, after vessel failure, but, after vessel failure, RCS pressure is not a necessary information need.

The trial applications identified 12 potential information needs that are not satisfied by direct measurements. Of these 12 information need parameters, except for two parameters (containment hydrogen concentration and containment atmosphere temperature), alternative methods were easily identified to obtain the needed

information. The containment hydrogen concentration is monitored by post-accident systems that are designed to provide hydrogen concentration information at least into the early stages of severe accidents, and will actually work up to vessel failure in most cases. Alternative methods of obtaining grab samples for laboratory analysis are available. Also, accident mitigation actions could be developed for this case since, in severe accidents, hydrogen will be present, even if the exact amount is unknown.

The containment atmosphere temperature is monitored by many temperature elements located throughout the containment. They are expected to survive for most severe accident scenarios. Extreme temperature is expected if no containment spray is available for a long period. In this case, the temperature elements provide information of severe conditions inside the containment until some point beyond their design limits, in most cases until after vessel failure (without containment sprays). Because of this, the temperature elements will probably be useful to help determine when the reactor vessel fails. It is worthwhile to note that the extreme temperature conditions will not be present if there is water addition (sprays) into the containment. Hence, water addition into the containment, a severe accident management strategy, is one of the options to increase the instrument availability.

CONCLUSIONS

The results of applying this methodology to two trial nuclear power plants, one PWR and one BWR, indicates that information needs for severe accidents are not extensive, that is, not many distinct options are required. There are some instances where plant instrumentation may not directly provide the required information or survive the harsh environment, but they provide the information needs when required, or there are indirect parameters that can provide reasonable information, or portable instruments can be used where necessary.

REFERENCES

1. R.D.Meininger, "Three Mile Island Technical Information and Examination Program Instrumentation and Electrical Summary Report," GEND-050, July 1985.
2. "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following as Accident," Reg. Guide 1.97, U.S.NRC.
3. "Instrumentation Availability During Severe Accidents for a Boiling Water Reactor with a Mark I Containment", NUREG/CR-5444 (EGG-2661), February 1992.
4. "Instrumentation Availability for a Pressurized Water Reactor with a Large, Dry Containment During Severe Accidents", NUREG/CR-5691 (EGG-2638), March 1991.
5. "Accident Management Information Needs for a BWR with a Mark I Containment", NUREG/CR-5702 (EGG-2639), May 1991.
6. "Accident Management Information Needs, Volume I - Methodology Development and Application to a Pressurized Water Reactor (PWR) with a Large, Dry Containment", NUREG/CR-5513 (EGG-2592), March 1990.
7. "Accident Management Guidance Technical Basis Report", Vols. 1 and 2, EPRI TR-101869, December 1992.
6. "Instrument Performance Under Severe Accident Conditions: Ways to Acquire Information From Instruments Affected", EPRI TR-102371, 1992.

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.)

SURVEY AND EVALUATION OF AGING RISK ASSESSMENT METHODS AND APPLICATIONS*

D. Sanzo and P. Kvam

Engineering and Safety Analysis Group
Probabilistic Safety Assessment Section
Los Alamos National Laboratory
Los Alamos, NM 87545

G. Apostolakis, J. Wu, T. Milici, N. Ghoniem, and S. Guarro

Advanced System Concepts Associates
2250 E. Imperial Hwy.
Suite 200
El Segundo, CA 90245-3547

The Nuclear Regulatory Commission (NRC) initiated the nuclear power plant aging research (NPAR) program about 6 years ago to gather information about nuclear power plant aging. Since then, this program has collected a significant amount of information, largely qualitative, on plant aging and its potential effects on plant safety. However, this body of knowledge has not yet been integrated into formalisms that can be used effectively and systematically to assess plant risk resulting from aging, although models for assessing the effect of increasing failure rates on core-damage frequency have been proposed.

The purpose of this review is to survey the work conducted to address the aging of systems, structures, and components (SSCs) of nuclear power plants (NPPs), as well as the associated data bases. The review takes a critical look at the need to revise probabilistic risk assessments (PRAs) so that they will include the contribution to risk from plant aging, the adequacy of existing methods for evaluating this contribution, and the adequacy of the data that have been used in these evaluation methods. A preliminary framework is identified for integrating the aging of SSCs into the PRA, including the identification of needed data for such an integration.

The major findings of this review are as follows.

- The issue of aging in NPPs cannot be addressed by models that are based solely on the current PRA structure and failure rates, such as the proposed plant-level and component-level models [NUREG/CR-5510 (Vesely, 1990) and NUREG/CR-4769 (Vesely, 1987)]. SSCs that the basic PRA model neglects as having very small

failure probabilities and the principal degradation mechanisms, e.g., fatigue, embrittlement, and erosion-corrosion, must be considered.

- Probabilistic models for degradation mechanisms would allow the effective use of information regarding the aging of SSCs, which is similar to that collected by the NPAR program. Failure-rate-based models cannot accommodate this type of information, which typically does not include significant numbers of failures.
- Probabilistic models for the degradation mechanisms also would allow effective risk management strategies to be developed. For example, in probabilistic models for fatigue, the crack nondetection probability is an important input; the effect of taking steps to improve this probability could never be assessed in the context of failure-rate models.
- The development of a methodology that includes aging mechanisms can build on existing PRA models, appropriately modified, as current external-event analyses do.

Current PRA practice is reviewed to identify the underlying assumptions of plant modeling and data treatment methods. This review considers PRA plant and system modeling, event-tree and fault-tree modeling and the underlying hypotheses and estimation techniques and the underlying assumptions of component failure probability. Based on this review, the PRA models and assumptions that need to be reassessed when aging effects may be present can be summarized follows.

1. As a general practice, event-tree and fault-tree analyses of current PRAs do not include passive SSCs (e.g., numerous valve bodies, cables, reactor vessel supports, containment, piping, and the reactor vessel). The argument for doing so is that the failure rates for the passive SSCs are negligibly small. Although this argument may be reasonable when SSCs are new, a critical evaluation of this assumption is needed when the subjects of the investigation are older.
2. The traditional PRA approach assumes a constant rate for each component failure mode, neglecting the possible effect of aging.
3. Except for the failure rates of identical components that have been covered by common-cause failure analyses and by complete state-of-knowledge correlation, the current PRA methodology does not model other kind of dependencies. Aging may introduce additional correlations of failure rates even among dissimilar components.
4. Failure probabilities of events other than hardware failures (e.g., pre-accident and post-accident human error rates, component unavailability because of testing and maintenance, etc.) could be different for older plants from those for new plants. The current PRA methodology does not make such a distinction, and this should be investigated further.
5. External-event analyses need to be revisited. For example, aging may cause a shift in seismic fragility curves and the degradation of fire barriers.

The models and methods that are used to estimate the reliability of components and systems that are subject to age-related degradation are reviewed; the linearly increasing failure-rate model (Vesely, 1987) is the primary model reviewed. The principal question that is addressed is "Under what conditions, or in what time interval of an aging component's life, a failure distribution derived from a detailed physical models leads to a failure rate that can be approximated reasonably by a linearly increasing function?" To answer this question, we examine several models that have been proposed for three important degradation mechanisms (fatigue, radiation embrittlement, and stress-corrosion cracking). Each model is discussed and presented in terms of its objectives and its formulation. The assumptions made in the model formulation are presented, as is a commentary on whether these assumptions can be considered valid under general conditions, and if they are not, under which specific condition they still may be valid.

This review concludes that a linearly increasing failure rate model would not generally and unconditionally be applicable to many aging-related degradation mechanisms. Even in the case where the damage accumulates linearly with time, the derived failure rate is, in general, a complicated function of time rather than a simple linear function. Further detailed modeling of the specific damage-accumulation mechanisms, as well as the

conditions that lead to failure, would have to be carried out to determine whether, and under what conditions, or in what time phase of the life of a specific class of components, the model of the linear failure rate remains a reasonable approximation. The currently available information is not sufficient for us to determine whether the linear model is a reasonable approximation in the life-time phase of interest for nuclear plant aging. For fatigue in particular, it is shown that, even though the damage accumulation resulting from fatigue may be (and commonly is in design applications) modeled as approximately linear, this model of linearly accumulated damage does not necessarily lead to a linearly increasing failure rate.

A major drawback of directly assuming a form for the failure rate (linear or not), rather than starting from the formulation of physical models for the degradation mechanisms, is that the underlying physical phenomena and parameters are not even identified in the analysis. This masking of the physics of the problem can affect aging risk management significantly. For example, working only with failure rates does not allow one to evaluate and understand the effect of an improved crack-detection probability on the reliability of a pipe. The proper way to do this would be to work with physical models that deal explicitly with crack growth.

The major advantage of the linear failure rate model is its simplicity and ease of application. If it could be demonstrated that this model is a reasonable approximation to the reliability of components experiencing age-related degradation, then it would be a very attractive choice. However, as stated earlier, for most of the degradation mechanisms of interest in nuclear plants, the true range of validity of the model has yet to be determined. Beyond the issue of the model validity in providing a means of estimating reliability and risk, a limitation would still remain in the model's inability to provide estimates of the effect of specific aging-management strategies on the probability of failure of components subject to aging mechanisms of a known physical nature.

The plant-level risk model proposed by Vesely in 1990 and 1992 uses Taylor-series expansions to incorporate aging effects into PRA. This model relates the change in individual component unavailabilities because of aging to the change in the overall plant risk (usually the core-damage frequency) through a Taylor-series expansion of the basic PRA model that calculates this risk from component unavailabilities. The results of the analysis are used to evaluate the effectiveness of maintenance and surveillance in controlling aging and to direct resources to those SSCs that are most important to NPP risk. Our review of this model has led to the following observations.

1. Aging may increase the importance of factors that had been judged as negligible or had not been accounted for in the basic plant-risk model. Most important in this regard is the possible increase in the failure probabilities of major passive components, such as the reactor pressure vessel and the reactor coolant piping, and of passive elements of active components, such as pump casings and valve seats.
2. Even though the model is presented in terms of changes in component unavailabilities, the only contribution to the unavailabilities currently considered is that resulting from changes in the failure rates. In fact, expressing the model in terms of changes in failure rates would be more appropriate because various contributions to unavailability, e.g., that because of testing, would be explicitly included. In general, the failure rate would appear in several of these terms.
3. Considering the effect of aging on risk through component unavailability is too restrictive because there are situations in which factors other than component unavailability may contribute to risk. For example, aging components (such as batteries) may reduce the available time for operator action during accidents, thus altering the probability of successful operator actions. More generally, any contributions that are analyzed based on the physics of the situation cannot be placed in this formalism. This includes seismic and fire analysis and Level 2 phenomena.
4. The restriction to component unavailabilities and failure rates masks the physics behind the various contributors to risk, thus inhibiting risk management.

It should be noted that, notwithstanding the above observations, the idea of building on the existing PRA model to assess the effect of aging on plant risk is a good one and should be preserved as much as possible.

The data used in NPP aging analyses were reviewed. The data used in the NPAR program include generic and plant-specific operating experience, plant documents, test and research results, and expert judgments. The most extensive data base used in aging-risk analyses is the TIRGALEX (Technical Integration Review Group for Aging and Life Extension) data base, which was developed at a workshop held in May 1987 (Levy et al., 1988). This data base, which was used in studies by Vesely et al. (1990 and 1992) under the NPAR program, provides the input necessary to evaluate (1) the risk significance of component aging (RSCA) and, hence, a component contribution to plant risk because of aging; (2) the risk significance of component aging and aging management practices (RSCAAMP); and (3) the effectiveness of current management practices of the industry for maintaining an acceptable level of plant risk in the presence of aging components. The overall objective of the TIRGALEX program was to set priorities for the aging evaluation of structures and components. Based on our review, we have the following observations.

1. The TIRGALEX database was intended to provide more of a relative ranking of the aging features of the various equipment categories than absolute numerical values for aging of such SSCs. However, these numerical values are used extensively as they are an essential input in the linear-failure-rate model
2. The data base is the result of unstructured expert-opinion elicitation procedures and, as such, is subject to the well-known location and variability biases (in other words, the values reported may be widely off the mark). Uncertainty ranges are not reported.
3. The data base is intended to be used as a generic data base that reflects industrial experience. However, in many cases, the TIRGALEX expert panel has based its judgment on a few plant-specific studies. Moreover, all numbers in the data base are assigned without statements on uncertainty, which may raise further concerns regarding the validity of its use for generic purposes.
4. Although test intervals, as well as inspection and repair probabilities, depend on the specific aging mechanism at work, no specific mechanisms are considered. This comment is related to our earlier observation, namely, that the use of failure rates alone masks the physics behind the various contributors to risk, thus inhibiting risk management.

The use of generic operating experience for identifying aging mechanisms also is reviewed. There are four principal conclusions.

1. No single data source (such as LER, NPRDS, IEEE-Std.500) provides the necessary information to perform a thorough analysis of component aging.
2. Although a combination of various sources may allow a qualitative evaluation of the failure modes, causes, and aging mechanisms, it is difficult to reach any quantitative conclusions.
3. In many cases, additional difficulties in the data analyses have been introduced because some vendors, utilities, and manufacturers have been reluctant to provide the necessary information.
4. Data from operating experience are not sufficient, in quantity or quality, for validating any of the proposed aging models (linear, exponential, or Weibull), and the uncertainties in the estimate of failure rates, and especially in the rate of change of failure rates, remain high.

Very few analyses of plant-specific aging data have been conducted. One such analysis has been conducted by PLG Inc. to evaluate aging trends in equipment failure rates, maintenance rates, and maintenance duration. Data from maintenance records of two systems of a boiling water reactor (BWR) plant with 17 yr of operating experience shows some interesting results (Bier et al., 1991). Although there is a slight tendency toward an increase in failure rates for some components, there is also a slight tendency toward a decrease in failure rates for some others. These rather ambiguous messages regarding the trend of component failure rates with time support our thesis that there is a need for deeper investigation of the underlying degradation mechanisms.

The existing physical models for aging mechanisms of passive components and the available data that pertain to these models also are studied. In general, the data required for

reliability physics-based models of passive components consists of material properties and component stressors. The availability and quality of such data vary, depending on the particular component and/or mechanism being studied. However, for actual SSCs of interest in NPPs, almost no relevant data exist except for piping and pressure vessels.

Our review indicates that, with respect to aging mechanisms, there is a large amount of information available in qualitative form that comes from operating experience. This information is particularly important for passive components, where few actual failures have been observed, although degradation related to aging has been observed (Shah et al., 1987). However, the immediate usefulness of this information in terms of quantitative measures of reliability and risk is limited because this information is qualitative in nature. Nevertheless, it is valuable because it provides insights about which aging mechanisms are affecting which SSCs and the relative importance of these mechanisms.

Based on the observations we have made on aging-related issues, we conclude that to adequately address the overall risk at an aging plant, current PRA methodology needs to be extended. This extension would be accomplished most expediently if the effect of aging on plant risk were assessed within a framework that was built on existing PRA models. Such a framework would allow the effect of aging on plant risk to be analyzed in a separate section of the PRA. This method of treating aging mechanisms "externally" is similar to that for other external hazards (e.g., seismic events, fires, and floods). This framework, shown in Fig. 1, consists of three major parts: the selection of aging components and mechanisms, the physical modeling of selected components and mechanisms, and the integration of the findings from the first two parts into the PRA.

The analysis starts with the selection of a set of aging SSCs and degradation mechanisms that are significant to plant safety. It is necessary to limit the scope of the analysis to a manageable size because physical models, such as those of probabilistic structural mechanics, involve complicated formalisms and require detailed information. A large number of components would render such an evaluation approach ineffective. Technical bases for the screening process include engineering judgment, operating experience, and risk-significance analysis. This part of the analysis yields a selected set of components and mechanisms for further investigation.

The second part of the framework deals with developing physical models for estimating the failure probabilities of the selected components and mechanisms. Several such models could be suitable for our purposes (perhaps after suitable simplification), e.g., the software package PRAISE developed for the evaluation of failure probabilities resulting from component fatigue. For other aging mechanisms, such as erosion/corrosion, more work is needed to develop physical models more suited to reliability analysis. As shown in Fig. 1, the inspection, test, and maintenance practices at specific plants directly affect the time-dependent component failure rates. These practices and their effect should be modeled explicitly in the analysis.

The third part of the proposed framework integrates plant aging into the existing PRAs. Based on the findings from the screening analysis and the physical models, the initiating events, event trees, and fault trees in the PRAs will be reviewed and updated. The modification of PRAs may include the addition of basic events to fault trees and/or constructing new event trees and fault trees. This proposed framework retains most of the basic structure of current PRA models.

The availability and adequacy of the data required for the proposed framework for aging-risk analysis are examined. Data sources that can be used in the process of selecting aging components and mechanisms (the first part of the framework) include expert judgment, operating experience, and the results of existing PRA and IPE studies.

A future TIRGALEX-like expert panel and workshop also could be useful in conducting the screening analysis. A formal evaluation of expert judgment should include structured procedures in the following areas.

1. The selection of SSC aging-related issues about which the experts will be queried
2. The identification and selection of experts
3. The design and execution of the elicitation
4. The treatment of biases of experts and biases induced during the elicitation process
5. The dependency among experts
6. The algorithms for aggregating expert judgments
7. The treatment of uncertainty

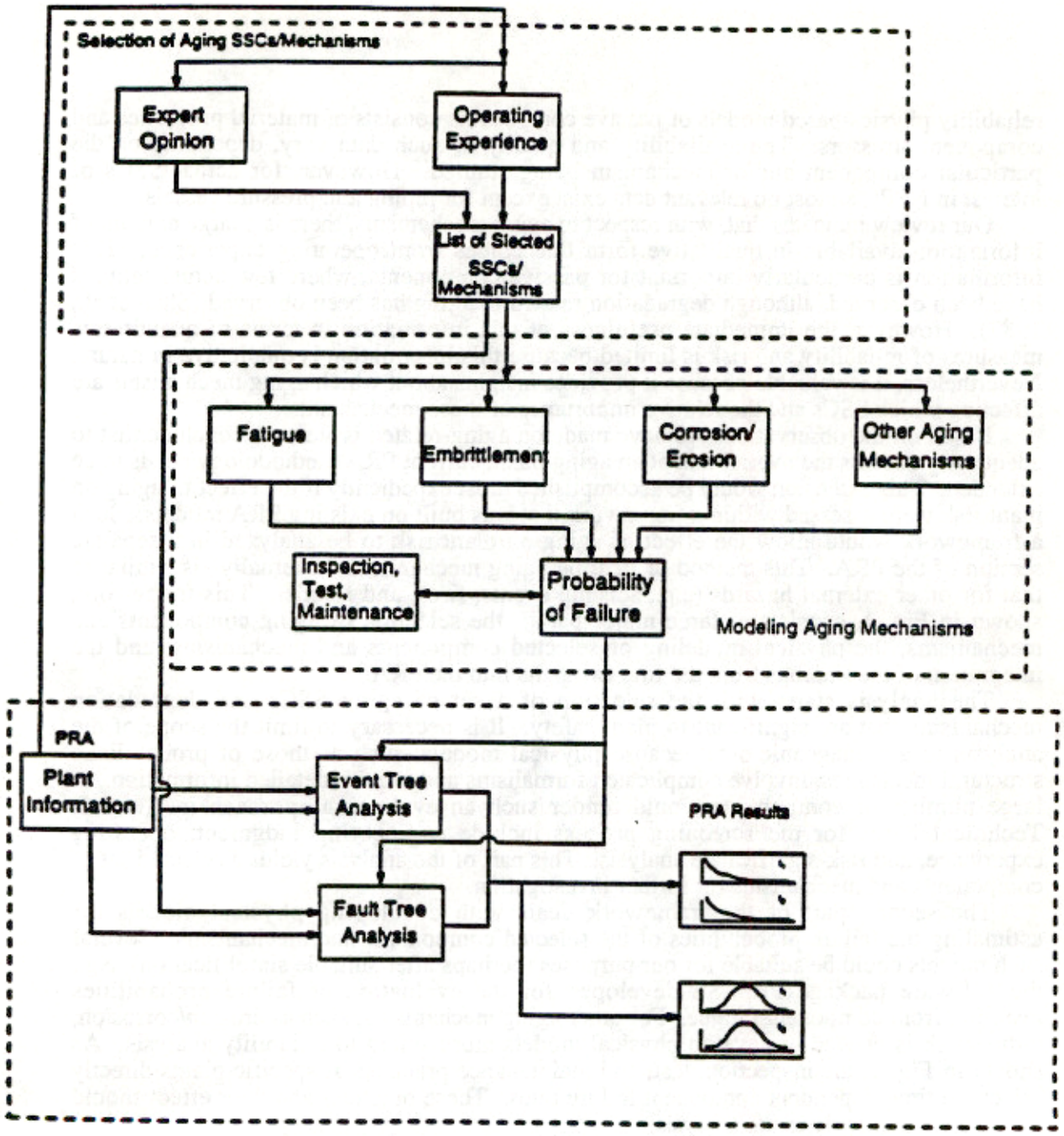


Figure 1. Aging-risk analysis.

In addition, the whole process of formal evaluation should be documented carefully. The qualitative reasoning process in support of the expert judgment constitutes an important portion of the elicitation process and also should be documented in detail.

Operating experience can provide two types of information: actual occurrences of failures caused by aging and evidence or direct observation of component degradation as a result of aging. Sources of operating experience include data from the In-Plant Reliability Data System (IPRDS) sponsored by the NRC, the Nuclear Plant Reliability Data System (NPRDS) managed by the Institute of Nuclear Power Operation, the Licensee Event Reports (LERs), plant maintenance records, in-service inspection reports and Nuclear Plant Experience (NPE) reports. Among these data sources, LER and NPRDS are the two most frequently used for aging analyses. The NPE data base is similar to that of the LER, whereas the IPRDS data base is very limited and incomplete.

When using generic data bases (such as NPRDS) in aging-risk analysis, one should be aware that they do not often contain information that is detailed and complete enough for drawing general conclusions. Events that are not of direct interest to the reporters are often overlooked or, at most, are roughly documented. The contents of the reports are often not detailed enough to allow aging-related root cause to be distinguished from other causes.

Plant-specific data generally contain more detailed information on the operational and failure history of specific systems and components. However, the major limitation of using plant-specific data in aging-risk analysis is that the number of incidents is often too small to reach a meaningful statistical conclusion, especially for plants that have only been in operation for a few years.

This situation could be improved by emphasizing the root-cause analysis in the existing data bases (such as LER or NPRDS). In particular, guidelines should be provided to the plant personnel regarding the reporting of aging-related equipment failures.

The results of plant-specific PRAs and IPEs can be useful for identifying components significantly affected by aging that are significant to plant safety. A recent study by Vesely (1992) on the prioritization of aging contributors and the evaluation of maintenance effectiveness is an example of such a use. As most PRAs and IPEs do not include passive components in their plant models, these would not be identified as risk-significant if the models were based on these data sources alone, even though some of these components might contribute significantly to aging risk. Consequently, it is important to note that the decisions made in the screening analysis should be based on sources broader than the PRA and IPE results.

Also, an assessment of the availability and adequacy of the data needed for the development of models for the aging mechanisms (the second part of the framework) is conducted. Physical probabilistic models for estimating aging effects on component failure rates often require a large amount of data related to material properties and operating conditions. In the review of degradation mechanisms and associated models, a wide range of data sources is identified.

For the aging mechanisms of fatigue and irradiation embrittlement, it is found that there is a wide availability of data related to the material properties associated with the physical modeling of these aging mechanisms. However, much of these data are presented in a conservative, deterministic framework, and it may be necessary to recast much of it in a statistical format so that probabilistic evaluations of the aging mechanisms can be performed.

For fatigue, there are a couple of areas for which the available data may not be appropriate for component and plant-specific reliability analyses. Special care should be taken when selecting crack-growth data, which can be affected by environmental effects such as corrosion. Therefore, the environmental conditions under which a component is operating should be assessed to determine whether the available crack-growth data are applicable and, if not, further research may be necessary to provide data that is appropriate. Also, more crack-growth data in the ultra-low growth-rate regime below 10^{-6} mm/cycle, approaching the so-called fatigue threshold, may be needed because fatigue lifetimes for some components can be dominated by crack extension in this region.

With respect to radiation embrittlement, it appears that, for most plants, the surveillance program provides an adequate supply of raw data to characterize the fracture mechanics parameters for a plant-specific vessel reliability study. However, for a probabilistic treatment of irradiation embrittlement, it may be necessary to convert the fracture-toughness data base into corresponding statistical data for stress intensity factors. Other areas of concern include the characterization of an initial flaw distribution and the extrapolation of neutron exposure data from the surveillance capsule locations to the vessel wall. Flaw distributions that are used in the probabilistic fracture mechanical (PFM) analysis portion of a pressurized thermal shock (PTS) risk assessment can affect the overall results by several orders of magnitude, and thus, care must be taken to use a technically appropriate flaw distribution when dealing with an integrity assessment of vessels with low upper-shelf toughness behavior.

Stress-corrosion cracking and erosion/corrosion are two damage mechanisms much less quantified and analyzed than fatigue and embrittlement. Data and models related to stress-corrosion cracking and erosion/corrosion are mainly of fundamental, rather than engineering, value, and thus, it is concluded that both data collection and modeling research are needed before reliability analyses of components affected by these mechanisms can be conducted.

REFERENCES

Bier, V. M., D. C. Bely, and D. H. Johnson, "Methods of Bayesian Aging Analysis," in *Probabilistic Safety Assessment and Management*, G. Apostolakis, Ed., Elsevier, New York, pp. 1269–1274 (1991).

Levy, I. S., J. Wreathall, G. Demoss, A. Wolford, E. P. Collins, and D. B. Jarrell, "Prioritization of TIRGALEX-Recommended Components for Further Aging Research," U.S. Nuclear Regulatory Commission report NUREG/CR 5248 (1988).

Shah, V. N. and P. E. MacDonald, Eds., *Residual Life Assessment of Major Light Water Reactor Components - Overview*, U.S. Nuclear Regulatory Commission report NUREG/CR-4731, Vols. 1 and 2 (1987).

Vesely, W. E., "Approaches for Age-Dependent Probabilistic Safety Assessments with Emphasis on Prioritization and Sensitivity Studies," U.S. Nuclear Regulatory Commission report NUREG/CR-5587 (1992).

Vesely, W. E., R. E. Kurth, and S. M. Scalzo, "Evaluation of Core Melt Frequency Effects Due to Component Aging and Maintenance," U.S. Nuclear Regulatory Commission report NUREG/CR-5510 (1990).

Vesely, W. E., "Risk Evaluations of Aging Phenomena: The Linear Aging Reliability Model and Its Extensions," U.S. Nuclear Regulatory Commission report NUREG/CR-4769 (1987).

DEVELOPMENT OF HIGH TEMPERATURE METALLIC MELTING PROCESSES RELATED TO THE DETRITIATION OF EXHAUSTED CONTROL RODS

G. MODICA *, R.NANNICINI **, H.DWORSCHAK *, F MANNONE *

* Commission of the European Communities
Joint Research Centre - 21020 - Ispra (Italy)
Tel.: 0039-332-789772
Fax: 0039-332-789108

** ENEA, Ente Nuove tecnologie Energia Ambiente
c/o J.R.C. - 21020 Ispra (Italy)
Tel.: 0039-332-788248
Fax: 0039-332-788253

1. INTRODUCTION

A rather critical problem to be faced in developing a safe strategy for the management of tritiated solid wastes is dealing with the outgassing property of tritium. Releases of tritium under elemental or oxide form may occur from waste items at different temperatures and rates depending upon the nature of tritium bonds into the waste matrix as well as on its "contamination history".

Apart from the commercial value of tritium its release from waste packages anyhow represents a risk of tritium exposure that cannot be accepted by shippers, store and disposal site operators as well as the general public.

Consequently it is mandatory to carry out the detritiation of such wastes before their packaging and storage or disposal. As and example, in France, at the CEN-Valduc the detritiation of highly tritiated steel wastes is currently practised either by surface thermal (800°C) or melting (1250°C) treatments under vacuum conditions.

The same problem concerns a tritiated non metallic waste such as exhausted boron carbide (B_4C) of neutron absorber rods used for the operating control of neutron flux in BWR cores. The tritium build up in such rods is the result of the $^{10}_{5}B$ isotope reaction with thermal neutrons leading to the formation of $^{7}_{3}Li$ ($^{10}_{5}B + ^{1}_{0}n \rightarrow ^{7}_{3}Li + ^{4}_{2}He$) which further reacts with fast neutrons to form $^{3}_{1}H$ ($^{7}_{3}Li + ^{1}_{0}n\,(f) \rightarrow ^{4}_{2}He + ^{3}_{1}H + ^{1}_{0}n\,(t)$). A second important contribution to $^{3}_{1}H$ build-up results from the $^{10}_{5}B$ reaction with fast neutrons ($^{10}_{5}B + ^{1}_{0}n\,(f) \rightarrow ^{4}_{2}He + ^{3}_{1}H$), whereas it is negligible that of $^{11}_{5}B$.

The tritium inventory accumulated in each rod is obviously proportional to the average $^{10}_{5}B$ burn-up.

In the boron carbide control rods from the LINGEN BWR [1] after about three years of operation (burn up ~43%) a tritium inventory of 23 MBq (0.85 Ci) per rod has been evaluated corresponding to a total tritium inventory of 1.35 GBq (~50 Ci) per rod assembly (60 B_4C rods per assembly).

According to the results of radiochemical analyses on samples taken from irradiated B_4C rods, tritium generated by neutron reaction (1) was essentially retained in the B_4C matrix (~99.99%) with only negligible fraction in fill gas and cladding. This is also confirmed by the results of laboratory scale research, showing most of tritium is retained in irradiated (dry) B_4C below 650°-700°C[1,2].

2. CONCEPTUAL ASSESSMENT OF PROCESS FEASIBILITY

2.1 Objectives

The objectives of the study are to demonstrate the feasibility of two processes aimed at:

i) Reducing to the maximum practicable extent the level of tritium contamination in such waste. The disposal of removed tritium has then to be carried out.
ii) Conditioning such wastes by compacting and converting them in a suitable form so that all the subsequent waste management are facilitated and may be done under more safe conditions.

Once the technical feasibilities of such processes have been demonstrated on a laboratory scale, a further objective of this study is to provide relevant input parameters and technical data needed for their scaling up to a pilot-plant.

2.2 Alternative Options

As experimentally demonstrated, a thermal treatment based on the simple heating up to 900°C is sufficient to attain the first objective, i.e. the nearly quantitative detritiation of irradiated B_4C provided some critical operating conditions are met [2]. This however does not give an answer to the question on how to subsequently process the detritiated B_4C rods (about 3 m long) for conditioning and disposal purposes.

Indeed, the simultaneous execution of both B_4C detritiation and rod compaction processes in one step could technically be more effective and rapid, while the integration of two processes in one step could perhaps result even less expensive.

At present the existing alternative process options that may be taken into account as potential candidates for detritiating and compacting purposes are the following.

a) The formation with other suitable components of an eutectic having a melting point sufficiently lower than that of B_4C itself (2450°C).
b) The chemical attack by alkaline fusion (NaOH) in the oxygen stream at relatively low temperature (700°C).
c) The alkaline fusion (NaOH) as described in point b) in presence of specific carbon oxidising agent (MgO, BaO) in oxygen stream.
d) The processes a, b or c in presence of a vitrifying agent, proportionally added to produce a final waste composite under the efficient disposable glass form.

All the above processes would enable to convert at temperatures well below 2450°C tritiated B_4C to a final partially or completely detritiated waste composite, sufficiently compacted and more safely disposable than the brittle B_4C cake (see below).

To facilitate the practical application of the above detritiation and compaction process options the mechanical dismantling of rod assemblies (3.5 m height x 0.4 width) and the mechanical parcelling of each single rod (~3.0 m height x 0.047 m width) have to be envisaged. In this context one has to point out that the rod conditioning based on mechanical parcelling of tritiated rods and the subsequent simple containerization of resulting sections is unacceptable from the safety point of view. This is due to tritium which is not sufficiently immobilised in

the rod sections to minimise the risk of tritium exposures for shippers, store or disposal site operators and general population as well.

2.3 Major Constraints

The assessment of the major constraints that may be found in parcelling and processing irradiated B_4C rods for detritiation and compaction purposes leads to the following comments.

Mechanical Parcelling of B_4C Rods

The B_4C of the BWR control rods is initially compaction vibrated into the cladding SS tube [1,3]. Under the neutron radiation effect it is found to consolidate into a solid cake [3] that could be removed from the cladding tube only by a mechanical force. This consolidation, that initiates at very low burn up, is, in combination with the production of ^4He, the major cause of the B_4C swelling hence of the circumferential stress in the absorber tube and subsequently of its longitudinal intergranular stress corrosion cracks [3]. Despite the consolidation attained during neutron absorption, the B_4C cake still remains brittle owing to the cracks produced in the B_4C original grains that increase as the burn up increases. Therefore the preparatory mechanical parcelling of irradiated B_4C rods (e.g. cutting, sawing) that is necessary to facilitate their processing becomes a critical and dangerous operation. This is essentially due to the brittleness of the irradiated B_4C cake that will cause, during any parcelling operation the production of powdered tritiated materials and their consequent dispersion inside the rod dismantling facility.

Heating and Melting

- Most of tritium has been demonstrated to be retained in irradiated B_4C heated below 650-700°C (2). Tritium starts to release at 700°C, a nearly quantitative outgassing of tritium from irradiated B_4C being achieved only at 900°C provided some specific operating conditions are met. Undoubtedly this shows evidence that tritium is rather firmly trapped and bounded ($C-^3H$, $Li-^3H$) into the irradiated B_4C matrix.
- As shown by some experimental results [2] at temperatures above 700°C the oxygen inhibits the release of tritium from heated B_4C by forming a glassy coating of B_2O_3 on the sample surface so that the further reaction of B_4C with oxygen is also inhibited. This is the reason why the B_4C heating atmosphere must be carefully purified from oxygen. Note that above 1300°C the B_2O_3 volatilizes so that an adequate trapping system has to be provided if this temperature is exceeded, as it could be required to complete tritium release or to melt SS cladding sections.
- To simultaneously perform both B_4C detritiation and absorber rod compaction a melting treatment has to be applied which would also entail the SS rod cladding sections. Obviously the required temperature to be attained for these purposes must not be so high as to make difficult and too expensive the future industrial scaling-up of the detritiation-melting plant. The application of this option to the B_4C rods alone appears to be difficult mainly because of the too high melting point of the pure B_4C (2450°C). The formation of a ternary eutectic of significantly lower melting points is therefore a more convenient option to be experimentally explored.

Chemical Attack by Alkaline Fusion

- The chemical of B_4C by alkaline fusion at 700°C in atmospheric air leads to the production of sodium borate with a non negligible amount of CO_2 (approx. 19 dm^3 per B_4C rod) in which tritium is diluted. This indeed will require a more sophisticated system for removing tritium if CO_2 is present with tritium in the entrainment atmosphere.
- The chemical attack does not entail the SS rod cladding as it is expected in the case of an eutectic formation. Therefore after such a process the compaction of a B_4C absorber rods appears to be still incomplete due to the presence of unreacted cladding sections. On the other end the melting at 1400°C of SS sections will entail the volatilization of B_2O_3 (see before).

2.4. Preliminary Conclusions

- The process option that will be firstly investigated to set up the most suitable conditions for a thermal processing of tritiated B_4C rods is the formation of a ternary alloy eutectic with Fe at a temperature far lower than the melting point of B_4C (2450°C).

- The formation of the above ternary eutectic should also enable the melting of the SS cladding of the rod simultaneously with the B_4C cake. The main advantage of this option, whose performance requires however an experimental verification, is that of eliminating the need of a preparatory mechanical parcelling of B_4C rods.

- The above process has to be carried out in a carefully oxygen-free entrainment atmosphere on to avoid the B_2O_3 formation on the B_4C surface, hence tritium retention in irradiated B_4C. Furthermore the absence of CO_2 will enable the use of a relatively simple gaseous detritiation system for removing tritium from the entrainment atmosphere .

3. LABORATORY EXPERIMENTS

3.1 Selection of the Ternary Eutectic

It is worth to remember that the main objectives of the present experimental investigation are at first to chemically decompose the boron carbide to ensure the complete removal of tritium and secondly to melt the SS cladding to avoid the individual parcelling of B_4C rods.

It is known from the literature[4] that the boron carbide can easily react with iron and iron carbide at 1000-1100°C to produce iron borides.

The possibility of achieving the first objective is supported by the existence of some eutectics of different compositions. As shown in Fig. 1 taken from Ref.[5] where the phase diagram of the Fe-B-C alloy is reported the Fe_3C-Fe_2B binary eutectic melting at 1155°C as well as the (Fe_3C-Fe_2B)-(Fe-B)-(Fe-C) melting at 1100°C can be formed. Note that the former eutectic participates with Fe-B and Fe-C eutectics to the formation of the latter one.

As indicated in the phase diagram of Fig. 1, this latter eutectic has an elemental weight percent composition of 95.5 - 3 - 1.5 for Fe - B - C respectively.

On the other end several other eutectics existing between Mn, Ni, Cr and B or C and melting at temperatures lower than 1550°C [6-7-8] let us anticipate that at the iron melting point also the component of the SS cladding (AISI 304), which is under a molten state, will further contribute to the B_4C decomposition by formation of borides or carbides.

3.2 Preliminary Exploratory Tests

According to Section 3.1 the preliminary tests concerning the B_4C decomposition have been based mainly on the formation at 1100°C of the Fe-B-C ternary alloy eutectic. This will be implemented by contacting solid B_4C with previously melted cast iron.

Samples

Based on the elemental percent composition of the Fe-B-C ternary eutectic described at 3.1, boron carbide, cast iron (UNI 5007) or elemental iron (ARMCO) and SS (AISI 304) have been utilised to prepare samples for melting tests. The components have been mixed according to the weight proportions indicated in Table 1.

The first two components were under a powder form while the AISI 304 was added either as a steel wool (tests No.3) or a steel tube section of 5 mm ext. diam. x 0.5 mm thickness (tests No. 4 and 5).

Equipment and Operating Conditions

- All experimental data are given in Table 1.
- Except for the tests No. 1, alumina crucibles were used in all other experimental tests.
- Except for the test No. 4 where an induction furnace has been used, a standard electrical resistance furnace has been utilised for all other tests. With both type of furnaces working temperatures did not exceed 1550°C.
- Except for the test No. 4 carried out under vacuum, all other tests were performed under helium stream.
- No more than a maximum total of 7 hours, have been initially spent for each melting test. One has however to point out that for last two tests carried out in presence of the AISI 304 tube only few minutes were necessary to obtain a homogeneous melt (eutectic) at approximately 1550°C.

3.3 Discussion of Preliminary Results

- Two types of crucibles were utilised for these preliminary tests. The porcelain crucible does not show any resistance to the chemical attack of the Fe_3C+B_4C mixture. Probably owing to this attack it becomes brittle and it will break in many pieces.
  As to the Al_2O_3 crucible, even if it apparently remains intact, some cracks of variable widths were visually observed on its external surface. Thermal shocks are probably the explanation of these cracks.
  As far as the materials of crucibles are concerned it is perhaps worthwhile to remember that according to the available bibliography [4] the B_4C will react at 1000 - 1100°C with Ti, V, Zr, Mo, Hf, Ta, W, Fe, Co and Ni with formation of carbides and borides.
  At higher temperatures also Pt and Pd are attacked. Only graphite exhibit an excellent resistance to B_4C at high temperatures [4].
  The selection of a crucible material of an adequate resistance to the chemical attack of B_4C at high temperature is therefore a problem to solve. The option that will be investigated is based on the utilisation of a double crucible, i.e. a graphite crucible used as an internal liner of an external metallic crucible acting as a supporting container. The utilisation of a double crucible associated with an induction furnace are reported in Refs [10,11].
  The use of an induction furnace appears to be the best choice as demonstrated by the very short time needed (see Table 1) to go up with temperature and to obtain the ternary eutectic melt.
- As reported in Table 1, from tests No. 2 to 4 it appears that the amount of carbon introduced in the mixture by cast iron and B_4C was exceeding the carbon proportion indicated by the eutectic composition from the ternary diagram of Fig. 1. This result could possibly explain the powdered carbon residue that normally has been, found together with the solidified mass obtained as the final product from tests No. 2 to 4.
- As observed during tests No. 4 and 5 cast iron or Fe mixed with B_4C do not give a homogeneous melt until the melting temperature of the SS is reached, i.e. until melted SS can contribute to the formation of the ternary eutectic that occurs in few minutes.
  The best evidence of this behaviour is obtained when SS is added to the ternary mixture (see in Table 1 tests No. 4 and 5) in form of a tube section of 5 mm ext. diam. x 0.5 mm thickness. This section is adequately positioned at the centre of the crucible with one end in contact with powder mixture of the two other components (cast iron or $Fe+B_4C$). As the SS melting point (1400°C) is reached, the SS tube goes rapidly down into the crucible to form a homogeneous liquid mixture (eutectic melt). An identical behaviour has been observed also when a fraction of the B_4C powder was filled into the section of SS tube instead of being totally poured into the crucible.
  According to these results it appears evident that also an entire B_4C rod or a whole set of rods (i.e. rod assembly wing) could continuously be processed by pulling down each rod or set of rods into the crucible as their melting go on. The application of this option, which has the essential advantage of eliminating rod parcelling operations and consequently any associated radiological risks, is therefore to be experimentally verified.

4. LAB TESTS ON BN CRUCIBLES

High temperature melting laboratory scale tests have been carried out by ENEA, in the frame of a collaboration contract with J.R.C., Ispra (Italy).
The tests were performed in a high frequency induction furnace (110. KHz - 80 Kw).
The aim was to carry out aging tests on some crucibles of BN (Boron Nitride) in order to verify the material capability of resisting stainless steel up to 1650°C.
The crucibles of 'Hot Pressed' BN were supplied by the "Boride Ceramics" english company.
The tests were carried out in presence of Ar (or N_2, only for one test) fluxed as inert gas into a quartz tube (equipped with the crucible inside). An optical pyrometer as well as W-Re thermocouples were used for measuring the temperature inside the crucible.
Both stainless steel only and a stainless steel (80%) and zirconium (20%) mixture were melted and heated up to 1650°C.
The main experimental result was that the molten stainless steel does not attack the inner side of the crucible wall, while the molten metallic mixture (S.S.+Zr) attacks it, since Zr , at high temperature (~1600 °C) probably reacts with N (from the inner crucible surface BN) to form yellow ZrN (Zirconium Nitride-M.P.=2980 °C), which can give rise to an auto-crucible containing the molten metal. So in this case the crucible is slightly corroded all along the side and the bottom. Anyway, if the temperature is kept under 1650°C (and even more when N_2 instead of Ar is used as inert gas), the corrosion level is very low.
In any case the corrosion reaction seems to occur only when BN starts to volatilize (probably as B_2O_3) forming white fumes, as one can see during heating at high temperature.
In addition a little weight loss of the crucible (together with the mass of molten metal) was noticed during each test .
Anyway, even if this last phenomenon has to be better investigated for confirmation, it has been demonstrated that BN is a refractory material very resistant both to thermal shocks and to the molten stainless steel up to 1650°C.

5. CONCLUSIONS

- After the encouraging results obtained from some exploratory tests the Ispra approach to the problem of treatment and conditioning of tritiated B_4C rod assemblies is oriented to continue tests on the melting process at 1500-1600° C in absence of oxygen. The peculiar interest of this process is due to the simultaneous melting of B_4C and SS (cladding balls and supporting material of the wings) in presence of iron or cast iron to form a ternary eutectic.
- The formation of a ternary eutectic with the contribution of SS cladding and supporting material of the rod assembly wings will enable to avoid the dismantling of the wings and the successive parcelling of each rod.
- A careful set-up of process conditions and equipment is required. The equipment will consist of an induction furnace with a controlled atmosphere and an "ad-hoc" system capable of supporting the assembly wing(s) over the crucible and always in contact with the melt. To this end the above system should provide the possibility of lowering the wing(s) into the melt as their melting proceeds.
- The chemical composition of final solid product of the melting process should be determined. These data are necessary to assess their compatibility with specific features of the final waste composites required by transport regulations and acceptance criteria of German disposal sites.
- After setting up operating conditions experimental tests involving at first tracer level tritiated B_4C and then neutron irradiated B_4C are to be envisaged to check the detritiation performance of the melting process.

6. REFERENCES

(1) A. Bleier et al., Evaluation of the Tritium Content in LWR Control and Adsorber Rods to Obtain Data for the Fuel Cycle Backend.

(2) C.C. Miles et al, Tritium Retention in EBR Irradiated Boron Carbide, ANL 8107 (1974).

(3) N. Eickelpasch et al., Operational Experience with and Postirradiation Examination on BWR Control Rods. Nucl. Tech. vol. 60 (Mar. 1983) 362.

(4) W. Stumps, Boron and Carbon1 Gmelin Handbook of Inorganic Chemistry, Boron, Supplement Vol. 2 (1981), pp. 185-186.

(5) International Critical Tables, Vol. II, MacGraw-Hill Book Co, (1927).

(6) Binary Alloy Phase Diagrams, Vol. I, American Society of Metals.

(7) F.W. Glaser, Contribution to the Metal-Carbon-Boron Systems, J. of Metals, 391-396 (1952).

(8) G. Pradelli, Ricerca sui borocarburi di cromo, La Metallurgica Italiana, 10, 551-557 (1974)

(9) W. Stumps, Boron and Carbon, Gmelin Handbook of Inorganic Chemistry, Boron, Supplement Vol. 2 (1981), pp. 188-189.

(10) H.E. Robson, P.W. Gilles, J. Phys. Chem., 68, 5 (1964), 983-989.

(11) D.L. Hildenbrand, W.F. Hall, J. Phys. Chem., 68, 5 (1964), 989-993.

Table 1 - Operating conditions and equipment utilized for preliminary experimental tests simulating the melting of B_4C rods under a controlled gaseous atmosphere.

Test	Mixture Components (g)			Type of		Melting conditions			Remarks
No	B_4C	Iron	AISI 304 [3]	Crucible	Furnace	°C	Atm	Time (h)	
1	1.50	39.5 [1]		Porcellain	SEF [6]	1250	He	7	Complete melting Chemical attack of crucible
2	1.50	39.6 [1]		Al_2O_3	SEF	1250 1550	He He	3 4	Complete melting; Same crucible cracking. Carbon powder residue.
3	1.55	34,9 [1]	4.0 [4]	Al_2O_3	SEF	1250 1550	He He	3 4	Up to 1250°C SS remains unchanged. Omogeneous melt at 1550°C. Carbon residue
4	2.0	39.6 [1]	4.0 [5]	Al_2O_3	F [7]	1550	vac.	0.16 (10')	After 1050°C cast iron and B_4C give a granular red-hot product without melting. Homoheneous melt at 1550°C . Carbon residue
5	1.55	34.2 [2]	5.0 [5]	Al_2O_3	SEF	1550	He	0.33 (20')	Homogeneous melt at 1550°C. No carbon residue.

(1) Cast iron, UNI 5007.
(2) Elemental Fe (ARMCO).
(3) Max C 0.08 w%; max Mn 2 w%; Si 1w%; Cr 18-20 w%; Ni 8-12 w%.
(4) Under metallic wool form.
(5) SS tube (5 mm ext.diam. x 0.5 mm thick).
(6) Standard Electrical resistance Furnace.
(7) Induction Furnace.

Melting points: B_4C = 2450 °C
Fe = 1535 °C
AISI = 1400 °C
Cast Iron = 1130 °C

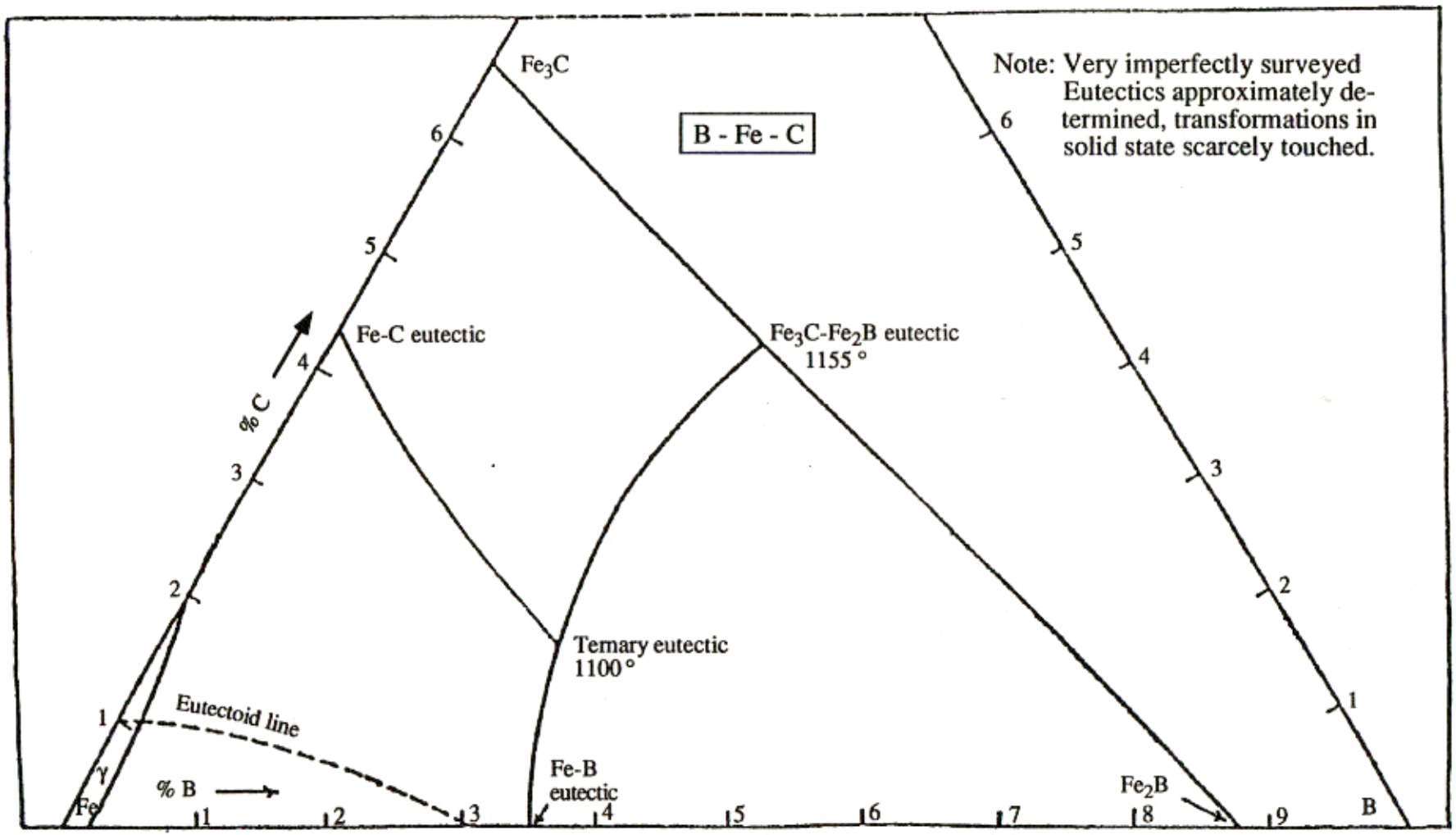


Figure 1 Fe-B-C phase diagram

USE OF SENSITIVITY ANALYSIS IN SELECTION OF UPGRADES FOR LOW SEISMIC CAPACITY COMPONENTS FOR THE ADVANCED TEST REACTOR

S. T. Khericha, S. A. Atkinson,[1] D. M. Henry,[2] and M. K. Ravindra[3]

[1]Idaho National Engineering Laboratory
Idaho Falls, Idaho 83415
[2]Tenera LP
Idaho Falls, Idaho 83401
[3]EQE International Inc.
Irvine, Ca. 92715

INTRODUCTION

The Advanced Test Reactor (ATR) located at the Idaho National Engineering Laboratory site is one of several Department Of Energy research or production reactors. EG&G Idaho has been assessing the core fuel and spent fuel damage frequency from the internal and external events using the Probabilistic Risk Assessment (PRA) technique. As part of the on going PRA for this reactor, a comprehensive and efficient seismic analysis was performed to evaluate the impact on the core and canal fuel damage frequency. This paper discusses the results of an extensive sensitivity analysis which provided a strategy for plant modifications.

An extensive sensitivity study was performed. Non-seismic failures did not contribute significantly to the total fuel damage frequency for seismic events. The bulk of the risk was due to certain low capacity components. First, a reduction in core fuel damage frequency was estimated for an individual component. The component was assigned a very high median capacity then fuel damage sequences were reanalyzed. Except for the overhead fire water injection tank and surge tank, upgrade of an individual component did not produce any significant reduction in core fuel damage frequency. However, when several selected components were assigned a very high median capacity at the same time, significant reduction in core fuel damage frequency was observed. The seismic failure modes were later evaluated to estimate the cost effectiveness of upgrading low fragility components to the high median capacities.

The key elements of seismic PRA are seismic hazard analysis, seismic fragility evaluation of structure and equipment, systems and accident sequence analysis and seismic risk quantification. The steps involved in the fragility evaluation were review of the plant design and seismic qualification information, plant walkdown, a simplified seismic response analysis to estimate realistic floor response, and estimation of the fragility

parameters for structures and equipment.

DESCRIPTION OF THE PLANT

The ATR is a 250-MW(t) test facility located at the INEL. The ATR, which began operation in 1968, has a smaller core, higher power density, lower primary coolant system (PCS) pressure and temperature (350 psig and 170°F), and greater ratio of coolant weight to power, than typical commercial pressurized water reactors (PWRs).

Designed to study the effects of intense irradiation on samples of reactor materials, the unique cloverleaf shape of ATR's 1.2-m high core provides positions for nine in-pile tubes (flux trap positions), and numerous smaller irradiation locations. The lobes of the cloverleaf core allow different power levels to be established at various lobe positions. Separate loop systems for each in-pile tube provide coolant at the experiment's designated temperature, pressure, and flow rate. A comparison of the ATR to a typical commercial PWR is presented in Table 1.

The top of the ATR reactor vessel is located at ground level, and two floors below house PCS pumps and heat exchangers, switchgear, loop systems, and other equipment. Framed with structural steel, the confinement structure above the reactor is designed as a barrier to radionuclide release into the atmosphere.

The ATR original design was to 1960 Uniform Building Code (UBC) Zone 2 provisions. But some supporting systems were built in the 1950's. Some of the structures and components were later evaluated for a safe shutdown earthquake (SSE) of 0.24g. It is planned that the ATR will remain in operation through the first decade of the next century, so an assessment of the additional risk posed by earthquakes is in order. The seismic accident sequence analysis performed for the ATR includes a unique fault tree based treatment of seismically induced fires and floods.

METHODOLOGY

In this seismic PRA, methodology suggested in Reference (1) was used to estimate the frequency of fuel damage at ATR. For the hazard analysis, ATR site specific hazard curves were not available. Therefore, The EBR-II site specific hazard curves were used[2]. The EBR-II is located at the INEL site approximately 25 km east of the ATR. Plant safety systems and operating procedures were reviewed to develop the seismically induced sequences that could result in fuel damage. The core fuel damage event tree for the seismic initiating event is based upon the loss of commercial power event tree modeled for the Level 1 PRA and includes explicit modeling of seismically induced loss of coolant accident (LOCAs)[3].

The system fault trees created for the Level 1 ATR PRA were modified using the guide lines provided in Reference 4. Then seismic failure modes were added for all major components and structures, e.g., pumps, tanks, block walls, etc. The fragility analysis included review of the plant design and seismic qualification information, plant walkdowns, and a seismic response analysis to obtain realistic floor response. Using the hazard curves, seismic fragilities and non-seismic unavailabilities, sequences were quantified to estimate the fuel damage frequency and its uncertainty.

SENSITIVITY ANALYSIS

An extensive sensitivity analysis was performed on selected low capacity components

[high-confidence-low-probability of failure (HCLPF) < 0.3 g]. Since seismic fragility of the components depend on level of earthquake, it is not possible to generate an importance list of components using conventional methods. Several components were selected from the low seismic capacity components (HCLPF < 0.3 g) for sensitivity analysis. More than 70% of the total core damage frequency due to earthquakes results from seismic failures of these components. From experience gained during the internal events analysis of the ATR PRA, these components were judged to be highly important. The contribution from the high seismic capacity components to the total seismic core fuel damage frequency is less than 1%; therefore, no sensitivity analysis was performed on these components.

The following ten sensitivity studies involving seventeen seismic basic events were performed in order to determine how changes in the probability values of certain seismic failure modes effect the results of the seismic analysis:

Case 1 Battery-backed Power

The event representing seismically induced failure of the battery charger and Utility uninteruptible power system (UPS) bus was set to a high fragility, i.e., the median capacity was assigned to 2.0 g. The sequences were requantified. No significant effects resulted on the total seismic core damage frequency.

Case 2 Bldg 609 480V Commercial-Diesel Power Buses

Loss of these buses results in the failure of both low pressure demineralized water pumps and the ATR instrument air compressors. The event representing seismically induced failure of these buses was assigned a high fragility i.e., median capacity was assigned to 2.0 g. The sequences were requantified. No significant effects resulted on the total seismic core damage frequency.

Case 3 Fire Water Injection System (FIS) Diesel Pump Daytanks

No significant effect was found on the total seismic core damage frequency when the seismic basic events representing failure of the fuel oil daytanks for the diesel firewater pumps were simultaneously removed from the core damage sequences by setting median capacity 2.0 g.

Case 4 FIS Diesel Pump Starting Batteries

The events representing seismically induced failure of the starting batteries for the diesel firewater pumps were simultaneously set to a high fragility, i.e., median capacity was assigned to 2.0 g. The sequences were requantified. No significant effects resulted on the total seismic core damage frequency.

Case 5 FIS Ground-level Tanks

No significant change in the total core fuel damage frequency was observed, when the basic event representing seismic failure of the ground-level firewater storage tanks was assigned a median capacity of 2.o g.

Case 6 Overhead Firewater Storage Tank

A high median capacity of 2 g was assigned to the event representing seismically induced failure of the overhead firewater storage tank. The sequences containing this basic

event dropped below 1.0E-7/yr. Thus, if the tank was made completely reliable (with respect to earthquakes), the risk from seismically initiated fuel damage would drop roughly 27%.

Case 7 Nitrogen Tanks in VVS

When two seismic basic events representing seismic failures of the nitrogen tanks for the reactor depressurization system were assigned median capacity of 2.o g, the total core fuel damage frequency was reduced by 21%.

Case 8 32 Vdc PPS Batteries

The event representing seismically induced failure of PPS batteries was set to high fragility, i.e., median capacity was assigned to 2.0 g. The sequences were requantified. No significant effects resulted on the total core damage frequency.

Case 9 Surge Tank

The event representing seismically induced failure of the surge tank was eliminated by assigning a high fragility, i.e., median capacity was assigned to 2.0 g. The sequences containing this basic event dropped below 1.0E-7/yr. Thus, if the surge tank was made completely reliable (with respect to earthquakes), the risk from seismically initiated fuel damage would drop roughly 46%.

Case 10 Seismic Events Initiated Fire and Flood

When these two events were removed individually, the total seismically induced fuel damage frequency decreased slightly more than 4.7% and 3.8%, respectively. Next, both seismically initiated fire and flood events were given their computed fragilities, while the probabilities for water propagation through the floor of the diesel pit events were set to zero. The estimated seismically induced fuel damage frequency decreased only 1.2%. Most of the contribution to the total seismically induced fuel damage frequency from diesel generator fires and floods is due to the failure of the backup diesel generator feeder cable and the loss of the PPS panels that support VVS actuation.

However, when groups of components were lumped together, a considerable reduction in the total seismic core damage frequency was observed.

Case 11

The components identified in the first four cases were assigned median fragility of 2.0 g for each. The total core damage frequency was reduced by less than 5%.

Case 12

In this case, the components identified in the first five cases were assigned median capacity of 2.0 g. The total core damage frequency reduced by 21%.

Case 13

When components identified in the Cases 7, 8 and 12 were lumped together and assigned median fragility of 2.0g to each component, the total seismic core damage frequency reduced by 48%.

Case 14

For this case, each component identified in the Case 9 and Case 13 were assigned the median fragility of 2.0 g. The total seismic core damage frequency reduced by 83%.

Case 15

In this case, each component identified in Cases 7 through 10 and Case 11 were assigned the median fragility of 2.0 g. The total seismic core damage frequency is reduced by 87%.

CONCLUSION

Recommendations based on the results of the seismic risk sensitivity study were made to management and accepted by management and the Department of Energy for the most cost-effective seismic upgrades. The recommended upgrades were those associated with sensitivity cases 2, 3, 4, 7, 8, and 9. In addition, upgrades associated with Cases 1 and 10 were already being planned and in engineering to relocate the Utility UPS and prevent flood propagation from the diesel pit in response to significant risk vulnerabilities associated with internal fire and flood sequences. Case 15, defined the seismic risk reduction associated with the combined effect of the recommended upgrades. All these upgrades have been completed except for the PPS batteries which are not a significant risk contributor and which will be replaced within a few years at their end of life.

The upgrade of the surge tank lateral support was the top priority upgrade. An earlier evaluation had concluded that collapse of the surge tank would only result in a small loss of coolant accident (LOCA). Re-evaluation associated with the PRA concluded that the consequence of a surge tank collapse was uncertain and that rupture of the surge line and a large LOCA could result. Therefore, the previously discounted seismic upgrade was now strongly recommended. The upgrade was cost-effective in that the total cost was less than $60,000 which did not require a capital expenditure and could be covered by the facility operating budget.

All the other recommended seismic upgrades were relatively cheap to accomplish since they required no significant material expense and only a small amount of engineering and maintenance labor hours. The total cost of the remaining recommended seismic upgrades is estimated to be less than $40,000. These upgrades do not include the Utility UPS and diesel pit upgrades which are considered separate from the seismic upgrades.

Seismic upgrade of the firewater system ground level tanks and overhead storage tank were estimated to require significant capital funding, probably $300,000 to $500,000. Since the more cost-effective recommended upgrades produce the desired significant reduction in seismic risk, these latter upgrades were not recommended at this time. However, an effective upgrade of the firewater ground level tanks may be accomplished as part of an overall fire safety upgrade program.

The seismic risk sensitivity study enabled the individual and combined affects of the dominant (low seismic capacity) components to be evaluated for the most risk-reduction effective and cost-effective seismic upgrades. As a result, a significant reduction in the estimated core damage frequency for seismic events, of 87%, was accomplished with an expenditure of less than $100,000. These actions helped to bring the total ATR PRA core damage frequency into an acceptable range comparable or less than that for other DOE and commercial power nuclear reactors. The application of the results of a PRA to define relatively low cost measures to significantly reduce the risk exposure to possible severe accidents is perhaps the greatest utility of a PRA.

ACKNOWLEDGEMENT

This work was supported by the U.S. Department of Energy, Assistant Secretary for Nuclear Energy, under DOE Idaho Field Office Contract No. DE-AC07-76ID01570.

REFERENCES

1. M.P. Bohn and J. A. Lambrihgt, *Recommended Procedures for the Simplified external Event Risk analyses for NUREG-1150*, NUREG/CR-4840, SAND88-3102, (1989).

2. Risk Engineering, Inc., Seismic Hazard Calculations for the EBR-II Reactor, Argonne National Laboratory (ANL)-Idaho, prepared for ANL, Argonne, Illinois, (1990).

3. S. T. Khericha et al., *Seismically Induced Accident Sequence Analysis of the Advanced Test Reactor,* Proceedings of the Third DOE Natural Phenomena Hazards Mitigation Conference, St. Louis, MO, (1991).

4. D. L. Moore, D. M. Jones, M. D. Quillici, and J. young, *Seismic Margin Review of the Maine Yankee Atomic Power Station: System Analysis*, NUREG/CR-4826, UCID-20948, Vol. 2, (1987).

Table 1. Comparison of ATR and PWR characteristics

Reactor Operating Conditions	ATR	PWR
Power MW(t)	250	2,000-4,000
Core power density (MW/l)	1	0.1
Operation pressure (psig)	355	2,250
Inlet temperature (°F)	125	550
Outlet temperature (°F)	170	600
Primary coolant flow rate (gpm)	<48,000	300,000
Primary coolant weight (lb)	600,000	450,000
Primary coolant weight/thermal power (lb/MW)	2,400	170
Decay Heat (MW at 10 s)	13	135
(MW at 1 d)	1.3	19
Fuel		
Total Uranium weight (lb)	89	180,000
Enrichment (% U-235)	93	2-4
Configuration	48 in. long Al plates attached to side plates	Zirc rods containing stacked pellets
Matrix	UAl_x	UO_2
Fuel temperature (°F)	430	2,000-3,000
Fission product inventory	60-d operation at 250 MW	10 times ATR

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)

HOW SHALL WE MEASURE THE RELIABILITY PERFORMANCE OF A SAFETY SYSTEM?

Per Hokstad

SINTEF Safety and Reliability
7034 Trondheim
Norway

1. INTRODUCTION

The paper treats reliability measures for safety systems. We discuss the definition of overall safety measures that are required to be consistent, intuitively appealing and reflect the essential features of the system.

As an example of a safety system (SS) we consider the shutdown system of an offshore oil/gas production platform. This system has the following main component groups:

- fire and gas detectors and other sensors (e.g. pressure switches)
- the logic (here computerized)
- actuating elements (e.g. valves that shut in by the occurrence of accidental events)

The safety evaluation of this SS can start by calculation of the *safety unavailability*, i.e. the probability that the safety system does not respond to a specific accidental event. The safety unavailability (*SU*) can be calculated for each component of the *signal path*, starting with the sensor(s) at the specified location, through the logic units and including all actuating elements to be activated by the occurrence of the specific event. This will provide the safety unavailability of the total SS related to the specific event.

This approach provides a safety quantification figure (i.e. *SU*) for each of the signal paths of the system. Several of these *SU* values can be different: Different voting can be applied to detectors at various location, and the specific set of valves to be shut in can also depend on the specific event. Further, the system will have detectors of various types (heat, flame, smoke, gas, pressure switch), and individual *SU*s will be calculated for each of these.

Thus, in total a rather confusing picture can emerge from this large number of *SU* figures. However, the question of managers and decision makers is *what is the safety of the installation?* Therefore the reliability analyst will be requested to provide a single measure of safety in order to quantify the overall level of protection provided by the SS.

The question arises: what are appropriate features of such a measure? For instance, should the size of the installation affect the result? One question of some controversy is the relative importance of the various component groups (detectors, logic and valves). In the standard single path calculation of safety unavailability, described above, all elements of the signal path are equally important. Thus, the detector, the logic and the valves are all given

the same importance. This conclusion is by many decision makers found counter intuitive, as they claim that the logic is the "heart" of the system, and therefore a safety measure should give higher weight to this than to detectors and actuators.

Requirements for reliability measures of SS are given, and several measures will be suggested and evaluated. A specific reliability measure for SSs will recommended.

This paper is based on experiences and result from the research programme *Reliability and availability of computer-based process safety systems - PDS*[3,4,5], carried out by SINTEF and sponsored by six oil companies and five vendors of safety systems.

2. REQUIREMENTS FOR RELIABILITY MEASURES OF A SAFETY SYSTEM

The objective of this paper is to discuss the desired features and requirements of quantitative measure for the reliability of a safety system. The reliability measure shall primarily be used in the early design phase in order to measure the *level of protection provided by the safety system*. Thus, the objective of using this measure is for instance to

- compare various design options, e.g. with respect to system architecture or component redundancy,
- come up with suggestions for cost effective improvements of the safety system.
- decide whether safety system requirements (acceptance criteria) are met,

The intention here is *not* to provide a measure for the total level of risk for the installation. Thus, a risk analysis of the installation, including a detailed consequence evaluation of accidental events, is definitely outside the scope of the analyses we have in mind. The evaluation of the performance of the safety system (SS) concentrate on loss of function of the system, i.e. unavailability of the system to shut in production on demand.

Based on the alleged use of the safety measure given above, we present the following requirements/requested features for reliability measures of a safety system:

***R.1*: *Interpretation*.** The measure shall be intuitively appealing and easy to interpret also for persons not being experts in reliability analysis.

***R.2*: *Criticality*.** The measure shall reflect the degree of protection provide by the SS against events that represent a *serious* hazard to the installation only. It is stressed that this implies that the measure shall reflect whether other means of protection are available by a SS failure. When it is *known* that the primary system is unavailable, alternative means of protection that can be put into action, and the unavailability of the SS is less critical. The measure shall account for this.

***R.3*: *Importance of various component categories*.** The measure shall depend on the various components and component groups in such a way that the importance of these is balanced in a consistent way. Thus, the component groups (as CPU or sensors) shall be weighted according to their actual importance for the SS performance. The actual importance of a component is essentially given by how much of the system (e.g. the number of sensor locations) that is made unavailable when the component fails. This requirement is further discussed in Section 4.1

***R.4*: *Overall installation measure*.** The measure shall be single (one dimensional), and shall predict the level of protection for the *total* activity/installation. In particular the measure shall aggregate the results for all *types* of safety scenarios, i.e. all types of accidental events, covering the various detection principles and various votings that are applied on the installation.

Observe that measures for safety only are considered in this paper, *not* measures for loss of production, i.e. trip failures. Measures of safety related to a specific accidental event are first discussed. Then measures for the overall installation are considered.

***R.5*: *Availability of input data*.** All input data required for calculating the measure must be easily available.

3. SAFETY UNAVAILABILITY

Measures for loss of safety often refer to a specific scenario, initiated by a accidental event. A basic measure is the

Safety Unavailability (SU): The probability that a component (or SS) is not not able to carry out its intended action by the occurrence of a specific hazardous/accidental event.

3.1 Critical and noncritical safety unavailability

The SS is said to be unavailable if one or more failures are present, that will prevent the intended action (automatic shutdown) when demanded. Further, part of the SS will be unavailable when it is bypassed due to testing or repair work. However, in this case it will be *known* that the SS is unavailable. This situation will not necessarily represent a serious hazard, but rather requires some additional precautions, e.g. locating personnel in field to detect gas leaks and activate shutdown actions manually. Thus, the *SU* is split into

Critical Safety Unavailability (CSU): The probability that the component (or SS) has an *unknown* (dormant) failure, preventing the system to react by an accidental event.

Noncritical Safety Unavailability (NSU): The probability that production is going on and it is *known* that the safety system is unavailable, e.g. bypassed due to repair or testing.

Observe that $SU = CSU + NSU$. The CSU is a fundamental parameter often denoted the *Mean Fractional Deadtime*[1,2]. It is determined from component failure rates and length of the test period[1,2]. More advanced models are also developed[3,4,5,6].

3.2 The CSU of a simple example system

As an introduction to the discussion, consider the following part of a SS (Figure 1) with

- 12 identical sensors (S_1, S_2, ... , S_{12}), in different areas/locations
- 2 identical input cards (I_1, I_2), each receiving signals from 6 sensors
- 1 Central Processing Unit (CPU), handling sensors signals and initiating proper action.

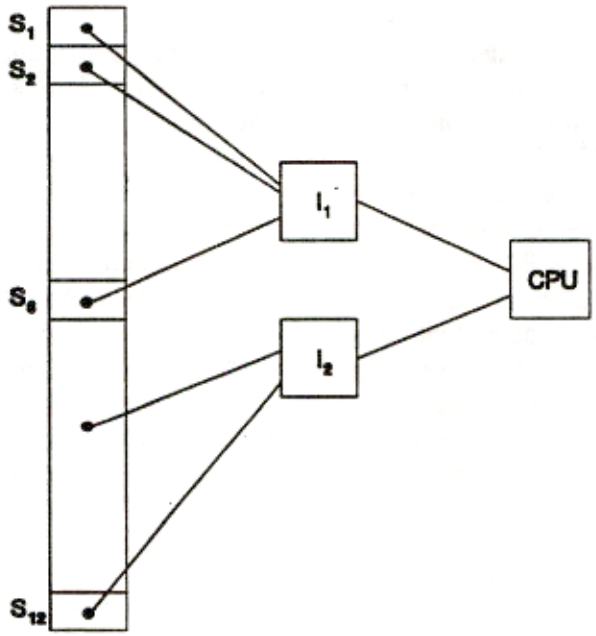


Figure 1 Example configuration with 12 sensor locations

Output cards and shut down valves are ignored here, and redundancy is not considered. Thus, we have a simplified SS, consisting of 15 components. Observe that failure of a sensor, S_i, cause *one* location to be unavailable. The CPU will by failure cause all twelve areas to be unavailable, while failure of I_1 and I_2 affects six locations.

Let *CSU(S)* be the critical safety unavailability for a sensor, and let *CSU(I)* and *CSU(CPU)* be defined similarly. When these are small the *CSU of the SS* is approximately

$$CSU = CSU(S) + CSU(I) + CSU(CPU) \quad (1)$$

This expression illustrates that all components of the signal path: sensor, input card, CPU, (and actually also output card, actuator) must function for the total SS to function.

4. MEASURES FOR LOSS OF SAFETY

A few measures are now evaluated with respect to the requirements of Section 2. First we review some measures related to *one* type of accidental events only (say gas leaks).

4.1 Evaluation of CSU

Now consider whether the measure $M_1 = CSU$, given in (1), meet the requirements.

R.1 Interpretation. The interpretation of $M_1 = CSU$ is rather straightforward. For instance $CSU = 0.02$ means that the system fails to perform its intended action in 1 out of 50 demands. So *CSU* is the average fraction of demands, not resulting in an automatic shutdown.

R.2 Criticality. According to this requirement *CSU*, and *not SU*, should be used as a measure for loss of safety, see Section 3.1. Thus, R.2 provides no objection to the use of *CSU* as a safety measure.

R.3 Importance of various component categories. As commented after equation (1), all component types of the signal path must function, and therefore we should conclude that they are all equally important. However, is it not the case that the CPU is much more important than a sensor? This are by decisions makers often considered to be a paradox. Our conclusion is as follows:

- The CPU is demanded by *every* accidental event, and is from a safety point of view without comparison more important than a *specific* sensor or an input card.
- All of the *component types* are equally important. This means that if we either reduce the *CSU(CPU) or* the *CSU(S)* of *all* 12 sensors with the same value it will have the same effect on the SS safety.

It is seen that the measure M_1 are in agreement with both these statements. Further, it follows that R.3 can be made more specific: A reliability measure should give the same weight on all *component groups* of the signal path. As a consequence it will give highest weight to the component belonging to the group with the smallest number of components. Actually, it can be argued that the weight on the CPU should be even higher than follows from this rule, as the sensors at various locations provide some redundancy for each other.

R.4 Overall installation measure. Evaluation of requirement R.4 leads to the following objection to the use of $M_1 = CSU$ as a measure for system loss of safety:

- Using *CSU*, it is required to give separate measures for loss of safety, related to each type of accidental event (gas leaks, fires). Thus, *CSU* will give no overall figure for the loss of safety, and requirement R.4 is not met by *CSU*.

We observe that *CSU* does not take the size of the installation (no. of locations) into consideration; the *CSU* of a large installation will be identical to the *CSU* of a small one.

R.5 Availability of input data. The CSU requires a minimum of input data. The component failure rates must be estimated and the length of the test period must be given.

4.2 Alternative measures for one type of accidental events

Two alternative measures for loss of safety (M_2, M_3) are now evaluated.

M_2: Mean Number of accidental events Between Failures (MNBF). The *MNBF* equals the inverse of the *CSU*, i.e. $MNBF = 1/CSU$. Having $MNBF = 50$ means that in one out of *50* accidental events the SS fails to carry out the intended action. This measure has essentially the same features as *CSU*, and it could be a matter of taste whether *CSU* or *MNBF* are used. However, *MNBF* may have a slight advantage as interpretation is concerned (see R.1). On the other hand, as seen from (1), quantifying the contributions of the various component groups is more straightforward using the *CSU* measure (see R.3).

The next measures account for the size of the installation, i.e. no. of locations/measure points. Consider an installation with N locations (in the previous example we had $N=12$).

M_3: Average number of unavailable measure points of SS. The mean number of locations where the SS would fail to operate by an accidental event equals $M_3 = N \cdot CSU$. Thus, M_3 equals the average number of measure points "not covered" with respect to this type of accidental events.

Obviously *CSU* and M_3 give very much the same information. Actually, M_3 has the same features as CSU, except that M_3 is proportional to the size of the installation, demonstrating that a larger installation should pose a bigger threat to safety than a small one, due to a higher level of activity (see R.4). However, it is typically irrelevant whether we quantify loss of safety *per measure point* or *per installation*, and both measures *CSU* and M_3 can be applied. An interesting question is whether acceptance criteria of a SS should be based on total installation safety or safety per location. We prefer the last option, accepting higher risk level for a higher level of activity. This is in favour of *CSU*.

4.3 Overall measures for loss of safety

Finally consider two overall measures meeting the objection raised to CSU in Section 4.1, i.e. the measure should comprise all locations and all types of accidental events.

M_4: Probability that at least one failure is present in SS. Assuming no redundancy, the SS will fail to respond properly on demand in at least one of the locations unless the installation is completely free of errors. This measure is for some decision makers intuitively very appealing, and should be given a serious consideration.

Referring to the example of Section 3.2, the probability of at least one failure being present equals the sum of all the *15 CSU* of Figure 1. This gives

$$M_4 = 12 \cdot CSU(S) + 2 \cdot CSU(I) + CSU(CPU).$$

Thus, choosing this measure, the sensors would get a much higher influence than in $M_1=CSU$, and all *15 components* are given the same weight. According to the discussion in Section 4.1, where requirement R.3 is detailed, we conclude that M_4 is *not* a good measure for safety. It does not take into consideration the *number* of measure points made unavailable by a failure. A sensor failure making one location unavailable, is given the same weight as a CPU failure that makes all locations unavailable.

Introducing the next measure, let the safety of the SS be defined by a series of scenarios related to various accidental events. Scenario no. i ($i=1, 2, \ldots K$) has critical safety unavailability CSU_i. Further, w_i is a weighting factor for scenario i (summing to *1*).

M_5: Weighted average of scenario CSUs. Based on the *CSU* of K scenarios let

$$M_5 = w_1 \cdot CSU_1 + w_2 \cdot CSU_2 + \ldots + w_K \cdot CSU_K \quad (\Sigma_i w_i = 1)$$

Now evaluate M_5 with respect to the requirements of Section 2. The interpretation of M_5 is not quite as simple as that of M_1 (see R.1) and will depend on how the w_i are chosen. If the weights reflect the frequency of the various scenarios, M_5 is simply the probability of a SS failure by a "random" demand. In general the interpretation poses no serious objection to

the use of M_5 as a safety measure. Also requirement R.2 is satisfied for M_5.

In order to discuss the implications of requirement R.3, now consider a simple extension of the example presented in Section 3.2. Let there be both a gas (G) detector and a heat (H) detector at each of the $N=12$ locations, and consider $K=2$ scenarios, related to gas leak and fire respectively. The relative contributions of the various component types to the measure, M_5 will then be given by (note $w_1+w_2=1$)

$$M_5 = w_1 \cdot CSU(G) + w_2 \cdot CSU(H) + CSU(I) + CSU(CPU)$$

It follows that the contribution from the *CPU* is higher than that of a specific sensor type (gas *or* heat). Actually, the contribution to loss of safety from the *CPU* equals that of *all* the sensors (gas *and* heat). Generally R.4 should be specified so that this a required feature.

R.4 was the reason for introducing M_5, and this measure obviously meets this requirement. The main objection to this M_5 is that reliable estimates of the w_i are often unavailable (see R.5). The w_i should be based on the frequencies and/or consequences of the various accidental events/scenarios. If this information is lacking or difficult to quantify we suggest the following approach for choosing the weight factors, w_i. Classify each scenario into one of say 7 criticality classes, following for instance a TÜV or DIN 19250[7] classification scheme. Class 1 corresponds to minor damage and class 7 to major accident/high frequency. Then choose the weight factors as given below and normalize.

Critic. class	1	2	3	4	5	6	7
Weight, w	0.05	0.05	0.10	0.10	0.15	0.25	0.30

5. CONCLUSIONS

Our recommendation is to apply the measure M_5. When information for identifying weight factors is lacking, these should be obtained by the rough approach indicated above.

There is one objection that could be raised also to this measure. As mentioned in Section 4.1, the *CSU* could be given even a higher weight than is done in the recommended measures, since sensors in adjacent areas provide some redundancy for each other. Similarly, referring to the example in 3.2, observe that for instance M_5 does not discriminate between the following two failure events:

- all 12 areas being "uncovered" for one day, e.g. CPU being unavailable 1 day
- one area "uncovered" in 12 days, e.g. one sensors being unavailable 12 days.

Again it might be argued that the first event is more serious.

6. REFERENCES

1. T. Aven. "Reliability and Risk Analysis" Elsevier Applied Science (1992).
2. A. Høyland and M. Rausand. "Reliability Theory, Models and Statistical Methods," John Wiley & sons, (1993).
3. R. Aarø et al, Reliability Prediction Handbook. Computer-Based Process Safety Systems. *SINTEF report STF75 A89023* (1989).
4. L. Bodsberg and P. Hokstad, Balancing reliability requirements for field devices and control logic components in safety systems. *Internat. Conf. on Safety, Security and Reliability of Computer-based Systems (SAFECOMP 91)*, Trondheim, 1991.
5. L. Bodsberg, Failure rate prediction for computer-based process safety system. In "Safety and Reliability '92", ed. K.E. Petersen and B. Rasmussen, Elsevier, London (1992).
6. L. Bodsberg, Comparative study of quantitative models for hardware, software and human reliability assessment. To appear in *Quality and Reliability Engineering International*.
7. DIN 19250. Messen-Steuern Regeln: Grundlegende Sicherheitsbetractungen für MSR-Schuttzeinrichtungen.

THE USE OF RISK CONTOURS TO CLARIFY RISK COMMUNICATION

T. Edward Fenstermacher,[1] Jerry T. Kopecek[2]

[1]PLG, Inc.
Suite 730
1615 M Street, NW
Washington, D. C. 20036
[2]Union Oil Company of California, d.b.a. UNOCAL
UNOCAL Refining and Marketing Division-Wilmington
1660 West Anaheim Street, P. O. Box 758
Wilmington, CA 90744

INTRODUCTION

No matter how well analysts perform risk assessments, the impact and information content may be lost if the results are not communicated effectively to the people who need to use the information. A considerable range of people may use the results of the risk assessment; these include other risk analysts, local authorities who may or may not understand risk analysis, and members of the local community who may be exposed to the risk. One way to communicate the risk in a meaningful way to this wide range of people is by using risk contours. In this paper we will discuss risk contours; what they are, how to determine them, and how to use them to clarify risk communication.

The consequences of an accident are not a simple scalar quantity, but include a wide range of different effects, and different levels of these effects, at different locations. While in this paper we will focus on just one type of event, a toxic release from a chemical plant, and one type of consequence, the exceedence of the second Emergency Response Planning Guideline[1] (ERPG-2) level, the concepts presented here can be easily extended to other types of plants and consequences.

RISK CONTOURS

As mentioned above, the risk of a particular type (e.g., exceedence of the ERPG-2 level), either from a single scenario or from a group of scenarios, is a function of the location of the receptor relative to the plant. The two primary things that affect the risk are the distance of a particular receptor from the plant and the direction from the plant to the

[1]Emergency Response Planning Guidelines, American Industrial Hygiene Association, May, 1992.

receptor. For most, but not all, types of releases, the consequences decrease with increasing distance from the plant. They also vary with the frequency with which the wind blows in a given direction, and with other meteorological parameters: wind speed, atmospheric stability, and temperature. If we can use dispersion and meteorological information to determine the frequency with which a given consequence level will occur at various locations around the plant, we can then draw isopleths of equal frequency on a map of the plant site. These are risk contours.

Determining Risk Contours

The first step in the construction of risk contours is to determine the size and shape of the area where the limiting condition, in this case ERPG-2, is exceeded. The plume exceedence area for a release consisting of a 0.25 inch valve break on a one-ton chlorine tank is shown in Figure 1. These areas are determined for a variety of wind speeds and atmospheric stability combinations. (The ambient air temperature can also be varied if it will affect dispersion.) For dense gas releases, the areas are found using the QCRR (Quantification of Consequences of Chemical Releases) computer program, which models the release, evaporation and dispersion of heavier-than-air and neutral buoyancy vapors and aerosols. QCRR output includes the chemical concentrations resulting from an assumed release as a function of time and position. The output from the QCRR runs is processed using the FUTPRINT computer program. FUTPRINT (for FooTPRINT, the approximate shape of contours of constant concentration from a continuous plume) computes the ratio of the maximum 10-minute (or other time period) average concentration to the specified concentration limit as a function of the distance downwind from the release point and the distance from the centerline of the plume. A simpler program, ELREL (for ELevated RELease), is used in place of QCRR and FUTPRINT for buoyant or elevated neutral releases. ELREL uses a Gaussian plume dispersion model, taking buoyancy (and optionally momentum) driven plume rise into account while determining the ground concentrations of the chemicals released.

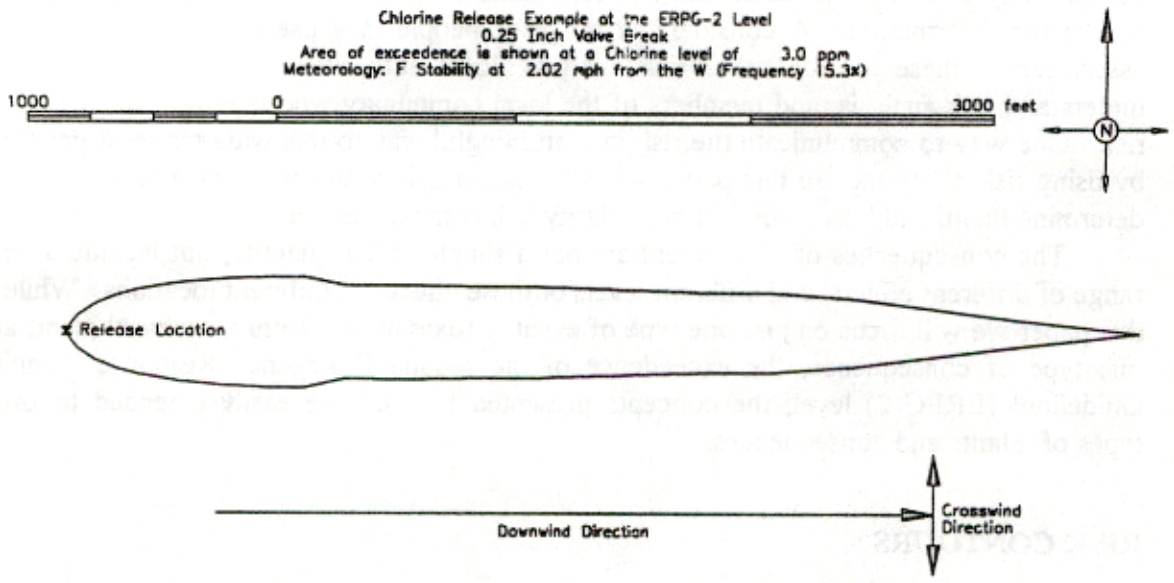


Figure 1. Plume exceedence area for the sample release at F Stability and a wind speed of 0.9 m/s at the ERPG-2 level.

In program RCONTOUR (for Risk CONTOUR), the frequencies of various combinations of wind speed, atmospheric stability, wind direction and temperature, if it is varied, are read from a joint frequency table. Rules are set up to determine the treatment of meteorological categories which have no corresponding dispersion results, with the objective of making sure that the treatment is conservative. Such a rule might be to use the next lower wind speed group or to use B Stability in place of A Stability for a missing run. This process results in an array of 16 frequencies for each dispersion case, corresponding to the 16 directions in the joint frequency distribution. For each dispersion case l, the angular half-width of the plume at the concentration limit is determined for each distance in the original run. These values are used to interpolate values for the angular half-width of the plume, $\alpha_l(r)$, at each distance on the grid used for the contours. Let a point where the frequency will be determined be located at distance r and angle θ from the North. Also, let the frequency of the wind for dispersion case l and sector k be given by f_k. The frequency density of wind in direction ϕ for dispersion case l is then:

$$F_l(\phi) = \frac{8 f_k}{\pi} \quad , \quad \frac{(k-1)\pi}{8} \le \phi < \frac{k\pi}{8} \quad . \tag{1}$$

The frequency with which dispersion case l contributes to exceedences at (r, θ) is

$$p_l(r, \theta) = \int_{\theta - \alpha_l(r)}^{\theta + \alpha_l(r)} F_l(\phi)\, d\phi \quad . \tag{2}$$

The total frequency of exceedance of the concentration limit is thus

$$P(r, \theta) = \sum_l p_l(r, \theta) \quad . \tag{3}$$

After this procedure has been followed for each run, a mathematical map exists of the risk of exceeding the concentration limit given that the release occurs. These are known as conditional frequencies. The final step is to multiply these conditional frequencies, tabulated for each release scenario, by the corresponding frequencies, and add them together. This produces a corresponding mathematical map of the risk from all of the releases taken together. A map is now drawn by computing the contours of equal frequency on that mathematical map. A sample of such a map, using the chlorine release cited earlier and meteorology typical of Southern California, is shown in Figure 2.

Shape of the Risk Contours

We expect that the risk contours will have irregular shapes. If the wind blew with the same frequency in all directions, we know that the contours would all be circles. Since it doesn't, we expect that contours will go out further in the directions where the wind blows most frequently. This is true for the highest frequency contours. A contour that is within a factor of one hundred of the total accident frequency is likely to be highly directional. On the other hand, low frequency contours tend to represent the worst that can happen. Thus, if the worst case combination of wind speed, stability, and temperature ever occurs in a given direction, the low frequency contours will show this by tending to be circular. Thus, for a given release or set of releases, the lower the frequency of the contour, the closer to circular it will tend to be.

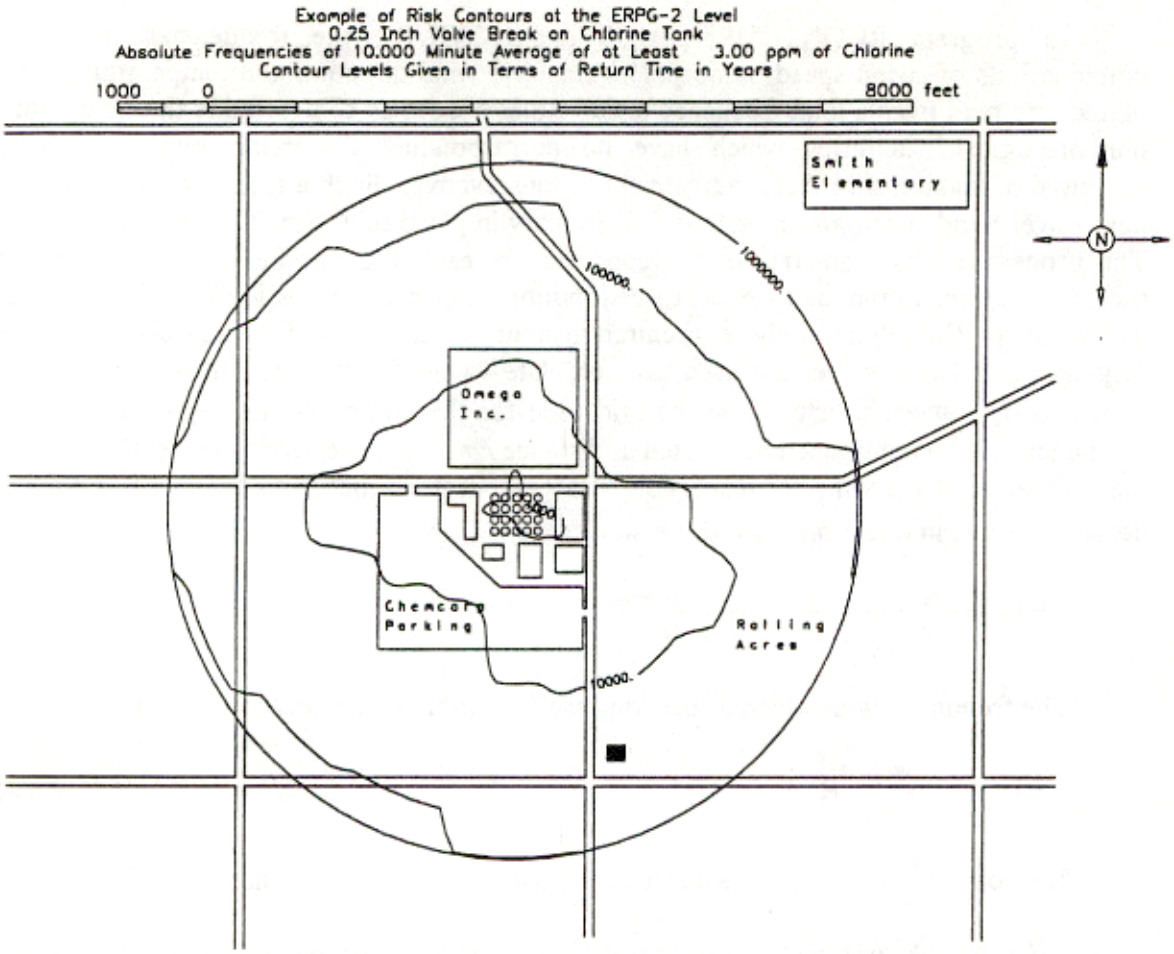


Figure 2. Risk contours for the chlorine tank line break reference case, using meteorology typical of Southern California. The plant site and surroundings shown are hypothetical.

Another phenomenon occurs with some risk curves that at first appears impossible. This is for a contour to appear separate from the main contour surrounding the source. This occurs due to the fast spreading of the plume in the crosswind direction, usually due to gravitational spreading of dense gas releases. Thus, a region further away from the origin may have a higher probability of being exposed to the limiting concentration than a closer region in the same direction. The closer region will exceed the limit by a greater factor but that will not show up on the risk contour plot (except at a higher concentration limit).

RISK COMMUNICATION USING RISK CONTOURS

Risk contours provide a useful way to look at the risk from a plant or operation. When planning the layout of a new plant, a set of risk contour maps allows the responsible engineers to determine a layout which minimizes the risk impact of the plant. When a change in the plant operations is planned, risk contours can show the change in the risk, whether positive or negative, in the vicinity of the plant. For an existing plant, they give a picture of the total risk from the plant, both within and outside the plant boundary.

For local officials, the risk contours show the impact of the plant on the total risk of accidents in their community. When the plant manager needs to deal with local officials on licensing matters, a risk contour map of the site can be compared with other known risks the community already faces from other facilities. It can also be a useful tool for helping local fire departments or hazmat teams with emergency planning.

For an individual living in the vicinity of the plant, examining a risk contour map could show that, for instance, the concentration limit would be exceeded about once in 3000 years at his workplace on site but only once in 30,000 years at his house near the site, while at his children's school, the concentration limit would never be exceeded. Thus, such a map gives people living or working near the plant which a better understanding of the impact of that plant on themselves and their families.

When presenting risk contour information to non-technical audiences, it is important to present the contour levels in terms meaningful to the audience. A risk level of 10^{-4} at an individual's home may be better presented as "once in ten thousand years" or even as "one chance in two hundred if you live there 50 years."

CONCLUSION

Risk contours are a graphical tool for presenting the results of a risk analysis. They are produced by combining the results of the risk analysis, including the consequence analysis, with historical data on the local meteorology. The resulting risk contour map shows the distribution of risk both at the plant site and in the surrounding area.

Risk contour maps can be used to present information to engineers, local licensing and emergency planning officials, and members of the general public who are concerned about the plant. Care must be taken assure that the target audience is familiar with the terms that are used to describe the risk contour levels.

IMPROVING NRC STAFF USES OF RISK ASSESSMENT

M. Cunningham, P. Baranowsky, W. Beckner, and P. Rathbun

United States Nuclear Regulatory Commission
Washington, DC 20555

INTRODUCTION

Probabilistic risk assessment (PRA) and risk management are used by the NRC staff as important elements of its licensing and regulatory processes. The NRC's first PRA, the Reactor Safety Study,[1] was completed soon after the creation of the agency in 1975. Since that time, the NRC has made use of risk assessment to address complex safety issues. A particular strength of risk assessment which has made it valuable to NRC is the structure it brings to an analysis of an issue. That is, PRA provides a logical and structured approach for issue analysis, with the capacity to provide estimates of the relative and absolute safety significance of issues as well the benefits and detriments of plant design or operational changes under consideration to deal with an issue. Another important strength of risk assessment is its capacity to quantitatively estimate the uncertainties associated with a safety issue and possible changes to plant design or operation to address the issue. This is particularly germane to many of the safety issues facing the staff, which often are related to rare combinations of facility system failures, poorly understood accident processes, and other uncertain factors.

The strengths of risk assessment have led to its use in a spectrum of NRC staff licensing and regulatory functions, including, for example:

- The licensing of advanced reactor designs, where the design is reviewed with respect to the balance of prevention versus mitigation capabilities for core damage accidents;
- The licensing of high level waste repositories, for which probabilistic acceptance criteria have been established in terms of public health risk;
- The monitoring of licensed reactor facilities, where operational events are routinely evaluated for their risk significance;
- The analysis of benefits, in terms of risk reduction, of certain possible improvements in licensed reactors, for which a probabilistic criterion has been established in terms of public health risk; and
- The allocation of staff resources in such areas as inspections and safety issue analyses.

Related to these uses of risk assessment are certain fundamental risk management policies. These include:

- A policy statement characterizing the acceptable risks from accidents in licensed reactors ("safety goals");[2]
- A rule establishing the process and decision criteria for value-impact analyses for certain potential changes in licensed reactor design and operations (the "backfit" rule);[3] and
- An EPA rule establishing the acceptance criteria for high level waste repositories.[4]

In a July 1991 letter,[5] the NRC's Advisory Committee on Reactor Safeguards (ACRS) identified a number of problems with the staff's risk assessment work. The letter identified concerns related to unevenness and inconsistency in the staff's uses of PRA, provided a number of examples illustrating their concerns, and included some recommendations as to how to address the identified concerns.

In response to the ACRS letter, the NRC's Executive Director for Operations formed a working group of staff management (the "PRA Working Group") to:

> Consider what improvements in methods and data analysis are possible and needed, the role of uncertainty analysis in different staff uses of PRA, if improvements are needed in the allocation of existing PRA staff, and the need for recruitment of more staff (or for identifying other means for supplementing staff resources).[6]

This paper summarizes the activities and results of the PRA Working Group to address the issues raised by the ACRS. In response, the Working Group developed two general recommendations, defined a set of basic principles for staff PRA use, and identified three areas for improvements. For each area of improvement, the Working Group took certain actions and made recommendations for additional work.

GENERAL RECOMMENDATIONS

The Working Group developed two general recommendations with respect to the agency's uses of PRA:

- Development of a integrated plan on staff's risk assessment and risk management practices. The Working Group's objectives and scope have been directed towards the resolution of the specific issues raised by the ACRS in their July 1991 letter. There are additional issues related to the staff's uses of PRA, some of which have been addressed by the Regulatory Analysis Steering Group,[7] the Regulatory Review Group,[8] and others. The Working Group recommends that all staff activities related to PRA uses be described in a single document which defines the present structure of the agency's risk assessment and risk management practices, summarizes the key elements of the staff's work, and lays out plans for improving and expanding PRA uses within the agency. When completed, it may be appropriate to summarize the basic principles contained in the document in a Commission policy statement.
- Improving interactions with industry PRA users. The nuclear industry has developed considerable capabilities in risk assessment and risk management. The Working Group recommends that mechanisms be found to improve interactions between industry PRA users and those in the staff.

BASIC PRINCIPLES

The Working Group identified a number of basic principles for PRA work to help ensure consistent staff use, including:

- Staff applying PRA methods should have training and experience commensurate with the particular use of PRA being undertaken.
- Methods should be used which:
  - Reflect the current PRA state of technology, plant design and operational features, and data; and
  - Reflect the intended use, both in terms of the appropriate level of detail and the associated decision criteria.
- Guidance to the staff should explicitly identify decision criteria for the particular use.
- Documentation of analyses should use proper PRA terminology, identify key uncertainties and sensitivities and their significance, and be sufficiently complete and scrutable to permit a quality assurance review.
- Quality assurance by knowledgeable staff should be performed, with the extent of review commensurate with the intended use.

AREAS FOR IMPROVEMENT

To support the implementation of these principles, the Working Group also identified three general areas of needed improvements in present staff PRA capabilities:

- Guidance on technical matters such as the need for and performance of uncertainty analyses, procedural matters such as documentation and quality assurance requirements, and decision criteria.
- Training related to both PRA techniques and the design and operation of licensed facilities.
- PRA methods and data bases to support staff PRA uses.

The Group's efforts and recommendations in each of these areas are discussed below.

Guidance Development

The Working Group developed general guidance for two PRA uses:

- The screening and prioritizing of issues and events, performed in NRR, RES, and AEOD; and
- The analysis of the more significant of these issues and events, also performed in NRR, RES, and AEOD, as part of backfit analyses, etc.

The Working Group focused on these two PRA uses because they were widespread in the agency and were found to have essentially no formal PRA-related guidance. The Group has developed initial general guidance for these uses and, as examples, more specific guidance for generic issue prioritizations and detailed analyses performed in RES.

The Working Group has also made recommendations with respect to additional use-oriented guidance development. The more significant of these are:

- Complete development of more specific guidance for other PRA uses related to screening and detailed analyses (e.g., AEOD's studies of operational events), based on the general guidance provided.

- Complete the development of guidance for PRA use in plant-specific reactor licensing actions (e.g., technical specification modifications), including how Individual Plant Examination (IPE)[9] results should be used.
- Develop guidance on how IPE results should be used to improve the ongoing PRA-based focusing of inspection activities.
- Develop guidance on the review of advanced reactor design PRA submittals, as part of revision to NRC's Standard Review Plan.[10]

Training Enhancements

The Working Group took two principal actions with respect to agency PRA training and skills:

- Guidance has been developed by the Group on basic terms and methods in technical areas important to appropriate uses of PRA by the staff. This guidance provides: definitions of terms used in PRA and related skills, with the goal of agency-wide adoption of these definitions; descriptions of methods commonly applied in the agency's business, including discussions of the strengths and limitations of each; and references for obtaining more detailed information.
- The Group initiated a systematic review of tasks needed to accomplish generic issue screening and analysis and the PRA-related guidance and skills needed to accomplish these tasks. This review uses job and task analysis technique (a portion of the Systems Approach to Training method). This technique provides an assessment of the PRA-related guidance and skills needed to accomplish these specific PRA uses as well as learning objectives which can be used to define training needs.

The Working Group has also made recommendations with respect to staff training and skills. The more significant of these are:

- A job and task analysis technique similar to that noted above should be applied to other major PRA uses within NRC. The PRA training program should be updated as these applications are completed.
- As the PRA training curriculum is developed, it should be closely coordinated with the agency's training in the design and operations of regulated facilities. The latter training, generally provided at the NRC's Technical Training Center, is an important element to successful use of PRA methods. The job and task analysis technique applications noted above should also explicitly identify facility/device design and operation learning objectives, which should then be compared with the present TTC curriculum, and, as needed, changes made to that curriculum as well.
- The PRA training curriculum should define a minimum set of courses, rotational assignments for on-the-job training (within NRC or with NRC contractors), etc. needed to adequately use PRA in specific staff activities.
- The Group was well aware that present staff recruitment opportunities are very limited. Within these limits, improvement of staff PRA capabilities would particularly benefit from recruitment of people with extensive experience in systems reliability (PRA Level 1) analysis or statistics.

PRA Methods Development

The Working Group initiated one effort with respect to agency PRA methods:

- The Working Group's survey found that most reactor event and issue analyses performed by the staff relate to Level 1 PRA information (e.g., failures of

components or systems resulting in core damage). However, the agency's risk-related decision criteria are often in terms of Level 3 products (e.g., regulatory analyses using risk information in terms of averted population dose).

In one case (generic issue prioritization) a simple transformation is now used for converting Level 1 to Level 3 results. However, this transformation is based on results of the Reactor Safety Study (completed in 1975). The Working Group concluded that this present core damage frequency-to-risk transformation should be replaced with information based on the NUREG-1150 study[11] (completed in 1990). The Working Group has initiated an effort to provide results from that study in forms appropriate for such transformations.

The Working Group also made a number of recommendations with respect to additional methods development and related data collection and analysis. The more significant of these are:

- The Group's survey results indicated that most PRA uses by the staff were adaptations of existing PRAs, rather than new studies. To support such uses, the Group recommends:
  - The continuation of PC-based code development (i.e., IRRAS[12] and SARA[13]) with a focus on using such codes to adapt PRA models; and
  - The continuation of efforts to put a representative set of modern PRA models (including, to the extent possible, IPEs) in a form usable with the PC-based codes.
  - The development of guidance on how to adapt PRAs for use in staff studies such as regulatory analyses. While guidance documents exist for developing PRA models, there is at present no guidance document for adapting PRA models.
- The feasibility of developing a structured classification of licensed reactors for use throughout the agency should be investigated. Both the issue screening and issue analysis uses of PRA in NRR, AEOD, and RES could benefit from such a classification scheme (structured, for example, by design type and containment design), with modern PRAs/IPEs identified to represent each class. This feasibility study should consider the present categorization scheme used for accident sequence precursor analyses for broader use throughout the agency.
- The feasibility of developing detailed PRA models for use in issue analyses which can also be "rolled-up" to more simple models for use in screening analyses should be investigated. If feasible, such models should be developed for a representative set of plants using the classification structure described above.
- The feasibility of developing accident sequence analysis models which can be more readily updated to account for plant design and operational changes and new component or system failure data should be investigated.
- The collection and analysis of reliability data, for both equipment and human performance, for use with these improved PRA models should be expanded. Such data should be updated on a periodic basis to reflect industry-wide and plant-specific performance.

FUTURE WORK

As noted above, several NRC staff groups have recently been dealing with issues related to the staff's uses of risk assessment, including the Regulatory Anaysis Steering Group and the Regulatory Review Group. Some recommendations of the Working

Group, such as guidance development for issue prioritizations and analyses, are presently being implemented. However, the larger set of recommendations requires integration with the work of these other staff groups. At present (October 1993), the mechanism for achieving this integration is under senior management review.

REFERENCES

1. United States Nuclear Regulatory Commision (USNRC), "Reactor Safety Study- An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400 (NUREG-75/014), October 1975.

2. USNRC, "Policy Statement on Safety Goals for the Operation of Nuclear Power Plants," Federal Register. Vol. 51, p. 28044, August 4, 1986.

3. USNRC, "Revision of Backfitting Process for Power Reactors," Federal Register, Vol. 53, p. 20603, June 6, 1988.

4. United States Code of Federal Regulations, Title 40, Part 190.

5. Letter from David A. Ward, Chairman, Advisory Committee on Reactor Safeguards, to Ivan Selin, Chairman, NRC, "The Consistent Use of Probabilistic Risk Assessment," July 19, 1991.

6. Letter from James M. Taylor, Executive Director for Operations, NRC, to David A. Ward, Chairman, ACRS, October 1, 1991.

7. USNRC, "Regulatory Analysis Guidelines of the U. S. Nuclear Regulatory Commission," Draft Report for Comment, NUREG/BR-0058, Rev. 2, August 1993.

8. USNRC, "Regulatory Review Group," August 1993.

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

10. USNRC, "Standard Review Plan," NUREG-0800, 3rd Edition, July 1981.

11. USNRC, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, Volumes 1 and 2, December 1990.

12. K.D. Russell et al., "Integrated Reliability and Risk Analysis System (IRRAS) Version 4.0 Reference Manual," NUREG/CR-5813, Vol. 1, January 1992.

13. K.D. Russell et al., "System Analysis and Risk Assessment (SARA) System Version 4.0 Reference Manual, NUREG/CR-5303, Vol. 1, February 1992.

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

M. Kajimoto, K. Muramatsu, N. Watanabe (JAERI)

Source Term Analysis for High Level Waste Storage Accidents

S. Medhekar, J. Kindinger (PLG); D. MacFarlane (LANL)

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

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH
D-85748 Garching, FRG, *D-50667 Köln, FRG
Telephone (089) 32004 - 373
Telefax (089) 32004 - 301

ABSTRACT

An application of the multi-compartment containment code FIPLOC-M(AEROS) to the dry part of the VANAM-M2 containment aerosol experiment is considered. The 640 m³ experimental containment is respresented by 11 control volumes (zones), 12 flow paths (junctions), 49 heat slabs and two flow paths to the environment. Steam, air and aerosols are injected and the corresponding time histories of the local aerosol concentrations, mass flows, pressures, temperatures etc. are computed.

For the purpose of uncertainty and sensitivity analysis a total of 179 uncertain parameters were identified. The state of knowledge on parameter level was expressed by subjective probability distributions and by correlations between selected parameters. 100 FIPLOC-M runs were performed with randomly selected parameter values as input. From the resulting 100 time histories of selected output quantities (1) uncertainty statements in form of statistical (90 %, 90 %)-tolerance intervals and (2) sensitivity measures from stepwise regression analysis were obtained for two selected points of time.

The results confirmed the expected high ranking of the main contributors to uncertainty from aerosol modeling and revealed the importance of uncertainties in thermal- and fluiddynamics for the computed aerosol behaviour.

INTRODUCTION

The mechanistic computer code FIPLOC-M /1/ has been developed at GRS for the integrated analysis of thermal hydraulics and aerosol behaviour in multi-compartment geometries. The main purpose of FIPLOC-M is to calculate the distribution and retention of airborne fission products in a LWR-containment during a severe accident and to predict the radioactive source term to the environment.

FIPLOC-M (Fission Product Localisation - MAEROS) uses the lumped parameter technique. The containment is represented by a number of control volumes which are

interconnected by atmospheric flow paths. The code includes (1) a thermal hydraulic model, (2) an aerosol model, (3) an iodine model, and (4) a decay heat model. These models are numerically tightly coupled so as to include also important interrelation phenomena.

The aerosol behaviour in each control volume is treated by the multi-sectional, multi-component model MAEROS /2/. MAEROS has been utilised for other containment codes and applications have been already subject to uncertainty and sensitivity analyses /3/.

The German VANAM series of experiments were performed in order to verify FIPLOC-M and comparable codes. Five tests were carried out in the 640 m³ model containment of the Battelle Institute in Franfurt/Main /4/ built with reinforced concrete (figure 1).

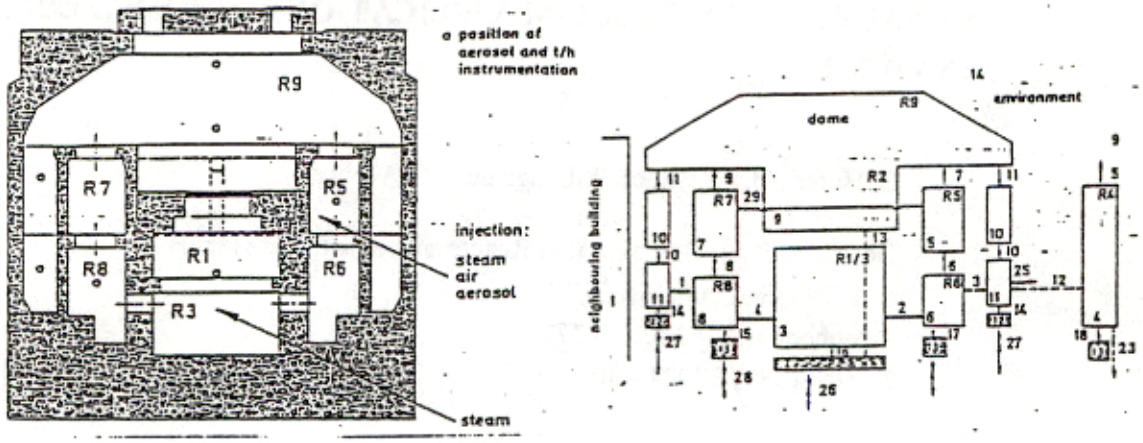


Figure 1. VANAM test geometry and the corresponding FIPLOC nodalization

For this uncertainty and sensitivity study the first three periods of a FIPLOC-M post test calculation of the VANAM M2 test were chosen /4/. The M2 experimental procedure started with a 14.5 h - heat up period of steam released into the room R5. This caused a pronounced stratified containment atmosphere with a hot steam-rich region above the steam source and a colder air-rich region below it. In the following second test period (45 min) the insoluble SnO_2 aerosol was injected into the room R5 by means of a steam-air carrier gas. For the third period (4.1 h) all injections were terminated. Pressure and temperature in the containment decreased due to the heat losses and the gas leakage through the concrete walls. The aerosol was inhomogeniously distributed by the atmospheric flows and depleted by natural deposition processes. No remarkable steam condensation on the aerosol particles occurred during these 'dry' periods.

Figure 1 shows the nodalisation used for the integrated thermal hydraulic and aerosol calculation with FIPLOC-M. Each room is represented by a control volume. Only R9 is divided into three control volumes, two of them simulating the annulus. The calculated aerosol concentrations for selected zones are shown together with the corresponding measured data in figure 2. The FIPLOC-M results are in good agreement with the experiments.

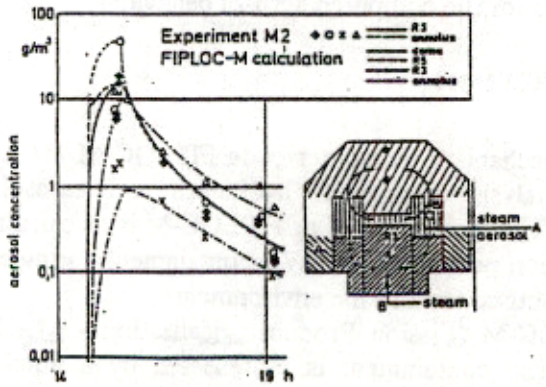


Figure 2. Selected local aerosol concentrations measured in the experiment and calculated by FIPLOC

UNCERTAINTY AND SENSITIVITY ANALYSIS

The probabilistic uncertainty and sensitivity analysis was performed with the aid of the program package SUSA /5/. Table 1 shows the list with the 179 identified uncertain parameters. More details about the parameters e.g. ranges, distribution types, distributional parameters, correlations etc. may be found in /6/.

Table 1. List of the uncertain parameters

No.	Description
	Uncertainties in aerosol physics.
	numerical analysis parameters
1	number of sections
2	accuracy criterion (transport)
3	accuracy criterion (agglom.)
4	maximum aerosol time step, s
5	highest expected atmosphere temp., C
6	highest expected total pressure, bar
7	relative error criterion for integration
8	absolute error criterion for integration, kg/m³
	geometry parameters :
9	ceiling area /volume, 1/m
to	for zones 3,...., 11
17	
18	floor area /volume, 1/m
to	for zones 3,...., 11
26	
27	wall area /volume, 1/m
to	for zones 3,...., 11
35	
	aerosol parameters, shape factors :
36	key for aerosol contrib. to atmosphere density
37	dynamic shape factor (chi)
38	diffusion boundary layer thickness, m
39	effective particle material density, kg/m³
40	agglom. shape factor (gamma)
41	particle sticking probability
42	thermal conductivity gas /particle
43	turbulence disspation rate, m²/s³
	aerosol source :
44	aerosol injection rate, kg/s
45	key for size distribution of source
46	mass geometric median diameter , m
47	geometric standard deviation
48	upper limit of particle diameter, m
	Uncertainties in thermalhydraulics.
	junctions :
49	cross section area of regular junctions
to	No. 1,...12, m²
60	
61	flow resistance number for regular
to	junctions No. 1...,12
72	
73	cross section area of leakage junct. 23, m²
74	cross section area of leakage junct. 25, m²
75	flow resist. number for leakage junct. 23
76	flow resist. number for leakage junct. 25
	zones :
77	volume of zones 3,..., 11, m³
to	
85	
86	injection rate of steam, kg/ s
87	injection rate NC gas, kg/ s
88	temperature of NC gas, C
89	geodetical hight of zones 3,..., 11, m
to	
97	
98	geodetical hight of junctions
to	No. 2, 4, ..., 11, m
106	
107	absolute accuracy crit. for integr. of gas flow, kg/s
108	residual water in zone 10, kg
109	residual water in zones 3, ..., 9, 11
to	
116	
	heat and mass transfer :
117	HTC for convection, W/m²/K
118	HTC for condensation, W/m²/K
119	dynamic viscosity of boundary layer, Pa·s
120	HTC for radiation, W/m²/K
121	specific heat of NC gas, J/kg/K
122	key for HTC options
	heat slabs :
123	49 heat slab areas, m²
to	
171	
172	heat conductivity of heat slabs, W/m/K
	(except slabs No. 14, 15, 47, 48)
173	heat conductivity of heat slabs
	No. 14, 15, 47, 48, W/m/K
174	specif. heat capacity of heat slabs, J/kg/K
	(except slabs No. 14, 15, 47, 48)
175	specif. heat capacity of heat slabs
	No. 14, 15, 47, 48, J/kg/K
176	density of heat slab material, kg/m³
177	thickness of waterslabs no. 14, 15, 47, 48, m
	additional parameters :
178	particle collision efficiency
179	slip factor

A parameter sample of size n = 100 was generated, i.e. 100 179-tuples of parameter values randomly selected according to the specified distributions and correlations (simple random sample) and the FIPLOC-M code was run for each. Figure 3 shows the 100 time histories of the aerosol concentration in zone 9.

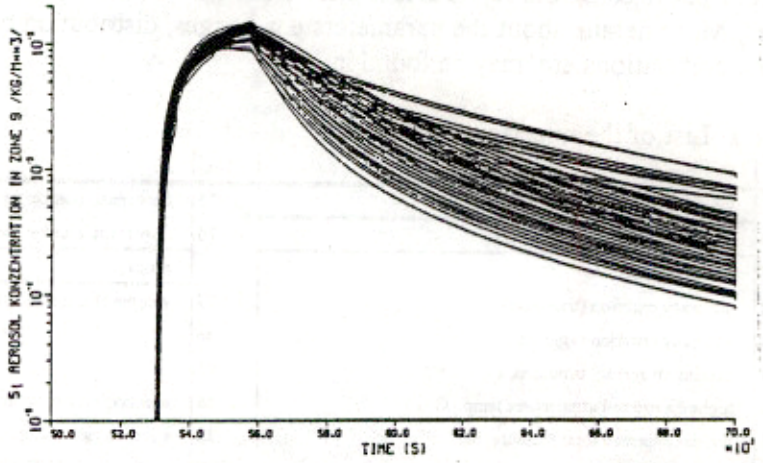


Figure 3. Aerosol concentration in zone 9. 100 time histories obtained with FIPLOC-M for randomly selected parameter vectors.

The 100 results along with the parameter sample form the data basis from which all subsequent uncertainty and sensitivity statements are derived. For the sake of simplicity two specific points of time were selected at which the analysis was performed : 55500 s = 15.4 h = end of the aerosol injection phase and 70000 s = 19.4 h = end of the calculation.
Figure 4 shows selected uncertainty results represented in terms of statistical (90 %, 90 %) two-sided tolerance intervals and empirical distribution functions. A tolerance interval is interpreted in this case as a region containing at least 90 % of the uncertainty of the corresponding aerosol concentration at the respective point of time at a confidence level of at least 90 %.

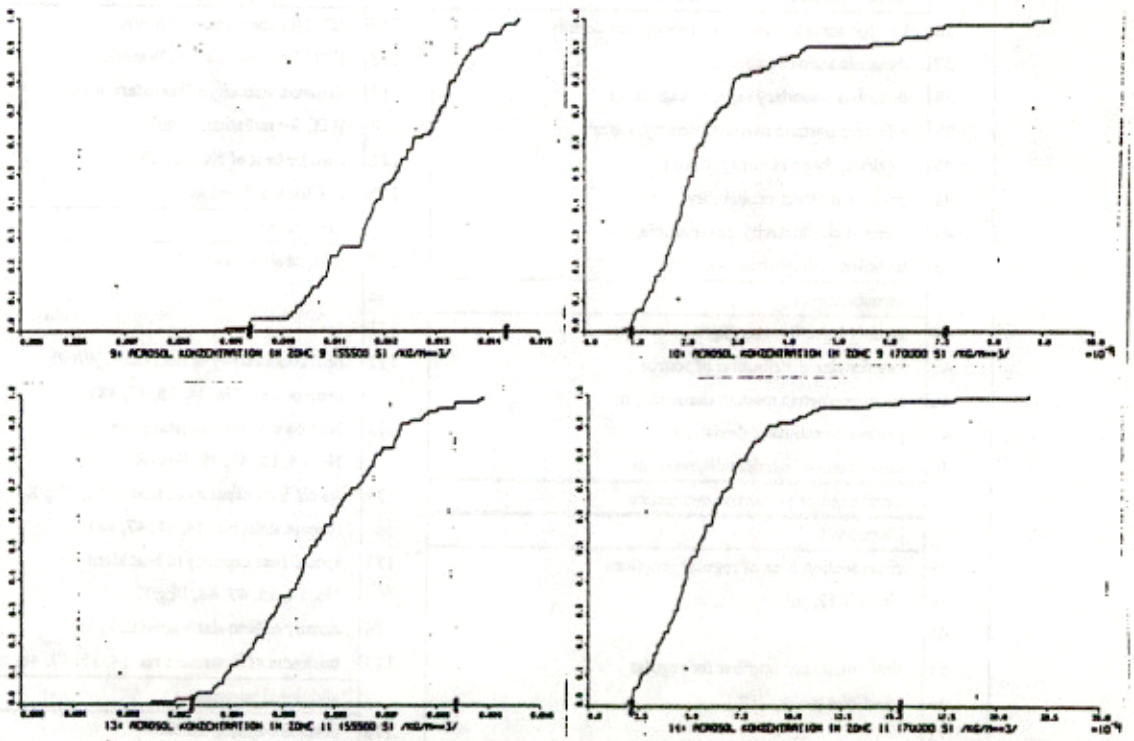


Figure 4. The empirical distribution functions and (90%, 90%) two-sided tolerance intervals for the aerosol concentration in zones 9 and 11 at 55500 s and 70000 s.

In table 2 the results of the sensitivity analysis for several output quantities from FIPLOC-M are summarized. At each of the two points of time a stepwise rank regression analysis was performed. This procedure selects from the set of 179 parameters the main contributors to uncertainty. Table 2 presents the corresponding sensitivity measures i.e. the standardized rank regression coefficients. In addition the total R^2 values are shown. They indicate the percentage of variability of the output quantity explained by a linear rank regression model in the selected parameters.

Table 2. The main contributors to uncertainty of the selected FIPLOC-M results

Selected results and most important parameters		Standardized rank regression coefficients from stepwise regression analysis and total R^2-values at 55500 s	at 70000 s
Aerosol concentr. in zone 9,	R^2	0.95	0.98
- (44) aerosol injection rate		0.75	-
- (43) turbulence dissipation rate		-0.33	-0.29
- (37/40) CHI and GAMMA*		-0.33	-0.56
- (1) number of sections		-	-0.45
Aerosol concentration in zone 11,	R^2	0.89	0.98
- (74) cross ssection area of leakage junct. 25		0.5	-
- (76) flow resist. number of leakage junct. 25		-0.35	-
- (44) aerosol injection rate		0.38	-
- (37/40) CHI and GAMMA*		-	-0.76
- (43) turbulence disspation rate		-	-0.38
Total aerosol mass suspended,	R^2	0.99	0.97
- (44) aersol injection rate		0.76	-
- (37/40) CHI and GAMMA*		-0.45	-0.63
- (43) turbulence dissipation rate		0.33	-0.36
- (1) number of sections		-	-0.36
Released aerosol mass,	R^2	0.99	0.98
- (74) cross section area of leakage junct. 25		0.57	0.52
- (76) flow resist. number of leakage junct. 25		-0.53	-0.41
- (37/40) CHI and GAMMA *		-	-0.44

* Complete positive dependence between the parameters CHI and GAMMA.

DISCUSSION OF THE RESULTS

At the end of the aerosol injection period (t=55500 s) the uncertainties of the calculated total airborne aerosol mass, the local aerosol concentrations and the total aerosol mass released are relatively small. Later on the uncertainties increased with time due to the dynamics of the involved processes.

At 70000 s 0.2 kg of the injected 8.91 kg of the SnO_2 aerosol are still airborne. The two-sided (90 %, 90 %) tolerance limits are 0.07 kg and 0.49 kg. The released aerosol mass is 0.29 kg with the tolerance limits 0.1 kg and 0.63 kg. A large portion was released early in the experiment, when the aerosol concentration and the gas pressure were high and uncertainties low. This is the reason why this uncertainty range is not broader than that of the total aerosol mass although large uncertainties of parameters for the leakage path and the gas pressure are involved.

The largest contributors to uncertainty of some selected aerosol results are summarised in table 2. Their influence varies strongly in time, e.g. the importance of the aerosol injection rate on the aerosol concentrations is much higher at t = 55500 s than at t = 70000 s. The dynamic and the agglomeration shape factors, CHI and GAMMA, and the numerical parameter 'number of sections' show an increasing importance with increasing problem time because of their influence on the dynamics of the aerosol depletion process. An increasing GAMMA accelerates agglomeration and sedimentation but an increasing CHI reduces sedimentation. Since the parameters are negatively correlated to the released and the suspended aerosol mass the influence of GAMMA is dominant.

An increasing turbulence dissipation rate increases the turbulent agglomeration. Qualitatively its influence on the results is similar to that of (GAMMA, CHI).

The uncertain parameter 'number of sections' is negatively correlated to the aerosol concentration in zone no. 9 respectively to the total aerosol mass suspended. Consequently a larger number of particle size classes, i.e. a numerically more accurate calculation, reduces these calculated aerosol results. This finding stands in contradiction to /3/ where a minor influence of the number of sections on the suspended aerosol mass was found. In both studies the number of sections was varied between 5 and 20, but the particle size domain is larger in the present study.

The aerosol concentration in the lower annulus zone no. 11 increases with an increasing cross section area of the leakage junction no. 25 and decreases with a decreasing flow resistance number at t = 55500 s. At this time the aerosol concentration in zone no. 11 is much lower than in the adjacent zone no. 10, which is connected to the dome. A higher gas leakage through junction no. 25 causes a higher inflow of aerosol loaded atmosphere from the dome via zone no. 10.

The uncertainty of the aerosol mass released to the environment depends on the uncertain leakage parameters and the most important aerosol parameter which is (GAMMA, CHI).

CONCLUSIONS

- The uncertainty of the total aerosol mass suspended and of the local aerosol concentrations depends mainly (1) on a few uncertain aerosol parameters (to be specified by the code user), e.g. the agglomeration shape factor and the turbulence dissipation rate, and (2) on the numerical parameter 'number of sections'. Additional contributors to the uncertainty of the local aerosol concentrations are uncertain parameters having an effect on the atmospheric flows in the containment and on the leakage flow: cross section area of openings, flow resistance number, steam injection rate, etc.
- The uncertainty of the aerosol injection rate influences only the short term aerosol results.
- The uncertainty of the leaked aerosol mass depends on (1) the uncertain leakage parameters, i.e. the cross section area and flow resistance number of the leak, and (2) on uncertain aerosol parameters, i.e. the agglomeration shape factors, etc.
- The uncertainty of the aerosol results is also influenced by the uncertainty of the numerical analysis parameter 'minimum number of sections needed so that the result is still sufficiently accurate'. Consequently, in less accurate calculations which have a small number of sections the aerosol concentrations are overestimated.

All results of this uncertainty and sensitivity analysis are well understood. They confirm the high quality of the coupling between thermal hydraulic and aerosol behaviour models in FIPLOC-M 1.5 for 'dry' aerosol cases. In the second part of this study a 'wet' case with condensation on aerosol particles is under investigation.

REFERENCES

/1/ H. Jahn, G. Weber, T. Pham,
Description of the Mod 2/85 Version of the RALOC/FIPLOC Family,
GRS-A-1315 (Dec. 1986)

/2/ F. Gelbard
MAEROS User Manual, NUREG/CR-1391(1982)

/3/ J.C. Helton, R.L. Iman, J.D. Johnson, C.D. Leigh
Uncertainty and Sensitivity Analysis of a Dry Containment Test Problem for the MAEROS Aerosol Model
Nuclear Science and Engineering 102, 22-42 (1989)

/4/ T. Kanzleiter, K.O. Fischer, H.J. Allelein, S. Schwarz, G. Weber.
The VANAM Experiments M1 and M2 - Test Results and Multi-Compartmental Analysis,
Journal of Aerosol Science, Proceedings of the EAC '91, 22 Suppl. 1 (1991)

/5/ E. Hofer
Probabilistische Unsicherheitsanalyse von Ergebnissen umfangreicher Rechenmodelle, GRS-A-2002, GRS Garching (1993)

/6/ J. Langhans et al.
Unsicherheits- und Sensitivitätsanalyse der Aerosolrechnung zum VANAM-M2 Experiment mit FIPLOC-M, GRS-A-Report, to be published

ANALYSIS OF SOURCE TERM UNCERTAINTY ISSUES FOR LWRs

M. Kajimoto, K. Muramatsu, and N.Watanabe

Risk Analysis Laboratory,
Department of Reactor Safety Research
Japan Atomic energy Research Institute
Tokai-mura, Naka-gun, Ibaraki-ken, 319-11, Japan

INTRODUCTION

In a Level 2 Probabilistic Safety Assessment (PSA), core damage sequences are systematically identified and the accident progression and source terms are analyzed for these sequences with computer codes. Such analyses provide valuable insights for planning accident management strategies. However, meaningful use of PSA results can not be made without good understanding of uncertainties in such analysis.

There are two necessary tasks for assessing the effects of uncertainties, namely, phenomenological research to define the variability range of each uncertain parameter and sensitivity study to examine the effect of change in such parameters on the source terms. This paper deals with a sensitivity study for the latter purpose. It is widely recognized that the source terms strongly depend on accident sequences. However sensitivity studies performed in the past were mostly limited to a small number of sequences selected by their high frequency and/or representative characteristics. Therefore it is desirable to examine how the effects of various uncertainty factors depend on accident sequences and to discuss how our understanding on the profile of source terms are affected by such uncertainty factors.

This paper presents a sensitivity study concerning the sequence dependency of the effect of uncertainty factors performed at the Japan Atomic Energy Research Institute as part of a generic level 2 PSA of a BWR with a Mark-II containment. Some results from this PSA were reported in previous papers[1,2] including a short discussion on the effects of two uncertainty parameters: relocation models of molten materials and containment failure location. This paper extends the discussion on these issues to their effects on various accident sequences. This paper also discusses the sequence dependent effect of the difference between the coupled and decoupled analyses of thermal hydraulics and fission product (FP) transport processes.

ACCIDENT SEQUENCE CATEGORIZATION

In JAERI's PSA, front line event trees identified 51 core damage sequences shown in Table 1 and a containment event tree, made for each core damage sequence, identified many scenarios of failure of the primary containment vessel (PCV). For each of the 51 sequences, a source term analysis was made for a scenario leading to over pressure failure of PCV in late phase using the THALES/ART code system[3], where accident progression was simulated by THALES and then FP transport process was analyzed by ART[4] with use of thermal hydraulic boundary conditions given by THALES.

In the previous paper[1], based mainly on the timing of key events, the accident sequences were tentatively classified into three groups. In the present study, based on considerations on the source terms, it was recognized that the accident sequences could be

better categorized into the following five groups by the availability of cooling systems for the core and the containment:

Group 1 : Accident sequences caused by loss of decay heat removal systems (RHR) with success of high pressure core spray system (HPCS) or reactor core isolation cooling system (RCIC) such as TQW sequence. In these sequences, over pressure failure of primary containment vessel (PCV) occurs at about 40 hours after accident initiation, leading to core melt after the PCV failure.

Group 2 :Accident sequences caused by loss of RHR with success of low pressure core spray system (LPCS) or low pressure core injection system (LPCI) such as TQUW sequence. Failure of coolant injection due to temperature rise in suppression pool lead to core melt. PCV failure occurs at about 25 hours after accident initiation.

Group 3 :Accident sequences caused by loss of all ECCSs such as TQUV sequence. Core melt occurs in early period, and The PCV failure occurs at about 25 hours.

Group 4 :Accident sequences caused by loss of all AC power such as TB sequence. Core cooling is available by RCIC. However, failure of coolant injection due to consumption of DC battery lead to core melt. PCV failure occurs at about 30 hours.

Group 5 :Accident sequences caused by failure of reactor scrum such as TC sequence. Over pressure failure of PCV occurs at about 1 hour, leading to core melt after the PCV failure.

The timing of major events, beginning of core melt, failure of core support plate, failure of reactor pressure vessel (RPV), failure of pedestal floor, and failure of PCV, are shown in Fig.1 for the sequences initiated by transients. Similar results were obtained for those initiated by LOCAs. The PCV failure timing did not depend much on whether the sequence was initiated by a LOCA or a transient.

UNCERTAINTY FACTORS EXAMINED IN THIS STUDY

Sensitivity studies for specific accident sequences in a PWR[5,6] and a BWR[7] were performed at JAERI in the past. In these studies, the effects of changes of about 20 parameters on the source terms were examined and showed that the selection of models for relocation of molten materials in the RPV and, for a BWR case, location of containment failure have quite significant effects. In addition, comparison of computer codes used in Japan for PSAs[8,9] showed that the interactions between thermal-hydraulics and FP behavior had strong effect on the calculated source terms. Therefore effects of the following three factors were investigated in this study:

- relocation models of molten materials,
- containment failure location,
- phenomena associated with the difference between the coupled versus decoupled analyses of thermal hydraulics and FP transport behaviors, such as revaporization of volatile FPs whose effect would be more significant in coupled analyses.

In the following discussions, the magnitude of source terms is represented by the fraction of CsI released to the environment.

METHOD AND RESULTS OF SENSITIVITY STUDIES

Effect of Relocation Models of Molten Materials

The fuel damage and relocation process involves highly complex phenomena and, even after the conduct of several large scale experiments, a precise prediction of material relocation is quite difficult. Therefore the THALES code provides several relocation models to allow sensitivity studies to examine the effect of modeling uncertainty on the source terms. Two models in THALES were used in this study: one model assumes that, when the fuel melting condition is reached, the molten material relocates to the bottom of core (model f_1) and the other to the vessel head (model f_2). Source terms were calculated for the 51 accident sequences adopting the models f_1 and f_2. Then the results were compared. The set of calculations with the model f_1 will be referred to as "base cases" in this paper.

The comparison of two sets of calculations indicated that the effect of relocation model was not significant for the timing of events, such as the time of containment failure. However the amount of release of FPs from fuel in the pressure vessel (in-vessel release)

was considerably different between two sets. Figure 2 shows the cumulative mass of CsI released in-vessel. The released mass of CsI for the model f1 were larger than that for the model f2 in all the sequence groups by about 20 to 30 percent of core inventory.

The difference between the results for the models f1 and f2 can be explained as follows. The release rate of FPs from fuel is calculated with the CORSOR-M model[10] as a function of fuel temperature. In the calculations with model f1, when the temperature of a fuel node reaches its melting temperature, the node relocates onto the core support plate and then transfers heat to the support plate. If the water level in the core shroud is higher than the plate, the heat transfer to the water is taken into account. Otherwise, it continues to heat up. When the support plate reaches its melting temperature, the core and the support plate collapse into the lower plenum, splashing out the water in the lower plenum to the downcomer due to the rapid steam generation by the heat transfer from the core debris. Therefore the molten material maintains high temperature without being cooled. On the contrary, in model f2, the "molten" node directly relocates to the vessel head and is cooled by the water in the lower plenum. Because of these differences, the temperature calculated with model f1 is kept at high temperature longer than that with model f2 and, consequently, yields higher in-vessel release of FPs.

In Figure 2, although there exist some sequence-to-sequence variations in the amount of in-vessel release, the difference of two relocation models has more significant effect on the in-vessel release than the difference of sequences does.

The present calculations predicted that the natural deposition mechanisms of aerosol, mainly the gravitational settling, would quite effectively remove the CsI aerosol and hence the source terms are strongly dependent on the time available for the FPs to deposit in the reactor coolant system (RCS) or in PCV, which is shortest for group 1 and 5 and longest for group 3. Therefore, in Figure 3, groups 1 and 5 have largest source terms; groups 2 and 4 have the second largest; and group 3 has the least.

Because of the effective natural removal mechanisms, the CsI released in-vessel would mostly deposit in RCS or PCV and the source terms were controled mainly by ex-vessel release of CsI. Since model f1 gave higher in-vessel release than model f2, it resulted in lower release during core-concrete interaction (ex-vessel release). Thus, as shown in Figure 3, the source terms for the model f2 were generally larger than that for the model f1.

In Figure 3, as for the sequence groups 1, 2, 4 and 5, the effect of changing the relocation model brought about the change in the source terms by a factor of 2 to 3, and as for the group 3, the change by a factor of 5 to 10. These differences among sequence groups are attributed to various group-to-group differences such as the difference in containment failure timing and the difference in the in-vessel release.

In summary, the difference of fuel relocation model considerably changed the amount of in-vessel and ex-vessel release of CsI and consequently changed the source terms for the sequences in all groups. However the significance of the effect is different from each other group by group.

Effect of Containment Failure Location

In a BWR plant, the failure location of PCV is important to calculate source terms. If the location is in wetwell gas space, FPs in the PCV would be released to the environment through the suppression pool where scrubbing effect can be expected. In this study, we considered three possibilities: drywell gas space, wetwell gas space, and wetwell liquid space. The drywell failure was assumed in the base cases. Analyses for all 51 sequences were performed for these three locations.

As shown in Figure 4, the wetwell failure cases resulted in smaller source terms of CsI than the drywell failure cases for all sequence groups because of the scrubbing in the suppression pool. However the degree of differences dependends on sequence groups.

The differences were quite significant in groups 2, 3 and 4; source term of CsI was by two order of magnitude smaller than the drywell failure case. On the other hand, the difference was much less significant in groups 1 and 5. This sequence dependency was explained by the difference in condition of the suppression pool water at the time when CsI pass through the pool water. In case of groups 1 and 5, suppression pool was in saturated condition while it was in subcooled condition in other cases. The decontamination factors for

Table 1. Radionuclide Source Terms[1,8]

Radionuclide	Ci/kg Convecting (Liquid)	Ci/kg Crust (Airborne)
90 Sr	3.0E-03	3.4E-02
Tc 99	1.3E-04	3.0E-04
I 129	6E-07	2.9E-04
Cs 137	4.5E-01	4.5E-01
Np 237	7E-08	5.1E-04
Pu 239	1.1E-07	1.6E-05
Pu 240	—	1.0E-09
Am 241	5E-07	1.5E-04

The airborne source terms consist primarily of materials picked up and entrained in high-velocity gas flow across the crust surface. It was assumed that the particles were all in the respirable range (<10 microns). The liquid release source terms contain materials dissolved in the liquids that are presumed to escape from the tanks in the leak/spill sequences.

Various source terms were developed for various release categories as presented in Table 2. The breakup of the release categories based on release pathway and radionuclide content was done to facilitate the comparison of high frequency/low-consequence accidents with low-frequency/ high-consequence accidents. The methodology used to estimate source terms is presented through the use of an example. Both airborne and water pathway source terms were similarly developed. The results of the source term analysis for the various release categories are also summarized in Table 2. The release terms for individual isotopes are obtained by multiplying the appropriate concentrations in Table 1 by estimated releases in Table 2.

METHODOLOGY EXAMPLE

Analysis of an airborne release sequence is presented as an example of the methodology used in generating source terms for the high-level waste storage accidents. The key feature of this methodology is the use of distributions to express the uncertainty or "state of knowledge" of the analyst. The distributions are used to reflect the analyst's confidence level regarding the estimates of various parameters that were used during the calculation of the source term for individual sequences.

BURP/BURN SEQUENCES — CATASTROPHIC DOME COLLAPSE (DCH)

The DCH release category represents those scenarios in which a catastrophic tank failure, resulting in collapse of the dome, leaves the tank open to the environment. Tank failure could occur if the Burp/Burn pressure loads are significant. Dome collapse leaves the tank vulnerable to winds and gusts which may entrain some material and provide a release path. The source term evaluation for this release category is summarized in Figure 2.

Table 2. HTF PSA release category and readiological source term summary.

Release Pathway		Radionuclide Content	Release Category	Low Release (kg) (10th%)	Mean Release (kg)	High Release (kg) (90th%)
To Atmosphere	Through HEPA	None	TG	—	—	—
	HEPA Bypassed	Low	BPL	3.4E-4	7.0E-4	2.1E-3
	HEPA Breached	Low	HEPAL	0.8	1.8	2.8
	HEPA Breached	High	HEPAH	4.1	6.9	10.2
	Dome Collapsed	High	DCH	14.7	32.8	55.2
	Dome Collapsed	Very High (fire)	DCVH	57 (Cs Enhanced)	113 (Cs Enhanced)	283 (Cs Enhanced)
To Ground	Subterranean Leak	Small	SLK	5,680	17,100	28,400
	Subterranean Leak	Large	LLK	113,600	340,800	568,000
To Atmosphere and Ground	Infiltration/Surface Spill	Small	SMSP	570	1,700	2,840
	Transfer Failure/Surface Spill (NA 101-SY)	Large	LLSP			
	Dome Collapse + Small Leak	High	DCSLK	—	DCH + SLK	—
	Dome Collapse + Large Leak	High	DCLLK	—	DCVH + LLK	—

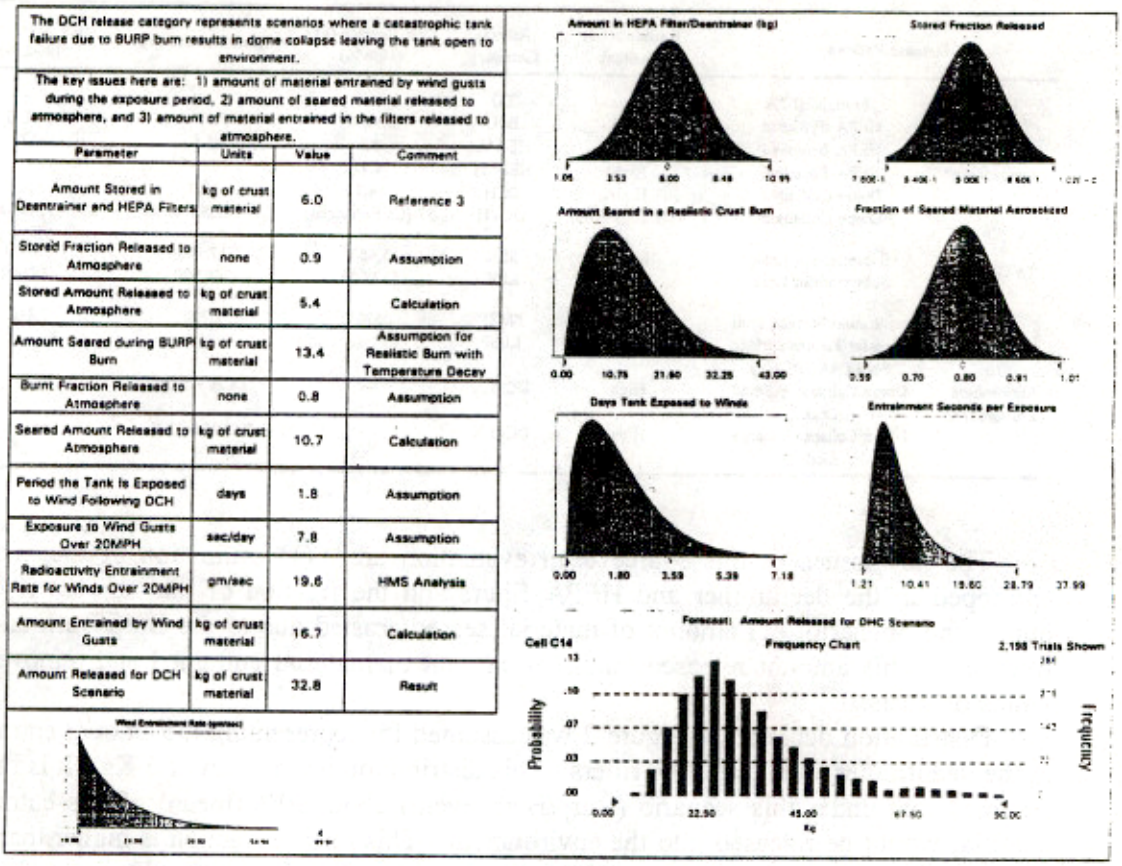
The key issues in this source term evaluation are: (1) estimation of the material entrapped in the deentrainer and HEPA filters and the fraction of this amount released during the Scenario; (2) amount of material seared/crusted due to the Burp/Burn and the fraction of this amount released; and, (3) amount of material entrained and removed by winds or gusts.

Distribution depicted in Figure 2 was assumed for representing the amount entrapped in the deentrainer and the HEPA filters. This distribution has a mean of 6 Kg. It is further assumed that under this scenario (Burp/Burn event) about 90% (mean) of this entrapped material would be released into the environment. This release fraction is higher than that for the HEPAH scenario since the DCH scenario with a Burp/Burp event leading to a dome collapse is likely to be much more energetic. It was assumed that the release fraction could range from 80% to 100%; thus, the distribution shown in Figure 2 was selected.

The amount of material seared was estimated in a separate calculation (using a heat transfer model). The amount is shown by the distribution presented in Figure 2 and has a mean of about 13.4 Kg. This distribution depicts the amount seared during a realistic Burp/Burn (short burn with temperature decay). Some fraction of this crusted material is prone to be carried upwards due to convection currents and thus be released into the atmosphere. As the Burp/Burn event is much more energetic, it is estimated that about 80% (as opposed to only 20% for HEPAH scenario) of the seared material will be released (mean 80%, with a range from 60% to 100%).

After a dome collapse, the tank contents can be directly exposed to the atmosphere and subject to wind entrainment. The exposure period for entrainment is the time from dome collapse to the time when the tank is completely covered as a result of postaccident recovery operations. This exposure time could vary from half a day to a week. The distribution, also shown in Figure 2, reflects this range and has a mean exposure time corresponding to 1 day.

It has been shown by separate HMS calculations that only winds greater than 20 MPH are capable of entraining the tank contents. Meteorological data report wind exceeding 20 MPH for a total of 20 hours in a given year. Based on this information, a time window for entrainment was evaluated (per exposure day). The distribution reflecting this time window is shown in Figure 2 and has a mean of 8 sec/day, with a distribution ranging from 1 to 28 seconds/day. HMS analysis also predicts entrainment rates ranging from 10 to 300 gm/sec for winds from 20 MPH to 70 MPH. The entrainment rate distribution assumed for this analysis is shown in Figure 2. This distribution has a mean of 20 gm/sec, with a



The DCH release category represents scenarios where a catastrophic tank failure due to BURP burn results in dome collapse leaving the tank open to environment.

The key issues here are: 1) amount of material entrained by wind gusts during the exposure period, 2) amount of seared material released to atmosphere, and 3) amount of material entrained in the filters released to atmosphere.

Parameter	Units	Value	Comment
Amount Stored in Deentrainer and HEPA Filters	kg of crust material	6.0	Reference 3
Stored Fraction Released to Atmosphere	none	0.9	Assumption
Stored Amount Released to Atmosphere	kg of crust material	5.4	Calculation
Amount Seared during BURP Burn	kg of crust material	13.4	Assumption for Realistic Burn with Temperature Decay
Burnt Fraction Released to Atmosphere	none	0.8	Assumption
Seared Amount Released to Atmosphere	kg of crust material	10.7	Calculation
Period the Tank is Exposed to Wind Following DCH	days	1.8	Assumption
Exposure to Wind Gusts Over 20MPH	sec/day	7.8	Assumption
Radioactivity Entrainment Rate for Winds Over 20MPH	gm/sec	19.6	HMS Analysis
Amount Entrained by Wind Gusts	kg of crust material	16.7	Calculation
Amount Released for DCH Scenario	kg of crust material	32.8	Result

Figure 2. Source term summary for release category DCH.

range from 10 to 50 gm/sec and was judged appropriate for the Hanford Tank Farm meteorological conditions.

Based on the amount of material entrapped in the HEPA filters/deentrainer, the amount of material crusted, the release fractions, the wind exposure period, the entrainment time window (fraction), and the wind entrainment rate, the source term can be evaluated for the DCH scenario. Figure 2 depicts the resultant distribution for the amount released for the Based on the amount of material entrapped in the HEPA filters/deentrainer, the amount of material crusted, the release fractions, the wind exposure period, the entrainment time window (fraction), and the wind entrainment rate, the source term can be evaluated for the DCH scenario. Figure 2 depicts the resultant distribution for the amount released for the DCH scenario with a mean release of 32.8 Kg. The salient point values for this distribution are summarized in Table 2.

SUMMARY

As the accuracy of the accident consequences is highly dependent on the accuracy of the source term, it is important that all uncertainties regarding the source term are reflected explicitly. This can be achieved by allowing the analyst to express his/her state of knowledge regarding the various input parameters used in the engineering evaluation of the source term. The methodology presented through an example achieves this goal. This methodology was successfully applied to define and evaluate a number of source terms for the high-level waste storage accidents.

REFERENCES

1. D.L.Herting, "Laboratory Characterization of Samples Taken in May 1991 from Hanford Waste Tank 241-SY-101," Westinghouse Hanford Company, Report WHC-SD-WM-DTR-024 (1992).
2. "Environmental Releases for Calendar Year 1990," Westinghouse Hanford Company, Report WHC-EP-0527 (1992).
3. "A Safety Assessment for the Proposed Pump Mixing Operations To Mitigate Episodic Gas Releases in Tank 241-101-SY: Hanford Site, Richland, Washington," LANL-SA-65, Rev. 8, 9, 10, Los Alamos National Laboratory, Los Alamos, New Mexico (1992).
4. J.R. White, "Filter System Release Accident Analysis," Calc-Note: N6-CN-WT-SA-RAD-1, Rev. 0, (1993)
5. J.R. Travis, "An HMS/TRAC Analysis of a High-Level Radioactive Waste Tank Farm," Los Alamos National Laboratory, Report LA-UR-91-2699, Los Alamos, New Mexico (19___).
6. D.I. Herborn, et al., "Hanford Waste Vitrification Plant Preliminary Safety Analysis Report," Rev. 1, WHC-EP-0250, Chapter 3.0, Site Characteristics (1992).
7. F.P. Lees, "Loss Prevention in the Chemical Process Industries," Vol. I, p. 518, Butterworths, London, (1986).
8. D. L. Herting, "Laboratory Characterization of Samples Taken in Window E from Hanford Waste Tank 241-SY-101," Westinghouse Hanford Company, Report WHC-SD-WM-DTR-026 (1992).
9. "Risk Assessment for Hanford High-Level Waste Tank," Westinghouse Hanford Company, Report 241-89-101 (1993).

APPLICATIONS OF PATTERN RECOGNITION TECHNIQUES TO ONLINE FAULT DETECTION

R. M. Singer[1], K. C. Gross[1], and R. W. King[2]

[1]Reactor Analysis Division and [2]IFRO Division
Argonne National Laboratory
[1]Argonne, IL and [2]Idaho Falls, ID

INTRODUCTION

A common problem to operators of complex industrial systems is the early detection of incipient degradation of sensors and components in order to avoid unplanned outages, to orderly plan for anticipated maintenance activities and to assure continued safe operation. In such systems, there usually are a large number of sensors (upwards of several thousand is not uncommon) serving many functions, ranging from input to control systems, monitoring of safety parameters and component performance limits, system environmental conditions, etc. Although sensors deemed to measure important process conditions are generally alarmed, the alarm set points usually are just high-low limits and the operator's response to such alarms is based on written procedures and his or her experience and training. In many systems this approach has been successful, but in situations where the cost of a forced outage is high an improved method is needed. In such cases it is desirable, if not necessary, to detect disturbances in either sensors or the process prior to any actual failure that could either shut down the process or challenge any safety system that is present. Recent advances in various artificial intelligence techniques have provided the opportunity to perform such functions of early detection and diagnosis. In this paper, the experience gained through the application of several pattern-recognition techniques to the on-line monitoring and incipient disturbance detection of several coolant pumps and numerous sensors at the Experimental Breeder Reactor - II (EBR-II) which is located at the Idaho National Engineering Laboratory is presented.

DESCRIPTION OF THE EBR-II PLANT

The Experimental Breeder Reactor No. II (EBR-II) is a small electrical power producing, liquid-metal-cooled nuclear reactor operated by Argonne National Laboratory for the U.S. Department of Energy. Its nuclear steam supply system produces about 20 MWe when the plant is operated at its full nameplate thermal power rating of 62.5 MW. The plant

is currently being used for testing of fuel behavior after cladding failure, demonstration of passive safety concepts and improved control systems, demonstration of a closed fuel cycle based upon an advanced metallic fuel design and as a test bed for advanced surveillance and diagnostic tools. Over 1000 signals from almost as many sensors are collected and routed to a data acquisition system (DAS) for monitoring and archiving purposes.

Signal Validation and Disturbance Detection with SPRT

An expert system has been developed for signal validation and sensor-operability surveillance in nuclear and industrial intelligent-control applications that require high reliability, high sensitivity annunciation of degraded sensors or discrepant signals. Signal validation and sensor-operability surveillance have recently taken on an elevated importance in the context of advanced intelligent control applications. This is because the most well designed control system, whether it is totally hardware based or retains a human in the loop, can give rise to improper control actions if it is acting on erroneous input signals due to one or more degraded sensors. This expert system comprises an interconnected network of high-sensitivity pattern-recognition modules, each of which embodies a new and powerful tool for automated parameter surveillance: the Spectrum-Transform Sequential-Testing (STST, or ST2) algorithm.

In recent years the Sequential Probability Ratio Test (SPRT[1,2,3]) has found wide applications as a signal validation tool in the nuclear reactor industry. Two features of the SPRT that make it attractive for parameter surveillance and fault detection are (1) very early annunciation of the onset of a disturbance in noisy process variables, and (2) the fact that the SPRT has user-specifiable false-alarm and missed-alarm probabilities. One drawback of the SPRT that has limited its adaption to a broader range of intelligent controller applications is the fact that its mathematical formalism is founded upon an assumption that the signals it is monitoring are purely gaussian, independent (white noise) random variables. We have undertaken a detailed statistical analysis of a wide variety of plant signals at EBR-II that show many types of variables are contaminated by noise that is serially correlated. We have found that the presence of serial correlation in a process variable monitored by a SPRT module can lead to excessive false-alarm and/or missed-alarm probabilities.

To avoid these difficulties, and to expand the domain of automated signal-validation methods, we have developed and patented a new technique for signal validation and for sensor and equipment operability surveillance applications[4]. The technique is called the Spectrum-Transformed Sequential Testing (STST or ST2) method. We call the ST2 method a dual transformation method, insofar as it entails both a frequency-domain transformation of the original time-series data and a subsequent time-domain transformation of the resultant spectrally filtered data.

The ST2 method provides a superior surveillance tool because it is sensitive not only to disturbances in signal mean, but also to very subtle changes in the stochastic patterns comprising the noise associated with the monitored signals. It can be mathematically proven that the ST2 module provides the earliest possible annunciation of the onset of anomalous patterns in physical process variables.

For sudden, gross failures of sensors or system components an ST2 module would annunciate the disturbance as fast as a conventional threshold limit check. However, for slow degradation that evolves over a long time period (gradual decalibration bias in a sensor, appearance of a new radiation source in the presence of a noisy background signal, wearout or buildup of a radial rub in rotating machinery, etc.) the ST2-based system can annunciate the incipience or onset of the disturbance long before it would be apparent to visual

inspection of strip chart of CRT signal traces, and well before conventional threshold limit checks would be tripped.

A second important feature of the ST2 technique that distinguishes it from conventional methods is that it has built-in quantitative false-alarm and missed-alarm probabilities. This is quite important in the context of nuclear reactor applications, because it makes it possible to apply formal reliability analysis methods to an overall intelligent control system comprising a network of interacting ST2 modules that are simultaneously monitoring a variety of plant variables. This amenability to formal reliability analysis methodology will greatly enhance the Nuclear Regulatory Commission process of granting approval for nuclear-plant applications of this system.

One example of the use of the SPRT algorithms to detect incipient failures during operation of the primary coolant pumps in EBR-II was a transient and temporary change in the rotational resistance of the shaft in one of the two pumps. A post-event analysis of the measured data from the primary pumps (including, for example, shaft speed, pump motor power and coolant flow rate, all digitized at 5 second intervals) indicated that the SPRT provided an indication with a 99% confidence factor, that the disturbed pump was not performing normally at least 6 minutes prior to any observable changes in the nominal signal values. It is possible that even an earlier indication was possible, but the data tape was available only for the 7 minutes preceding the observed pump changes.

SYSTEM MONITORING AND ANALYTICAL SENSOR REPLACEMENT WITH SSA

The second technique used for monitoring is the System State Analyzer of SSA which is a state identification and estimation algorithm based on pattern recognition. This algorithm can identify and estimate the current state of any system based upon its previous operating history. The current state is determined by comparing a vector of sensor signals that are closely associated with the performance of the system under consideration with previously measured sets of the same signal vectors. This comparison by SSA is accomplished by software-based pattern-recognition algorithms that establish pertinent relationships (i.e., measure the similarity or overlap) between the signals within a defined operational domain. These learned patterns or relationships among the signals are then used to identify the learned state that most closely correspond with the current measured set of signals. This process of system state identification is used to detect and diagnose deviations in the operational characteristics of a system due to any cause as well as to estimate the "true" state of the system. The SSA is presently being used as an engineering surveillance tool for monitoring of EBR-II plant conditions.

Experience with the SSA at EBR-II has shown that the normal plant signal pattern characteristics identified by the SSA during steady-state operation are highly repeatable during a reactor run. When a sensor signal drifts or when a change in the plant occurs, such as a slight adjustment in reactor power level, the current observed pattern no longer matches the previously overlap with the previously learned states. The SSA evaluates and provides a measure of the new pattern overlap with the previously learned states. The SSA flags those signals which have the highest relative deviation from the expected pattern and estimates the value for each signal that would make the pattern consistent with some combination of the previously learned patterns. This feature of the SSA provides signal validation capability similar to analytic redundancy techniques and opens up the possibility of replacing the signal from a failed or degraded sensor with a validted estimate of the signal value.

In several instances during routine monitoring the SSA has detected signal problems, ranging from instrument drift to sensor failures. One of the occurrences was a degradation

of a thermocouple measuring the reactor outlet coolant temperature (which provides the basis for the reactor core temperature rise) that is used by the reactor operator as a control parameter. The degradation of the thermocouple resulted in a decrease in the indicated temperature of about 7 °F over 40 minutes (see Figure 1). In the Figure, the central trace is the estimated value and the two bounding traces represent the uncertainty in the estimation. Over this same time period, the SSA estimated value indicated an increase of several degrees. Later analysis showed that the reactor operator, observing the indicated decrease in reactor temperature rise, slightly increased the reactor power to compensate. After noting that the indicated signal did not respond to the change in power, the operator switched to another channel for control. During this entire period of operation with this degraded thermocouple, the SSA-estimated temperature provided an accurate value for this parameter, including the proper response to the operator adjustments. As can be seen from the data in Figure 1, the comparison of the estimated signal with the measured signal provided a direct indication of a developing problem with that sensor rather than a change or disturbance in the operating state of the reactor. Following this experience, we performed a series of controlled tests to show that in a real-time operating mode, SSA could determine the "true" state of the reactor system based upon 11 previously learned operating stated in the presence of multiple sensor faults as well as predict the values of signals in the presence of these simulated sensor failures and/or malfunctions. To accomplish this, the code was used in a learning mode to establish a learned-state matrix embodying information from 115 signals covering 11 separate operating states of the plant. Then, simulated failures in 15 individual signals were sequentially instituted through programming changes in the data acquisition system. The types of failures included sudden shifts in values as well as total loss of signal. As the signals were failed, the code was used in a real-time monitoring mode where all of the signals were estimated and compared with the actual plant measurements.

The SSA algorithm estimates the current state of the system by comparing the current sensor measurements with the previously learned states of the system. Even though 15 sensors were providing erroneous data, the pattern recognition scheme was able to identify the system state and estimate real-time values of all 115 signals. As shown in Figures 2 and 3, which show faulted signals as well as the estimated signals from SSA (and are representative of all the other data), it can be clearly inferred that: (1) the state of the system has not changed since there is no change in the estimated signals; and (2) the specific sensors shown (here the reactor flow rate and inlet temperature) have developed faults since they have deviated from the estimated signals.

SUMMARY AND CONCLUSIONS

The pattern-recognition techniques embodied by the SSA and SPRT continue to be exploited for use in sensor validation, fault detection and in other applications. The SSA is being applied at EBR-II in several specific areas related to fault-tolerant control, operability surveillance and plant-life extension. One application is the substitution of the on-line SSA calculated estimate of the temperature rise of the primary coolant across the reactor core to replace the signal from a failed, inaccessible thermocouple in the reactor outlet pipe. Because some of the originally installed primary system instrumentation has failed and is inaccessible for replacement the capability to replace key parameter sensor signals with validated calculated signal values is important to continued long-term availability of EBR-II. The other application is the use of the SSA along with SPRT for long-term degradation monitoring of the EBR-II primary pumps which are critical to extended-life operation of EBR-II.

Although these applications are in their early stages, the initial results together with the results of other SSA and SPRT application at EBR-II, have indicated that pattern-recognition techniques can be very useful in plant surveillance.

REFERENCES

1. K. C. Gross and K. E. Humenik, "Sequential Probability Ratio Tests for Nuclear Plant Component Surveillance," *Nucl. Tech.* **93**, pp. 131-137 (Feb. 1991).
2. K. Gross and R. Singer, "Automated Surveillance of Reactor Coolant Pump Performance," *Proc. Fourth Intl. Workshop on Main Coolant Pumps*, Phoenix, AZ, USA, 16-19 (April 1991).
3. R. Singer, K. Gross, K. Humenik, and M. Walsh, "Reactor Coolant Pump Monitoring and Diagnostic System," *Proc. 2nd Intl. Machinery Monitoring and Diagnostic Corp.*, Los Angeles, CA, USA pp. 19-24 (1990).
4. K. C. Gross and K. K. Hoyer, "Spectrum-Transformed Sequential Testing Method for Signal Validation Applications," *Proc. 8th Power Plant Dynamics, Control and Testing Symp.*, Knoxville, TN, USA pp. 36.01-36.12 (1992).
5. R. King, W. Radtke, and J. Mott, "Pattern-Recognition System Application to EBR-II Plant-Life Extension," *Proc. Nuclear Power Plant Life Extension*, Snowbird, UT, USA (31 July-3 August 1988) **II**, 512-518.
6. R. W. King, J. E. Mott, and W. H. Radtke, "Pattern-Recognition System Appliction to EBR-II Plant Life Extension, *Proceedings of the Topical Meeting on Nuclear Power Plant Life Extension*, Snowbird, UT, July 31 - Aug. 3, 1988.

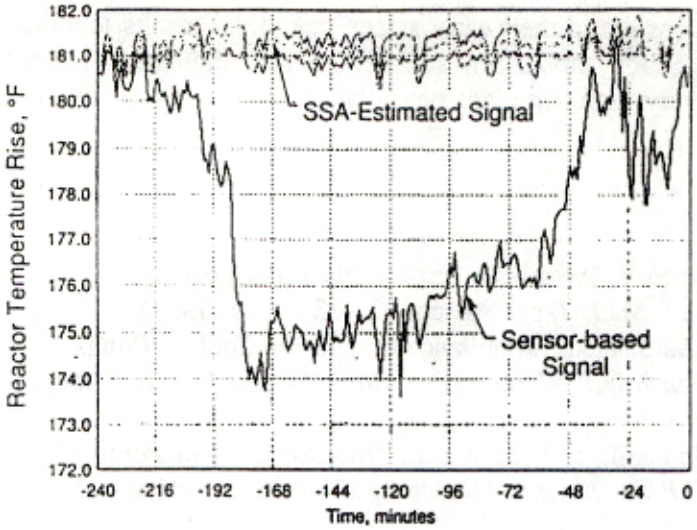


Figure 1. Detection of a Natural Disturbance in the Sensor Indicating Reactor Temperature Rise

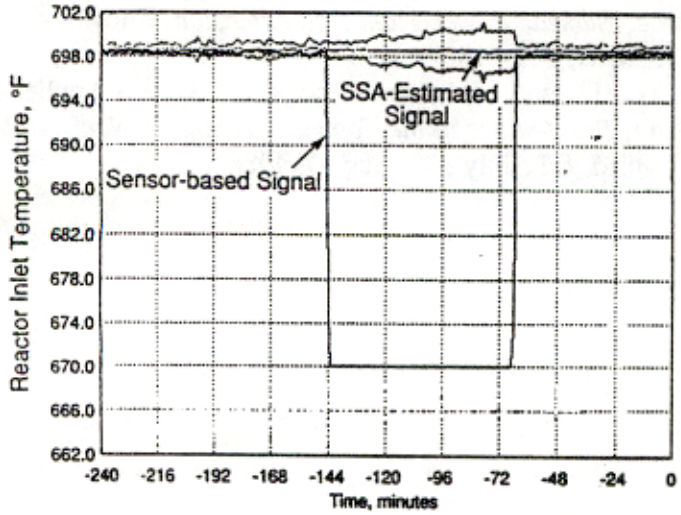


Figure 2. Estimation of the Inlet Temperature when the Temperature Sensor has been Artificially Failed

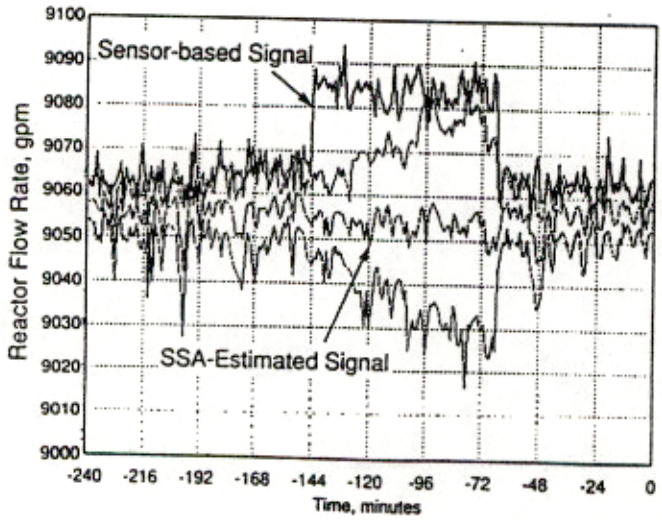


Figure 3. Estimation of the Flow Rate when the Flow Sensor has been Artificially Failed

PRINCIPAL FACTOR ANALYSIS OF THE REACTOR COOLANT PUMP SYSTEM

William S. Grenzebach
Applied Management Consultants
Box 5
325 Huntington Ave.
Boston, MA 02115
(617) 277-6173

Thomas J. Marx
Marx Social Science Research
196 Appleton Street
Cambridge, Massachusetts 02138

ABSTRACT

In today's operating environment of nuclear power plants, setpoints are established for key plant parameters, such as temperature, pressure and flow rate. Reducing excursions beyond these setpoints would save millions of dollars as a result of improved plant availability and, as well, improve plant safety. The paper presents the statistical method of principal factor analysis and the results of three computer runs. The results of the statistical analysis indicated that it is possible to consistently rank order the eleven tracked variables of the reactor coolant pump system. Implementation of the principal factor method would permit the decision maker to predict unanticipated transients and reduce plant unavailability.

1.0 Background

In today's operating environment of nuclear power plants, setpoints are established for key plant parameters, such as temperature, pressure, or flow rate. When these setpoints are exceeded, it is often common practice to scram the reactor, resulting in plant shutdown for those cases where extended maintenance and repair are necessary. Reducing excursions beyond these setpoints would save millions of dollars as a result of improved plant availability and, as well, improve plant safety. In a recently published case study,[1] classical statistical process control techniques (X-Bar, R, and CUSUM charts as well as regression analysis) were implemented on actual plant data gathered in real time over a 121-day period for the Reactor Coolant Pump

[1]W. S. Grenzebach and C. D. Heising, "A Computerized Diagnostic System For Nuclear Power Plants Based Upon Statistical Quality Control," *Nuclear Technology,* Vol. 90:1, pp 7–15, April, 1990; W. S. Grenzebach and T. J. Marx, "Principal Factor Analysis of the Reactor Coolant Pump System," *Transactions of the American Nuclear Society,* Vol. 63, pp 276–278, June, 1991 [Abstract]; W. S. Grenzebach, C. D. Heising, T. J. Marx, "Maximum Likelihood Factor Analysis of the Reactor Coolant Pump System,"*Proceedings of the International Topical Meeting on the Safety of Thermal Reactors,* (La Grange Park, Illinois), pp 50–62, 1991; W. S. Grenzebach, C. D. Heising, T. J. Marx, "Regression Analysis of the Reactor Coolant Pump System," *Joint International Power Conference* ASME Paper 91-JPGC-NE-B, September, 1991; W. S. Grenzebach, C. D. Heising and T. J. Marx, "Canonical Correlation Analysis of the Reactor Coolant Pump (RCP) and Component Cooling Water (CCW) Systems," Accepted by the *Probabilistic Safety Assessment International Topical Meeting,* Clearwater Beach, Florida, January 27–29, 1993; W. S. Grenzebach, C. D. Heising, T. J. Marx, "Canonical Correlation Analysis of Reactor Coolant Pump Interaction," Accepted by the Second IASTED Conference on Reliability, Quality Control, and Risk Assessment, Cambridge, MA., October 13–15, 1993.

System.[2] Analysis of the data showed the eventual plant trip could have been anticipated by at least 15 days by using statistical methods.

In a highly complex system such as a nuclear power plant with over 4,000 variables tracked in some form daily, simple accumulation of X-Bar, R, and CUSUM charts would be a formidable challenge to record and interpret as in the model study discussed above. More advanced statistical techniques are needed to reduce the number of variables under observation to a more manageable set. Can the objective of assessing the viability of the system at any given point in time be met by focusing on a small subset of these measurements? The statistical procedure of principal factor analysis, pioneered in intelligence testing, can help answer this question.

Factor analysis is an exploratory technique without the firm foundation in probability and statistics characteristic of regression analysis. "The characterization of factor analysis as mainly an exploratory technique seems correct, because, being based on the analysis of covariational data and normally indeterminate in its identification of common factors can ultimately only provisionally establish its common factors as causal mechanism accounting for the relationships among variables."[3] Factor analysis presents the analyst with one or two factor rotations possible in a multidimensional space: "... it may have been the failure to recognize the fact that a given matrix of correlations could be factored in an infinite number of different ways that led to the many controversies about the 'true', the 'best', or the 'covariant' solution for a set of data.... It should be perfectly clear that many factor solutions are possible for a given set of variables for a single sample of individuals."[4]

2.0 The Principal Factor Method

Building upon the classical factor analysis model discussed above, the principal factor method chooses the first factor coefficients, a_{j1}, so as to maximize the sum of the contributions of that factor to total communality. The sum is given by the following formula:

$$V_1 = a_{1i}^2 + a_{2i}^2 + ... a_{n1}^2$$

In order to maximize a function of n variables, the methods of La Grange multipliers is applied to maximize V_1. The details of this procedure may be found in the classic text by Harman.[5]

The maximization of the original equations, using La Grange multipliers, results in a system of V equations for the solution of n unknowns, a_{j1}. Disregarding the important mathematical foundations which are necessary to obtain this result, the useful conclusion from this procedure is that the factor of proportionality is $g = \sum_{j=1}^{m} a_{j1}^2$. This is really another expression of V_1 the quantity to be maximized. Thus, V_1, is equal to one of the roots of the characteristic equation, the largest root λ. These roots are known as eigenvalues in matrix notation. The sum of the eigenvalues for each factor accounts for total communality.

Thus it is possible to use the eigenvalues for each factor in a way analogous to the use of R^2 in regression analysis, i.e., as an indicator of the proportion of statistically significant variation due to a variable. In regression analysis, of course, R-squared is directly linked to an observable variable, while in factor analysis, the "factor," itself, is not part of the original data set. In regression analysis, the contribution of R-square is based upon the method of least-squares, whereas in factor analysis, the eigenvalues represent contributions to variance.

In the following analysis, for reasons of space, results are only presented for pump 2B2. Also, pump 2B2 had consistently the higher factor loadings in the first factor (temperature) compared to the other pumps.

3.0 Principal Factor Analysis of Pump 2B2 (First Run)

The factor analysis of Pump 2B2 repeats the pattern of Pumps 2A1 and 2B1 with a reduction in system complexity to two factors (see Table 1). The two-factor model explains 99.9% of explained variance. The first factor accounts for 80.71% of the variance, while the second factor explains the remaining 19.19%. Again, the

---

[2]See Douglas C. Montgomery, *Introduction to Statistical Quality Control*, (New York 1985), Pages 173–175, and Page 226. Where means and standard deviations are unknown repeated sampling may be required to establish their values.

[3]Harry H. Harman, *Modern Factor Analysis*, (Chicago, 1973), Page. 342.

[4]*Ibid*, Page 4

[5]Harmon, *op. cit.*

first factor is heavily loaded by temperature variables (.77351 for upper bearing, .64007 for downward bearing, and .69156 for lower cavity temperatures) and controlled bleed-off flow (.77627). The second factor receives important weightings from bleed-off cavity and upper seal cavity pressures (.21745 and .18071, respectively) and controlled bleed-off flow (.22262). The largest loading is, however, contributed by lower oil level (.46848). The Varimax rotation for Pump 2B2 does not change the total variance explained, but does shift the relative contributions of the two factors. The relative contribution of Factor 1 declines to 53.16%, while the contribution of Factor 2 increases dramatically to 46.83%. Again, the first factor is heavily loaded by temperature variables (upper bearing .75766, downward bearing .72118, and lower cavity temperatures), while the second factor reveals a very disparate pattern. The largest loading for the second factor is lower oil (.66706), followed by lower cavity temperature (.52240), and controlled bleed-off flow (.68524). The fact that both lower cavity temperature and controlled bleed-off flow have positive loadings in both factors makes it very difficult to come up with a sensible physical explanation for the Varimax model of Pump 2B2.

Table 1. Factor Pattern.

	Factor 1	Factor 2	
LOL2B2	0.47655	0.46848	Lower Oil Level 2B2
UBT2B2	0.72351	–0.32907	Upper Bearing Temperature 2B2
DBT2B2	0.64007	–0.36712	Downward Bearing Temperature 2B2
LCT2B2	0.69156	0.07974	Lower Cavity Temperature 2B2
BCB2B2	–0.12911	0.21745	Bleed-Off Cavity Pressure 2B2
USCP2B2	–0.07116	0.18021	Upper Seal Cavity Pressure 2B2
MSCP2B2	–0.36976	–0.10501	Middle Seal Cavity Pressure 2B2
CBF2B2	0.77627	0.22262	Controlled Bleed-Off Flow 2B2
V2B21	0.44388	–0.05079	Vibration 2B2-1
V2B22	0.18299	0.11379	Vibration 2B2-2

Variance Explained by Each Factor

Factor 1	Factor 2
2.630082	0.624767

4.0 Communalities Across Pumps (First Run)

Communalities are, in effect, the proportion which each individual variable contributes to total system variance. Communalities are a weaker indicator than R-square because individual communalities are apportioned between the various factors and, therefore, cannot be used directly to account for the proportion of statistically significant variation due to any particular variable. However, it still is interesting to rank order communalities across pumps to discover whether there is a consistent pattern across pumps. For a normal variable, the sum of the variances must equal one. Therefore, it is possible to use the eigenvalues of the final communality estimates to apportion the percentage of system variance for each variable. These values are not disturbed by the Varimax rotation procedure (see Table 2).

Table 2. Average of Communalities of Four Pumps (First Run).

Rank Order	Variable	% Contribution to Variance
1.	Upper Thrust Bearing Temperature	.1983
2.	Downward Thrust Bearing Temperature	.1781
3.	Lower Cavity	.1469
4.	Controlled Bleed-Off	.1274
5.	Lower Oil Level	.0744
6.	Upper Oil Level	.0642
7.	Middle Seal Pressure	.0594
8.	Upper Seal Pressure	.0434
9.	Vibration 1	.0400
10.	Bleed-Off Cavity	.0362
11.	Vibration 2	.0303

These communalities indicate a fairly consistent pattern across pumps in which the temperature-related variables account for over 50% of explained variance (52.33%). These are also the variables which loom large in the first factor with heavy loadings.

5.0 Principal Factor Analysis of Pump 2B2 (Second Run)

The pattern of temperature dominance is repeated for Pump 2B2 (see Table 3). The single factor accounts for virtually 100% of explained variance. Heavy loadings to the single factor are contributed by upper bearing (.78594), downward bearing (.70632), and lower cavity temperatures (0.62014). The pressure variables have negative loadings, while only vibration measure one has a significant positive loading (.47529).

Table 3. Factor Pattern.

	Factor 1	
UBT2B2	0.78594	Upper Bearing Temperature 2B2
DBT2B2	0.70632	Downward Bearing Temperature 2B2
LCT2B2	0.62014	Lower Cavity Temperature 2B2
BCB2B2	–0.24721	Bleed-Off Cavity Pressure 2B2
USCP2B2	–0.00103	Upper Seal Cavity Pressure 2B2
MSCP2B2	–0.28811	Middle Seal Cavity Pressure 2B2
V2B2-1	0.47529	Vibration 2B2-1
V2B2-2	0.18498	Vibration 2B2-2

Variance Explained by Each Factor

Factor 1
1.905402

6.0 Principal Factor Analysis of Pump 2B2 (Third Run)

In the case of Pump 2B2, the single factor model is confirmed (see Table 4). The single factor model accounts for 100% of explained variance. Once again, the single factor is dominated by heavy loadings from temperature-related variables: upper bearing (.83268), downward bearing (.75792), and lower cavity (.72834) temperatures. The pressure-related variables have either negative coefficients or small positive factor loadings. Again, no Varimax rotation was possible with one factor.

Table 4. Factor Pattern.

	Factor 1	
UBT2B2	0.83268	Upper Bearing Temperature 2B2
DBT2B2	0.75792	Downward Bearing Temperature 2B2
LCT2B2	0.72834	Lower Cavity Temperature 2B2
BCB2B2	–0.28740	Bleed-Off Cavity Pressure 2B2
USCP2B2	0.05267	Upper Seal Cavity Pressure 2B2
MSCP2B2	–0.41279	Middle Seal Cavity Pressure 2B2
V2B2-1	0.57577	Vibration 2B2-1
V2B2-2	0.16120	Vibration 2B2-2

Variance Explained by Each Factor

Factor 1
2.411546

7.0 Summary of Three Principal Factor Runs

The third run used the entire 121-day data base for eight variables. Controlled bleed-off flow and oil level indicators were excluded based upon the good modeling results of the second run. The powerful impact of

temperature variables on system performance is demonstrated by the consistency between the three factor runs. In some ways the third run was the most important demonstration of the importance of the temperature variables as it was based upon all values in the data base. In the third run, as well, in three of the four pumps only one factor, the temperature factor, was required to explain 100% of explained variance. The rank order of the temperature variables was similar to the second run in terms of relative factor loadings (see Table 5):

Table 5. Contribution of Top Three Variables to First (or Single) Factor Loadings

Pump 2A1		Pump 2A2		Pump 2B1		Pump 2B2	
Upper	.88744	Upper	.85499	Upper	.82652	Upper	.82667
Down	.88365	Down	.83031	Down	.74022	Lower	.82646
Lower	.77448	Lower	.61465	Lower	.69452	Down	.65398

These loadings are far more consistent than those of the second run: upper bearing temperature has the highest factor loadings for all four pumps while downward bearing temperature is second for all pumps but Pump 2B2. Lower cavity temperature is third in rank except for Pump 2B2.

The rank order of communalities for the three runs is presented in Table 6.

Table 6. Average Communalities of RCP Pumps.

First Run			Second Run			Third Run		
1. Upper Bearing	19.83	>52.33	1. Upper Bearing	29.25	>76.76	1. Upper Bearing	28.97	>79.37
2. Downward Bearing	17.81		2. Downward Bearing	27.38		2. Downward Bearing	26.63	
3. Lower Cavity	14.69		3. Lower Cavity	20.13		3. Lower Cavity	23.77	
4. Controlled Bleed-Off	12.74		4. Vibration 1	5.67		4. Vibration 1	6.95	
5. Level Oil	7.44		5. Middle Seal	5.57		5. Middle Seal	6.91	
6. Upper Oil	6.42		6. Vibration 2	5.02		6. Upper Oil	4.67	
7. Middle Seal	5.94		7. Bleed-Off	3.96		7. Bleed-Off	4.05	
8. Upper Seal	4.34		8. Upper Seal	2.67		8. Vibration 2	2.72	
9. Vibration 1	4.00							
10. Bleed-Off	3.62							
11. Vibration	3.03							

Amazingly, the second and third runs rank order the variables identically except for the swapping of places between Vibration Indicator 2 and upper seal cavity pressure. In the second run using variable values within two sigma ranges, the top three variables account for 76.76% of explained variance while using the entire data base this percentage increases to 79.37%. In other words, using outlier values, the explanatory power of the top three variables is only increased. This is an important finding for it means that factor analysis could be utilized to predict RCP System behavior even in extreme system states. In any case, principal factor analysis permits ranking of all system variables in a consistent fashion. This permits the analyst or operator to focus his attention on those parameters which contribute the largest proportion of explained variance. Principal factor analysis thus achieves what defeated both regression and principal components analysis.

8.0 Summary of Factor Analysis

Both the principal factor and maximum likelihood methods produced a self-consistent pattern which is compatible with a basic thermodynamic understanding of the RCP System. It was not possible, using either

regression analysis or principal components, to rank order RCP System variables or to develop a consistent statistical model of underlying physical processes.

When the oil level indicators and Controlled Bleed-Off Flow were excluded from analysis, both principal factor and maximum likelihood methods reduced the dimensionality of the problem to one factor: temperature. In the case of every pump for both methods, the very same three variables accounted for heavy factor loadings as well as contributed a large proportion to explained variance (see Table 7).

Table 7. Contribution of Top Three Variables to Communality (Percent) (Upper Bearing, Lower Bearing, Lower Cavity Temperatures). Comparing Principal Factor (PF) and Maximum Likelihood (ML) Methods.

	PF	ML[6]
2A1	70.42	83.93
2A2	71.23	73.35
2B1	87.83	90.28
2B2	78.78	82.69
Average	77.07	82.56

In no case was the percentage attributed to the top three variables less than 70 percent for either method. Maximum likelihood, which is the method with the stronger analytic foundation, attributed, on average, a marginally higher proportion of variance to the temperature variables (82.56 percent versus 77.07 percent). These results provide a powerful tool for rank ordering the variables within the RCP System for decision analysis by statistical importance for safety monitoring. In effect, with only one factor dominated by temperature variables, the decision maker could focus upon the top three variables for each pump and lose only 20 percent of statistically significant information provided by the other variables. In effect, one could reduce the dimensionality of the problem from 44 to 12 parameters. If one includes the four indicators of the Component Cooling Water (CCW) System, total dimensionality is reduced from 48 to 16 parameters, a reduction of 66 percent. For decision analysis, it would then only be necessary to maintain quality control charts (X-Bar, R, and CUSUM) for the top three temperature variables and the four indicators of the CCW System rather than for all 48 variables. The results of factor analysis are also consistent with and reinforce the results of the regression analysis on the relationship between the RCP and CCW Systems. These results will be analyzed in further studies. Suffice it to say that the CCW variables are good predictors of the top three RCP variables. Thus, both factor analysis and regression analysis establish temperature-related variables as key predictors of system performance.

If the methodology outlined here were applied systematically to all plant's systems ranked according to their contribution to unit downtime, it would be possible to reduce the tracking of variables by 75% (from roughly 4,000 variables to 1,000). This enormous reduction in dimensionality would considerably simplify the application of statistical process control modeling to nuclear power plant management. Equally, it would be possible to identify system degradation in real time and apply this knowledge to Reliability Centered Maintenance (RCM) programs and to link statistical modeling to existing predictive maintenance programs.[7]

The authors wish to thank Dr. John F. Brenner, Director, Image Analysis Laboratory, New England Medical Center, for his moral and material support of this project. Without his generous donation of computer support this paper would have been considerably delayed. Analysis of the database was performed on a VAX 11/780 using SAS®. SAS is the registered trademark of the SAS Institute Inc., Cary, North Carolina.

[6]Grenzebach, Heising, Marx, "Maximum Likelihood Factor Analysis of the Reactor Coolant Pump System," *op. cit.*

[7]R. J. Colsher (EPRI), W. J. Leonard (PECO), James J. Hlebik (Leeds and Northrup), and John R. Scheibel (EPRI), "A Method of Combining Many Diagnostic Monitors Into One Integrated System," Unpublished Essay; EPRI Technical Brief, RP 1864-1, 2338-1, "Automated Remote Monitoring System"; EPRI Results, RP 1864-1, 2338-1, "PG&E Uses Automated Remote Monitoring System to Track Critical Equipment at Several Plants," December 1988.

FLOWSIM/FLOWRISK: A CODE SYSTEM FOR STUDYING RISK ASSOCIATED WITH MATERIAL PROCESS FLOWS*

Alfred M. Kaufman

Lawrence Livermore National Laboratory
P.O. Box 808, L-85
Livermore, CA 94551

INTRODUCTION

The need to study and assess life-cycle risks of Pu release by nuclear warheads during peace time lead to the development of a code suite which could model day to day operations involving nuclear weapons and calculate the associated risk involved in these proceedings. The life-cycle study called LIONSHARE is described in Reference 1. The code that models the flow is called FlowSim. The code that evaluates the associated risk is called FlowRisk. The flow chart in Fig. 1 illustrates the relationship of these codes.

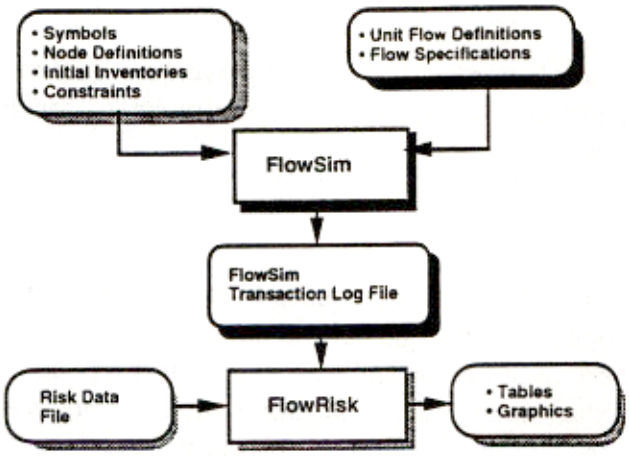


Figure 1. FlowSim/Flow Risk is a code system designed for risk analysis of material flows.

We shall concentrate here on the methodology used by FlowSim in modeling material flows. FlowRisk, mainly a postprocessor of FlowSim runs, will be dealt with in less detail.

* Work performed by Lawrence Livermore National Laboratory under the auspices of the U.S. Department of Energy under contract number W-7405-ENG-48s.

THE FLOWSIM PARADIGM

The FlowSim universe is characterized by material inventory populating a set of states called nodes. A state, depending on the application, can be interpreted as a physical location. The dynamics of this universe consist of a set of inventory transactions which take specified intervals of time to complete. There are two basic transaction types: *material transfer* between nodes and *material transformation* at a node. Inventory transfer between nodes is the model for material flow. Inventory transformation is the model for material processing.

The nodes, inventories, flows and processes are defined at run time using a special input language. Definitions are sufficiently general to allow definition of almost any flow problem of interest. Figure 2 illustrates the elements required to specify a generic problem.

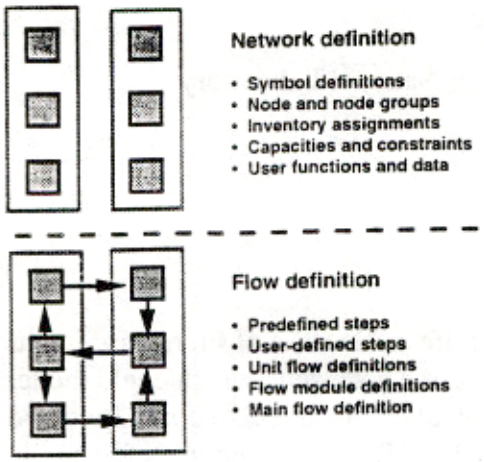


Figure 2. Elements for FlowSim problem definition are specified on input. The elements are a description of the network and a description of the flows.

FlowSim has been implemented as an event driven simulation using *Mathematica.*[2] The *Mathematica* programming paradigm is especially suited for dealing with symbolic entities such as inventories.

Network Definition

The FlowSim network definition introduces inventory symbols, nodes, node groups, inventories, inventory constraints and specialized data.

Inventory symbols come in two varieties: unit symbols and container symbols. A unit symbol represents an irreducible quantity in the simulation. A container symbol is employed in circumstances where packaging of a unit may be important; e.g. **"passenger"** may be a unit symbol, **"auto"** may be a container symbol. FlowSim then uses the construct: **"auto"[4*"passenger"]** to represent a complex entity of an auto containing four passengers.

Nodes are represented hierarchically. They are designated by path names Thus, the path designation **"US:California:San Francisco:Golden Gate Park"** could be a node in FlowSim. The path **"US:California:San Francisco"** represents a node group that contains **"US:California:San Francisco:Golden Gate Park"** as a node. The entire set of nodes and node groups form a tree-like structure in FlowSim.

Initial **Inventories**, constraints on inventory amounts and limits on number of simultaneous active processes are assigned to nodes at run time. Inventories of **Assets**

required for the completion of certain processes are associated to nodes and node groups as well.

Flow Definition

In FlowSim, flows are built up hierarchically from a set of elementary predefined steps. Aggregations of predefined steps, called **user-defined steps,** can be defined and symbolically referenced by the user as well.

A unit flow is defined as a set of steps that operate initially on specified inventory at a specified node. The inventory upon which the flow will operate is tagged so as to associate it with the flow. The tag protects this inventory so that steps belonging to other unit flows cannot operate on it. The steps in the unit flow are sequential. At the completion of the unit flow the inventory tag is released.

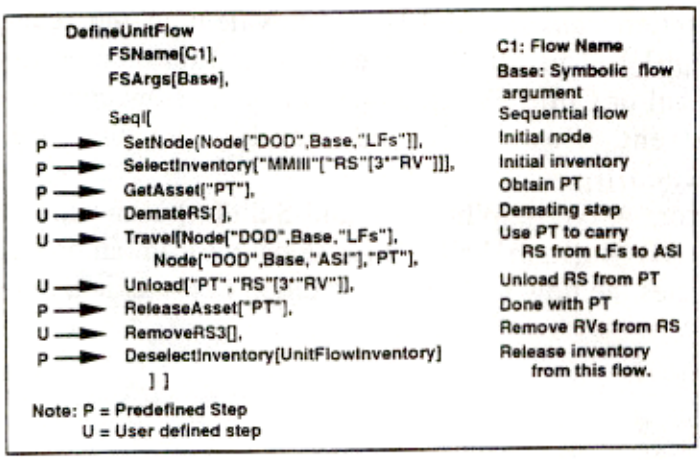


Figure 3. The anatomy of a unit flow definition in FlowSim. Unit flows are built from a sequence of predefined and user-defined steps.

Figure 3 shows the construction of a unit flow in a recent weapon safety assessment. The flow simulates the removal of a Reentry System (RS) from a Minuteman III missile, and transportation of the RS to an AS&I building. The three RVs are removed in the AS&I building and subsequently stored at a facility called an Igloo.

A flow module as well as the main flow is defined by aggregating unit flows. FlowSim has several flow constructors as outlined in Fig. 4.

The flow constructors **Seql[ ]** and **Conc[ ]** are all that are needed to describe the relationship among an arbitrary set of flows. The flow **Seql[f,g,h]** is interpreted as a sequential set of flows **f, g,** and **h** in which a predecessor must terminate before a successor can begin. The flow **Conc[f,g,h]** is interpreted as a **concurrent** set of flows **f, g,** and **h** in which all begin concurrently upon initiation of the main flow. The termination of the flow defined by either **Seql[ ]** or **Conc[ ]** is signaled by the condition that all have terminated.

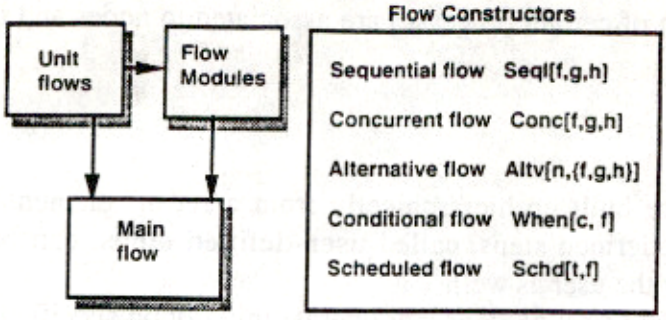


Figure 4. Flow constructors are used to aggregate flows. *Seql* is used to define flows that must follow one another and is the constructor used in building unit flows from steps. *Conc* is used to define flows that occur concurrently. *Altv* is used to select from among several flows. *When* is used to initiate flow when some condition is met. *Schd* initiates a flow at a predefined time.

The additional notation ***const*[n,{f,g,h}]** is equivalent to the recursive definition ***const*[f,g,h,*const*[n-1,{f,gh}]]**. This allows for easy definition of repetitive flows where ***const*** stands for either **Seql** or **Conc**. For example, the main flow comprising the flow **c1** followed by concurrent flows **c2**, **c3**, and **c3** can be written as **Seql[c1,Conc[c2,Conc[2,{c3}]]]**

The other constructors **Altv[ ]**, **When[ ]**, and **Schd[ ]** allow for control of flows. Using the parameter **n**, **Altv[n,{f,g,h}]** allows for selection from among alternative flows **f,g, or h**. **When[c,f]** initiates the flow **f** *when* the condition **c** is satisfied. **Schd[t,f]** schedules the flow **f** at time **t**.

Flow Management

FlowSim manages all flows with a time-ordered event stack which stores process initiation and process termination events. The current simulation time is set by the time of the latest executed event. The stack is therefore naturally divided by the current simulation time. Events whose time stamp precede the current simulation time are in a wait state. They will execute when some condition upon which they wait is satisfied. The remaining events are expected to be executed at the simulation future. The events in the wait state are polled each time a process termination event that is also the termination of a predefined step is encountered. Only such a step can change a condition upon which initiation of a flow might depend. Figure 5 illustrates event stack operation.

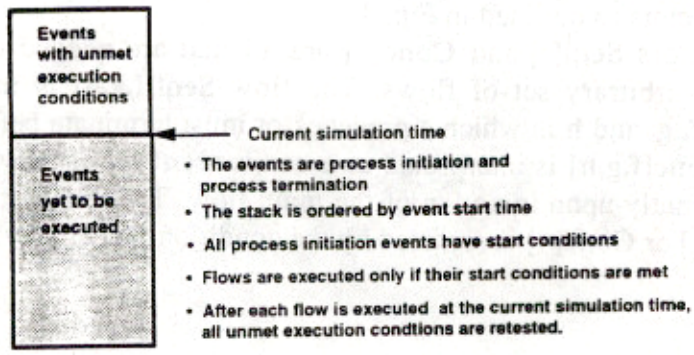


Figure 5. FlowSim has an event stack that manages the flows.

By itself, the event stack is not sufficient to manage the flows being simulated by FlowSim. A supporting data structure is also required. The data structure is a tree in which a node corresponds to a flow and the branches correspond to subsidiary flows. Each flow has a status designator which has the values Waiting, Active or Complete. The Waiting state is assigned to flows which are queued with unsatisfied conditions. The Active state designates flows in progress. The Complete state indicates that the data structure supporting the flow is no longer needed. Obviously, the Complete state for a parent flow is set by completion of all of its children. The time required for completion of a given flow can thus depend, in a very nonlinear way, on the times to completion of each of its subsidiary flows.

Figure 6 shows a sample FlowSim simulation log file which recounts the changes of state and activities associated with the simulation. The simulation log file contains a preamble that describes symbols and nodes used in the simulation and a body in which flow activities are recounted. The flow activities contain **NewInventory**, **NewActivity** and **EndActivity** messages. A **NewInventory** message is generated by a change in inventory at any simulation node. **NewActivity** and **EndActivity** messages are user defined and are used as the link to FlowRisk.

```
MMIIIRetro.01.93.04.25                                          Preamble
UnitSymbolList["RV"]
ContainerSymbolList["RS","PT",MMIII"]
NodeSymbolList["DOD:Min:Igloos","DOD:Min:LFs","DOD:Min:ASI"]

NewInventory[0.,"DOD:Min:Igloos", 10""RV"]                      FlowMessages
NweInventory[0.,"DOD:Min:LFs",150""MMIII["RS"[3""RV"]]]
NewInventory[0.,NewInventory[0.,"DOD:Min:ASI",0.]
NewInventory[0.,"DOD:Min:LFs",150""MMIII["RS"[3""RV"]]+"PT"[ ]]
NewActivity   [0.,"DemateRS",1,"DOD:Min:LFs",150""MMIII["RS"[3""RV"]]+"PT"[ ]]
NewInventory[1.,"DOD:Min:LFs",MMIII[ ] + 149""MMIII"["RS"[3""RV"]] +
              "PT"["RS"[3""RV"] ]]
EndActivity   [1.,"DemateRS"]
NewActivity   [1.,"PT Travel",2,"DOD:Min:LFs","PT"["RS"[3""RV"]]]
NewInventory[1.06,"DOD:Min:LFs","MMIII"[ ] + 149""MMIII"["RS"[3""RV"]]]
NewInventory[1.06,"DOD:Min:ASI","PT"["RS"[3""RV"]]]
```

Figure 6. The FlowSim Simulation Log File contains messages for use by FlowRisk in its postprocessing risk analysis run.

FLOW RISK

FlowRisk is the postprocessor of the FlowSim **simulation log file**. Risks per operation, risk rates keyed to the nodes, inventory, and activities modeled in the FlowSim simulation are incorporated in a risk data file. FlowRisk merges this information with the simulation log file to produce a time history of cumulated risk and risk rate for the simulation. This information is displayed graphically. It can show risks associated with a particular simulation node, or group of nodes, as well as the entire node network. Figure 7 shows the relationships just described.

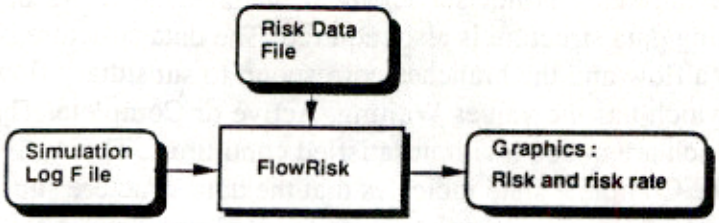


Figure 7. FlowRisk is a postprocessor of the simulation log file. It incorporates risk data found on a risk data file to produce graphical output of cumulative risk and risk rate.

The Future of FlowSim

FlowSim has shown the ability to simulate arbitrary flows of material. It has been employed successfully in weapon safety analysis where, heretofore, average weapon risk models have been used. The code may also be useful in logistic simulations and manufacturing operational problems.

Future developments of FlowSim will focus on speeding up the code. It is presently written in *Mathematica*, which is an interpretive language. Parts of the code could be written in C and linked to *Mathematica* by using MathLink, a protocol for transferring information and C programs..

REFERENCES

1. Park Winter, "LIONSHARE," forthcoming.

2. Stephen Wolfram, "Mathematica, A System for Doing Mathematics by Computer," 2nd ed, Addison-Wesley, 1991.

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)

A NEW APPROACH TO THE UNCERTAINTY EVALUATION IN RISK ASSESSMENT

P.Cecchella and M.Mazzini

Dipartimento di Costruzioni Meccaniche e Nucleari , University of Pisa
Pisa, 56126 Italy

INTRODUCTION

In the past years, various informatic tools have been set-up for risk assessment in industrial activities. One of the main problems in this field, yet subject of research, is the treatment of uncertainty of the models used for the evaluation of the accident probability or of the area in which given consequences occur.

The uncertainty of risk assessment models is connected to the limits of the physico-mathematical models used for describing the phenomena, to the poor knowledge of the boundary conditions and, at the end, to the same nature of the problem: in fact the studied phenomena involve stochastic aspects. For this reason the problem cannot be analysed in deterministic terms, but one should consider the various parameters entering in the model with their true probabilistic distribution function (pdf).

The uncertainty of risk assessment for an industrial plant may be determined by different methods. The first methodology uses directly the pdf of the various input parameters. Inserting these directly in the equations of the model, one obtains the exact pdf of the output (Damsleth, 1990). A second method is based on the principle of the Montecarlo procedure: various calculations are performed, in number sufficient to derive an approximate form of the output pdf (Buslenko et al., 1966). A third methodology is based on the experimental design to reduce the number of needed calculation runs, without loosing the representativeness of the model response. This is very useful in complex cases to assess the relative importance of the various parameters. Using also the response surface methodology, it is possible to obtain a mathematical approximation of the output as a function of the input parameters (Cortese et al., 1989) . Finally, the use of orthogonal experimental matrices allows to reduce at minimum the number of runs sufficient to describe the possible combinations between the input parameters (Cecchella et al., 1993).

The paper discusses a little different approach to the evaluation of uncertainty propagation in the risk assessment of industrial accidents. The goal is achieved again by the application of the experimental design based on the orthogonal matrix; then a random statistical (Montecarlo) procedure allows a better resolution of the results. The first step constitutes a preliminary sensitivity analysis which allows to distinguish the input parameters into two categories: the

first category includes the parameters which play an essential role in the code, the second all others. In this way, a good description of the pdf is necessary only for the parameters of the first category. This overcomes the main problem in the use of the Montecarlo procedure, i.e. the difficulty to perform a very height number of runs for describing the pdf of all input parameters with sufficient precision.

As an example, the proposed methodology is applied to an ammonia release scenario.

THE METHODOLOGY

As already mentioned, the proposed methodology consist of the following steps: (1) a sensitivity analysis of the code in order to select the variables which have the main influence on the response. This is performed by the application of the experimental design, based on orthogonal matrices; (2) random generation of the input arrays to the code, according to the adopted pdf; (3) drawing of the uncertainty histogram of the response and statistical analysis of the results.

The Sensitivity Analysis

The general form which may be used to describe an experimental matrix with m experiments is shown by the relationship:

$$\begin{bmatrix} y_1 \\ y_2 \\ \cdot \\ y_m \end{bmatrix} = f \begin{bmatrix} x_{1,1} & x_{1,2} & \cdot & x_{1,n} \\ x_{2,1} & x_{2,2} & \cdot & x_{2,n} \\ \cdot & \cdot & \cdot & \cdot \\ x_{m,1} & x_{m,2} & \cdot & x_{m,n} \end{bmatrix} \tag{1}$$

where the generic row of the matrix $[x_{k,1}, x_{k,2},..,x_{k,n}]$ is the k-th input, f is the transformation function (representative of the computer code implementing the model) and y_k is the corresponding k-th value of the output. In our case each parameter x is described by a limited number of levels (L) which represent with enough approximation the real distribution of this parameter.

In first approximation we can write the relationship (1) as:

$$y_j = \mu + \sum_{i=1}^{n} \xi_{k,i} + \varepsilon \tag{2}$$

where μ is the mean of the observed values of y in the region defined by the experimental matrix, $\xi_{k,i}$ is the deviation from μ caused by setting the i-th variable with the value of k level end ε is the error associated to the linear approximation. Introducing the mean effect factor, defined as:

$$m_{k,i} = \frac{1}{z} \sum_{j=1}^{z} y_j \tag{3}$$

were z is the number of observations in which the k value of i-th variable is present and substituting in the equations (2) and (1) (Cecchella et al., 1993), $m_{k,i}$ can be considered an index of the effect of the i-th variable at the k level on the mean μ.

If we use the orthogonal arrays in the experimental matrix (Phadke, 1989) we can demonstrate that the variance of the error term is given by the relationship (Scheffé, 1971):

$$E = \sum_{j=1}^{m} \left(y_j - \mu\right)^2 - \sum_{i=1}^{n} \left[L \sum_{k=1}^{L} \left(m_{k,i} - \mu\right)^2 \right] \qquad (4)$$

where L is the number of levels for the i-th variable.

The equations (2) and (4) permit to evaluate the level of significance (terms $m_{k,i}$) of all input variables of the model and the error due to the linear approximation.

The Random Procedure

The parameters which play a fundamental role in the code are randomised by a procedure which takes into account the exact pdf of these variables, using a large experimental matrix (10^3 rows for each important variable). On the contrary, the variables with a limited level of significance can be analysed with an approximation of the real distribution or fixed to the nominal values (if $m_{k,i}$ is very small). In this way the number of runs is reduced with respect to a complete Montecarlo procedure, without loosing to much information.

The random procedure consists in a random generator, which for any variable determines for each run a casual value, taking into account its pdf. In general terms, a random generator may be implemented in tree different manners: (1) analytic, in which the random number α_i is formed from the preceding one α_{i-1} by applying a mathematical algorithm (Sobol, 1958) (2) using a special apparatus on the computer, which transforms the results of a random physical process (Sterzer, 1958); (3) using a table of uniformly distributed random numbers (Sobol, 1975). We used the first type of random generators

THE STUDY CASE

For the first application of the methodology discussed we choose the evaluation of the uncertainty, due to source term and more important meteorological parameters of the consequences of an ammonia release. The accident scenario is that considered in the benchmark exercise in risk assessment, recently organised by the European Community (Amendola et al., 1992).

In particular the release of ammonia occur from a pressurized tank (98% liquid phase) with a capacity of 233 m^3, a mass inventory of about $6 \cdot 10^4$ Kg at pressure of 1.3 MPa and temperature of 293 K. The release brings to the formation of a poll under the storage tank, with an area of 300 m^3, limited by the containment walls. According to the various participant to the benchmark exercise, the flowrate outcoming from the tank is comprised between 10 and 90 Kg/s. The source term is determined by various contributions: the first is given by the gas flowing out from the break due to the adiabatic expansion of the vessel content (2% of the total flowrate); others are due to the evaporation from the pool because of the surface heat, of solar radiation and of convective heat transfer from the atmosphere.

The characteristics of airborne ammonia can be that of a neutral o heavy gas, depending by the release conditions. With the assumptions made, in our case, it can be considered a neutral gas. To estimate the ammonia concentrations downwind, the dispersion model adopted is the Industrial Source Complex Short Term (ISCST), set-up by the US Environmental Protection Agency (Wagner, 1988). It is a gaussian model and considers multipoint, linear, area or volume sources of neutral and buoyant airborne emissions. In conclusion our analysis refers to the evaluation of the uncertainty in the ammonia concentration averaged on a time interval of 1h, along the bisector line of the sector in which the wind is blowing.

According with the data used in the benchmark exercise, Table 1 shows the main input parameters used in the simulation. For the sensitivity analysis we considered 5 levels for each variable around the mean value. Figure 1 shows the assumed pdf of the input parameters in stability class D. Analogous set of data were used for the other stability classes (with the notice that the pdf of the mixing height is assumed uniform for classes A and C).

The sensitivity analysis carried out by the ISCST code gave the results shown in Figure 2. The preponderance of the wind direction in all classes is evident, with the exception of class A; in this class the relevant parameters are the wind speed and the mixing height. All other variables play a minor role in the output of ISCST code and can be inserted in the second category of importance. These less important quantities are considered with a simplified pdf with a standard deviation so that the limit of confidence of 5% correspond to the minimum values of these variables. For solar radiation and break flowrate with nominal value are assumed. In general, the wind direction is described by a wind rose at 16 directions. In this way, all directions belonging to a sector of $\pi/8$ are associated to the related bisector; the uncertainty is $\pm\pi/16$ and is uniformly distributed on this interval. The effect of this uncertainty was studied by the Montecarlo procedure considering 1000 runs for each stability class, apart from class A for which we performed 2500 runs to assess the effect of wind speed and mixing height.

Table 1. Meteorological parameters

Pasquill stability class	A	C	D	F
Mean wind speed (m/s)	2	3.5	6	2
Mean mixing height (m)	300	700	1380	-
Mean air temperature (K)	298	303	293	288
Mean solar radiation (W/m2)	750	600	400	0

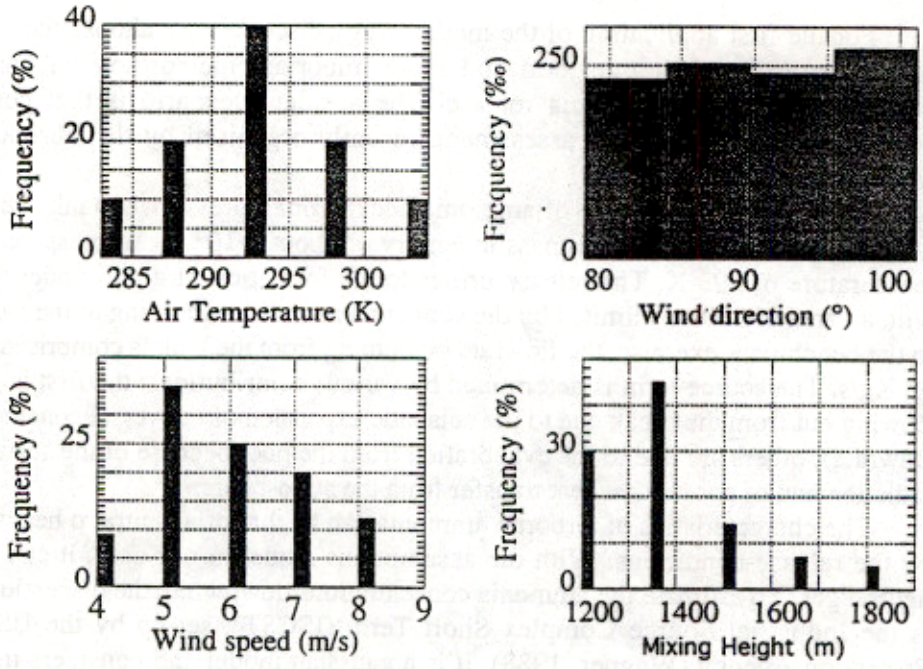


FIGURE 1. PDF of the examined parameters in stability class D.
(for the parameter wind direction, 90° is the receptor axis direction in ISCST code).

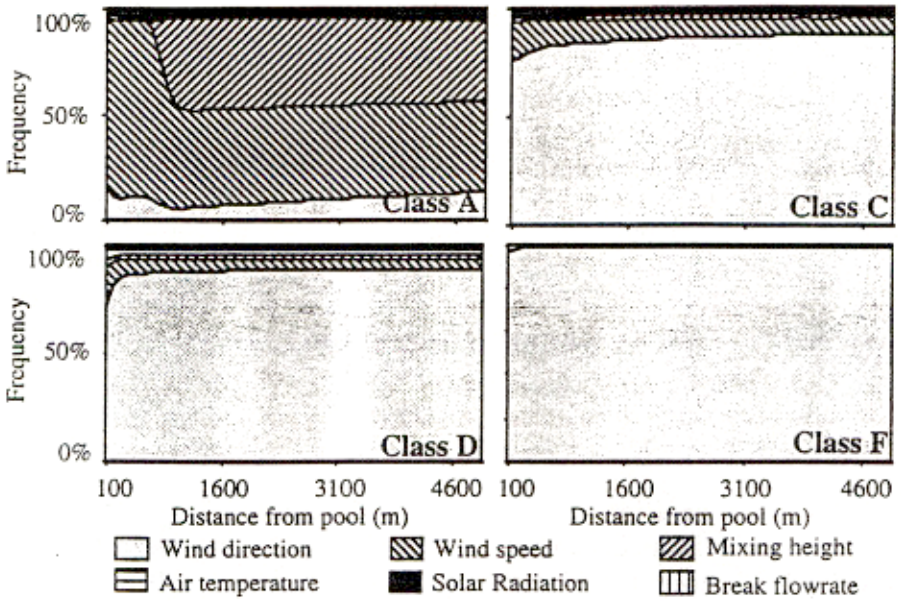


FIGURE 2 Sensitivity analysis of ISCST code.

Analysis of the Results

Figure 3 shows the pdf of the ammonia concentration at 1 Km from the pool centre in the various stability classes. The total range of ammonia concentrations varies from 2 g/m^3 to zero. The major contribution to the total uncertainty is due to the stability class F. In fact, in the other atmospheric stability classes, the variation range is lower, being less than an order of magnitude in class A and a little more in classes C and D. These results confirm those obtained without applying the Montecarlo procedure (Cecchella et al., 1993).

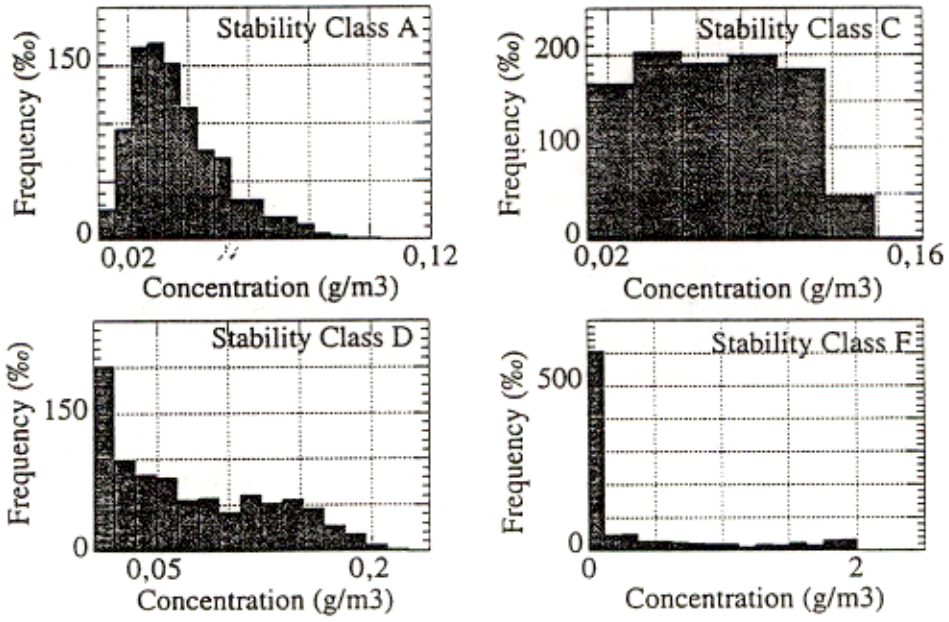


FIGURE 3 Pdf of NH3 concentration at 1000 m from the pool center for the various stability classes.

The large range of uncertainty related to the variation of the wind direction in class F needs further discussion. The ammonia concentration goes practically to zero at all the distances from poll centre for a small change of wind direction because the form of plume is very narrow. However, from the practical point of view these uncertainty does not preclude any conclusion considering the risk area. In general terms, the risk area is the area in which a specific dangerous value is exceeded. If we fix this value at the level of 0.35 g/m3 (Graziani, 1991) the results show an uncertainty in the risk area of a few hundred of meters for the classes A, C and D. For class F, this can arrive at about 3000 m, but in the form of a very narrow ellipse. It is sufficient to evacuate people in direction orthogonal to the wind direction at low speed (walking) to reduce the consequences about to zero.

CONCLUSIONS

A first conclusion concerns the applied methodology. The height resolution of the results with a rather limited number of runs ($5{,}5 \cdot 10^3$), with respect to the classic Montecarlo procedure, is encouraging. However, its application is realistic only for small codes, which have a limited running time. The simulation of the discussed study case on a PC of 386 class required about 5 hours of CPU. A larger future field of applications could be assured to the methodology by the more powerful computers (i.e. workstations) now in common operation.

A second conclusion can be drawn about the uncertainty in the evaluation of risk of ammonia releases. The results show that most of the uncertainty derives from the uncertainties in stability class and wind direction. In particular, in stability class F, a wind rose at 16 directions is insufficient to describe the plume dispersion. However, if the analysis is performed for an uniform distribution of people around the industrial activity, the wind direction is not longer relevant and only the stability class plays a decisive role.

Finally, it has to be emphasised that to have a complete scenario of an accidental ammonia release is necessary to apply the methodology whit a model for heavy gas plumes. In fact the choice of the model is already cause of uncertainty for this type of releases

REFERENCES

Amendola A., S.Contini and I.Ziomas, Uncertainties in Chemical Risk Assessment: Results of a European Benchmark Exercise, J.Hazardous Materials, 29, 347:363.

Buslenko N.P., D.I.Golenko, Yu.A.Shreider, I.M.Sobol and V.G.Sragovich, 1966, "The Monte Carlo Method", Pergamon Press, New York.

Cacchella P. And M.Mazzini, 1993, A Statistical Method for Uncertainty Analysis of Risk Assessment, Fourth Conference SRA Europe, Roma.

Cortese R., M.Mazzini and G.Volta, 1989, A New Approach for the Analysis of Sensitivity and Uncertainty on LWRs PRAs, Based on Response Surface Methodology, Proceedings Int. Meet. PSA '89, Pittsburgh.

Damsleth E., 1990, MANIP - A Program to Perform Calculation on Statistical Defined Variables, HYDRO Research Centre, Oslo.

Graziani R., L.Lepore, U.Poli and M.Villarini, Metodo per l'Analisi e la Valutazione delle conseguenze di Eventi Incidentali Connessi a Determinate Attività Industriali, ISPESL DIPIA-np1040, Roma.

Phadke M.S., 1989, "Quality Engineering Using Robust Design", Prentice Hall, New Jersey.

Scheffé H., 1971, "Analysis of Variance, John Wiley & Sons, New York.

Sobol I.M., 1958, Pseudo-Random Numbers for the Strela Computer, Teorija Verojatn. I Yeje Primen., 3, 205-211.

Sobol I.M., 1975, "The Monte Carlo Method", MIR Publisher, Moscow.

Sterzer, 1958, Random Number Generator Using Subarmonic Oscillator, Rev. Scient. Instr., 30, 241-243.

Wagner C.P., 1988, Industrial Source Complex Dispersion Model, EPOA PB88-171475, Springfield.

USES OF ZERO-ONE SAMPLING IN PROBABILISTIC RISK ASSESSMENT*

Allen L. Camp

Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185

INTRODUCTION AND BACKGROUND

The recent NUREG-1150 studies and the LaSalle Probabilistic Risk Assessment (PRA) include the most in-depth uncertainty analyses ever performed for commercial nuclear reactors.[1,2,3] As a result, the methods used in these studies are often emulated and referenced as being the definitive approach for performing such uncertainty analyses. While the methods are believed to be robust and to reasonably reflect the magnitude of the uncertainties, it is important for future users of these methods to understand some of the subtle points of the analysis. In particular, zero-one sampling (ZOS) was a technique employed extensively in these studies. The purpose of this paper is to clarify the actual use of zero-one sampling in NUREG-1150 and discuss more precisely those applications for which zero-one sampling is appropriate.

PROBABILITIES AND FREQUENCIES

ZOS cannot be discussed without first understanding the meaning of the PRA models and the manner in which they are formulated. The discussions in this paper assume that the PRA model is based on a "probability of frequency" formulation. This concept was first introduced in Reference 4 and has undergone much discussion and interpretation in the years since. While not universally approved, it is the most commonly used approach. Using the probability of frequency interpretation, "frequency" refers to the outcome of an experiment involving repeated trials, even if the experiment is only a

*This work is supported by the U.S. Nuclear Regulatory Commission and is performed at Sandia National Laboratories, which is operated for the U.S. Department of Energy under Contract Number DE-AC04-94AL85000.

thought experiment. Frequency, therefore, represents a measurable number. "Probability" is a numerical measure of a state of knowledge, a degree of belief, or a state of confidence. Probability is considered to be a subjective term, while frequency is more of an objective concept. It must be noted that "frequency" is used very loosely as a statistical term in this context; it is simply another view of probability. In the context of a PRA, we use frequencies to estimate such things as hardware failure rates or human error rates and use probabilities to reflect our confidence in a particular value of the frequency.

The reader should note that it is fundamentally different to estimate the frequency of occurrence of an event, such as core damage, and the probability of an event occurring within a given time frame. A more detailed discussion of this topic is beyond the scope of this paper, but future users of ZOS should review the available literature concerning these concepts thoroughly before proceeding with ZOS techniques. In particular, for approaches other than probability of frequency, such as probability of probability, ZOS may not be appropriate.

DESCRIPTION OF ZERO-ONE SAMPLING (ZOS)

In an uncertainty analysis involving random or stratified sampling techniques, the outcomes are quantified repeatedly using sampled values for each of the probabilistically treated parameters in the PRA model. The individual quantifications are referred to as "sample members." Many different parameters can be treated, such as pump failure rates, the quantity of hydrogen generated, or the time at which the station batteries will be depleted. For many of the parameters in the PRA model, continuous probability distributions are sampled, producing a different frequency for each sample member. This is done for events, such as pump failures, that are believed to be governed by random behavior and for which probability distributions have been generated.

ZOS is a sampling scheme where zero and one are the only allowed frequencies for selected parameters. For example, if an event tree question asks whether or not an event occurs, each sample member would have a value of zero or one for a branch in that question. The fraction of sample members assigned a frequency of one would be based on a probability supplied by the PRA analyst. If a physical quantity or a time interval is being evaluated, ZOS provides a frequency of one for a particular discrete interval of the quantity or time. These concepts are discussed further below.

USE OF ZOS IN NUREG-1150 AND LASALLE PRAs

The NUREG-1150 and LaSalle PRAs were among the first to make widespread use of ZOS. These PRAs involved a relatively comprehensive approach to uncertainty analysis that integrated the three levels of the PRA into an overall uncertainty calculation. This broad scope for the uncertainty analysis led to the consideration of many different types of issues and variables. For the issues deemed to be most important, panels of experts used a formal expert judgment process to provide uncertainty estimates. For less important issues, the PRA analysts supplied the uncertainty estimates without the complete expert panel process. In some of these cases, continuous probability distributions were provided, usually consistent with a probability of frequency interpretation. In other cases, constant branching probabilities were provided.

Interpretations of probability and the use of ZOS were hotly debated among the PRA analysts involved in the NUREG-1150 and LaSalle PRAs. However, few such discussions took place within the expert panels. Although the experts received essential training in probabilistic elicitation, most of them had expertise in reactor safety and

particular phenomena, as opposed to PRA and statistics. In general, they supplied technical information as requested by the PRA analysts. Therefore, it should not be concluded that, because a distribution or a constant branch probability was provided, the experts had unequivocally determined the best characterization of uncertainty for that issue. Further, the experts did not usually conclude how the uncertainty information that they provided should be treated in the sampling process. As discussed below, practical issues often outweighed the need to be statistically precise. In NUREG-1150 and LaSalle, ZOS was used for three different cases.

Case 1: Time Intervals and Physical Quantities

There are many variables in a PRA that describe a time of occurrence or a physical quantity, rather than a probability or frequency. For example, one of the important uncertainties in the Level 1 PRA analysis was the battery depletion time in long-term station blackout sequences. The operator recovery probabilities depend on the time to battery depletion. At the time of the analysis, there was no easy method for sampling the time-reliability curve and automatically adjusting the recovery parameters. Therefore, the approach taken was to divide the time range into five discrete time intervals, essentially generating a five-branch question on the event tree. Probabilities were determined for each of the five branches. Using ZOS, each sample member contained a frequency of one for exactly one of the branches and zero for the other four. The fraction of sample members with a value of one for a particular branch was equal to its probability.

In the Level 2 PRAs, there were several event tree questions asking about particular phenomena. For example, the vessel failure size is very important and affects several subsequent event tree questions. The approach taken in NUREG-1150 in some instances was to consider discrete sizes and estimate the probability of each case, much as was done for the time intervals. Using the probabilities, ZOS was performed, and a frequency of one was assigned to exactly one of the cases for each sample member.

In other parts of the Level 2 PRAs, continuous distributions for parameters were sampled, with a single value used for each sample member. An example of this is the amount of hydrogen generated during an accident. At first, this may seem to be the same as sampling pump failure rates where a single value of the failure rate is produced for each sample member. However, they are different, because both pump success and pump failure are quantified for each sample member, i.e., both outcomes are possible, while the amount of hydrogen is treated as the only possible outcome for that sample member. Therefore, the latter treatment is equivalent to ZOS (in this case, the approach is equivalent to a simulation approach).

Case 2: Maximize the Uncertainty

A comprehensive PRA involves many hundreds of variables. Generating probability distributions for all of these variables is a significant undertaking. There were many instances in NUREG-1150 where probability distributions were unavailable for particular events. This could occur if the experts did not provide distributions for a particular event, if joint probability distributions were involved, or if the analysts simply did not expend the resources to generate distributions. In each of these cases, the analysts had only constant branch probabilities to describe the events. The use of these probabilities as constant split fractions in the model yields no uncertainty in the estimates of mean risk (i.e., every sample member has the same value). As an approach to maximize the uncertainty from some important variables, ZOS was employed where the split fraction was used as the appropriate ZOS probability. This approach is an effective screening technique to identify variables that could be important contributors to the

uncertainty, although in NUREG-1150 and LaSalle many of the variables were treated this way in the final analysis also.

The case of joint probability distributions is particularly difficult to treat. In these cases, a probability is estimated from the combination of other probability distributions. An example of this is the containment failure event. The probability of containment failure can be determined from the probability of a given pressure loading combined with the probability of structural failure, given the loading. The overlap in the two distributions determines the probability of containment failure. Although the experts provided distributions for pressure loads and structural failure, the combined probability is a single number. Generating an uncertainty distribution for containment failure would require generating families of distributions for the two underlying variables. This was not done for NUREG-1150; rather the analysis effectively used the single number as a constant split fraction in ZOS.

Case 3: Zero-One Events

A few events were identified where one or more of the experts believed that a particular event either always occurred or never occurred; they simply did not know which was the true answer. This type of event can be thought of as a "true zero-one event." Probabilities were provided that were interpreted as the probability that the true frequency was equal to 1.0. ZOS was used, with the fraction of ones being equal to the assigned probability. An example of this is the question of Mark I BWR liner meltthrough, although further examination of the expert responses indicates that the interpretation of the distributions is not straightforward. In fact, there were very few cases where an expert indicated that he/she believed an event was a true zero-one event, and in those cases, other experts often disagreed.

ACTUAL BEHAVIORS AND PROPER TREATMENTS

In many cases, ZOS is being employed for reasons of convenience. Cases involving three or more branches for one event tree question, cases involving quantities or time intervals, or cases where only a single probability (and not a whole distribution) is available are instances where ZOS is employed as a practical solution. The rationale for using ZOS in these cases is that it (1) is easy to implement, (2) maximizes the uncertainty and (3) allows the variable to be included in an uncertainty analysis to obtain an approximation of the uncertainty importance. While these reasons are often appropriate, the only absolutely "correct" use of ZOS is for true zero-one variables in combination with the "probability of frequency" interpretation of the PRA models. The discussions below address appropriate uses of ZOS, based on our current understanding.

Uncertainty Scoping Studies

As noted previously, Level 3 PRAs can involve many hundreds of variables. ZOS can be used as an effective technique in evaluating which variables are contributing to the uncertainty and should receive additional attention. ZOS effectively maximizes the uncertainty for a variable and is simple to implement. Only a single point estimate is needed to estimate branching probabilities. Subsequent regression analyses can indicate the importance of each variable to the overall uncertainty.

Multiple Branch Questions

Multiple branch questions have been difficult to address until recently. Sampling continuous distributions is difficult because of the constraint that the probabilities must add to one. Approaches involving sampling all branches and normalizing or sequential conditional sampling can not be shown to be unbiased in all cases. At the time of NUREG-1150, our available computer codes did not include methods for evaluating continuous distributions for more than two branches. Therefore, ZOS was used as the practical solution for multiple branch questions.

Since NUREG-1150, a new approach has been developed that allows straightforward treatment of continuous distributions for multiple branch questions. This approach is described in another paper at this conference.[5] The approach uses the asymmetric Dirichlet distribution to provide practical and unbiased sampling of the multiple outcomes. The new method will yield a much more accurate representation of the uncertainty than ZOS and is recommended as a replacement for ZOS in future PRAs unless an event is a true zero-one event as discussed below.

Zero-One Events

True zero-one events, as defined previously, are the only events for which ZOS is the statistically correct approach, and then it is appropriate only in the probability of frequency interpretation. In fact, ZOS is simply a degenerate case of the normal probability of frequency formulation in which the probability distribution is a special case with zero and one as the only allowed frequencies. The real question in this situation is how to determine whether an event is truly a zero-one event.

It is difficult to imagine a perfect zero-one event in a PRA, that is, an event for which the true frequency is exactly zero or one. On the other hand, true frequencies might lie close enough to zero or one that the difference is negligible. Determining what is negligible depends upon the particular PRA application. If one is calculating accident sequence frequencies and retaining cut sets with frequencies greater than 10^{-6}, then a true event frequency of 10^{-10} (or $1 - 10^{-10}$) could be treated as zero (or one). That is, if a frequency is clearly either less than 10^{-10} or greater than $1 - 10^{-10}$, but the analyst does not know which, then the variable could be treated appropriately as zero-one in this instance. This process is complicated by the fact that what is negligible changes in different parts of the PRA. A level 1 success criteria may be important at a different probability level than a containment failure mode, depending upon the particular risk measure. Further, a level 1 variable may have more influence on the level 2 results than on the level 1 results. Therefore, ZOS should only be used when its impact has been carefully examined for all risk measures.

SUMMARY AND CONCLUSIONS

ZOS was employed extensively in NUREG-1150 and the LaSalle PRA. ZOS was a practical solution to a variety of problems. ZOS remains a useful tool for uncertainty scoping and sensitivity studies. It is the correct approach for true zero-one variables within the context of the probability of frequency approach. However, true zero-one variables are rare in the context of PRA models, and in most other cases, ZOS overestimates the uncertainty (there are a few special cases where the uncertainty may be underestimated). Recent improvements in our capabilities make ZOS unnecessary in most cases. In particular, the use of the Dirichlet distribution allows us to deal with the

problems associated with multiple branching. Therefore, we expect the use of ZOS to be reduced in the future.

REFERENCES

1. Severe Accident Risks: An Assessment for Five U. S. Nuclear Power Plants, NUREG-1150, U.S. Nuclear Regulatory Commission, January 1991.

2. A. C. Payne, Jr., Analysis of the LaSalle Unit 2 Nuclear Power Plant: Risk Methods Integration and Evaluation Program (RMIEP), NUREG/CR-4832, SAND92-0537, Sandia National Laboratories, July 1992.

3. T. D. Brown, et al., Integrated Risk Assessment for the LaSalle Unit 2 Nuclear Power Plant, NUREG/CR-5305, SAND90-2765, Sandia National Laboratories, August 1992.

4. S. Kaplan and B. J. Garrick, "On the Quantitative Definition of Risk," Risk Analysis, Vol. 1, No. 1, 1981.

5. A. C. Payne, Jr. and G. D. Wyss, "Coherent Sampling of Multiple Branch Event Tree Questions," Sandia National Laboratories, PSAM-II, San Diego, CA, March 20-24, 1994.

COHERENT SAMPLING OF MULTIPLE BRANCH EVENT TREE QUESTIONS[1]

Arthur C. Payne Jr.* and Gregory D. Wyss**

* Arms Control Studies Department 4115
**Reactor Systems Safety Analysis Department 6412
Sandia National Laboratories
Albuquerque, NM 87185

INTRODUCTION

In the detailed phenomenological event trees used in recent Level III PRA analyses,[1,2,3] questions arise about the possible outcomes of events for which the underlying physics is not well understood and where the initial and boundary conditions are uncertain. Examples of the types of events being analyzed are: What is the containment failure mode?, Is there a large in-vessel steam explosion?, How much H_2, CO, and CO_2 are produced during core-concrete interactions? The outcomes of each of these questions must be defined based on an understanding of the basic physics of the phenomena and the level of detail of the probabilistic analysis.

Many of these phenomena have never occurred since severe reactor accidents are extremely rare events. The only information we have about these phenomena comes from four basic sources: general theoretical knowledge, limited experimental results (i.e, limited in number and in applicability), a few actual events, and various models of the phenomena. All of these phenomena have significant uncertainty arising from three basic sources: level of detail, initial and boundary conditions, and lack of knowledge. Since it is not possible to conduct enough full scale tests to generate a set of "objective" relative frequencies, the probabilities, therefore, will have to be "subjective" and generated based on expert knowledge.

In assessing the conditional probabilities of the various possible outcomes of an event during an accident, the expert must amalgamate his knowledge with the level of detail being used in the PRA analysis to generate a set of probabilities for the defined set of outcomes. It is often convenient for an expert to formulate his opinion in terms of expecting to see n_i occurrences of outcome E_i in N occurrences of event E. The order of the outcomes is typically not important because the individual trials are viewed as being independent of one another. Mathematically the problem can be stated as follows: Given a finite sample $\mathbf{n} = (n_1, n_2, ..., n_t)$, where $\Sigma_i n_i = N$, the sample size, for an event with t possible outcomes (t>1), how do we estimate the probabilities $\mathbf{p} = (p_1,..., p_t)$ of the various outcomes, and how do we represent our degree of confidence in these values?

[1] This work support by the U. S. Department of Energy under contract DE-AC04-76DP00789.

CURRENT METHODS OF APPROACH

Because of the difficulty of developing a coherent set of probability distributions for the simultaneous sampling of the probabilities of multioutcome events, past nuclear power plant probabilistic risk assessments (PRAs) have used various practical workarounds to incorporate uncertainty for multioutcome events:

1. The uncertainty is assumed to be represented by the list of potential outcomes itself. In its simplest form, this method represents the uncertainty in *outcomes* while neglecting the uncertainty in *probabilities*. This method is simple but provides only minimal uncertainty information for the analyst.
2. "Zero/One" sampling, in which the outcomes of the event are assigned probabilities of either zero or one in each observation, and the fraction of observations in the overall sample that contain a probability of one for a particular outcome is intended to represent the "relative probability" of that outcome. This is similar to Monte Carlo calculations for deterministic processes; but, the circumstances under which Zero/One sampling is truly appropriate for the probabilistic analysis of risk is subject to much debate within the risk assessment community.
3. The multibranch event is evaluated in such a way that only two possible outcomes are considered likely to occur given each potential set of prior events within the APET model. Other outcomes are considered unlikely and are neglected. Traditional uncertainty distributions are used to represent these binary pieces of the overall multibranch event. While this method provides more uncertainty information to the analyst, it is only applicable in a few very special instances.
4. The multibranch event is decomposed into a series of binary events with each question asking about the occurrence of successive outcomes for the original multibranch event. An unconditional uncertainty distribution is derived for the first outcome, and conditional distributions are derived for subsequent outcomes (conditional upon the non-occurrence of previously evaluated outcomes). This method increases the size and complexity of the APET by increasing the number of events in the model. In addition, the conditional distributions are difficult to visualize and very difficult to determine, and it may be very difficult to determine an appropriate order for the resulting binary events. This method has been used only for questions with a small number of outcomes, at most 3 or 4.
5. Individual distributions are constructed for each of the potential outcomes to the multibranch event. Since there is no guarantee that the sampling process will yield probabilities that sum to unity, the probabilities are normalized for each observation. Our limited investigations of this technique indicate that the statistics of the normalized distributions can be very different from those of the original distributions. The result being that it may be difficult to defend the validity of such a study in the larger scientific community.

The above methods represent practical "work arounds," but they do not produce coherent uncertainty information for complex multiple outcome events. This paper presents a systematic method that resolves these long-standing difficulties. The solution is based on the use of the Dirichlet distribution, which is a multivariate generalization of the beta distribution. This distribution has been used in economics and in expert systems to address similar problems.[4]

JOHNSON'S SUFFICIENTNESS POSTULATE

W. E Johnson,[5] a Cambridge philosopher, addressed this problem in a posthumous paper in 1932. He postulated that the expected value of probability p_i depends only upon n_i, N, and t. Based on this assumption, it can be shown that, for an infinitely exchangeable sequence, the probabilities p can be appropriately represented by a t-category symmetric Dirichlet distribution (the implication being that the relative magnitudes of the n_i's do not contain any additional information about the probability p_j). I. J. Good,[6] generalized the argument to finitely exchangeable sequences with posterior expectation of success linear in the frequency count. Neither Johnson nor Good

proved the result for the case t=2; S. L. Zabell[7] completed the mathematical proof of the generalized argument. Zabell proved that, for a finitely exchangeable sequence, if the n_i's do not shed appreciable light on the value of p_j except through the roughness of **p** (i.e., the deviation of the p_i's from the equiprobable case, p_i=1/t) then the probability of category i depends only on n_i, N, t, and a constant ω_i and the distribution of the probabilities **p** can be represented as an asymmetric Dirichlet distribution.

If the expert judgement problem is represented in this form, then the job of the expert is to select appropriate values for the Dirichlet distribution constants ω_i. However, these constants can be derived based on the values n_i (i.e., when formulated in this fashion then $\omega_i = n_i+1$). When this is done, the size of N represents the degree of confidence that an expert feels in his expectation of the p_i's ($E(p_i) = \omega_i/\Sigma_j \omega_j$).

There are, of course, instances where the assumption of interchangeability is not a good approximation of the problem being modeled. Also, additional information could be conveyed by the relative magnitudes of the n_i's other than by the roughness of **p**. A physical example would be the frequency of frequencies (i.e., the frequency with which a particular value of n_i appears) obtained in sampling biological species or vocabulary where, for example, all odd n_i's might be larger than all even n_i's. However, for the risk assessment problem, we feel that these assumptions are usually valid and that the asymmetric Dirichlet distribution is an appropriate modeling tool.

THE DIRICHLET DISTRIBUTION

Since the Dirichlet distribution is defined on the surface $\Sigma_i p_i = 1$, the general asymmetric Dirichlet distribution for a t-category event has only (t-1) degrees-of-freedom and can be written as:

$$f_{P_1,\ldots P_{t-1}}(p_1,\ldots,p_{t-1}) = \frac{\Gamma(\sum_{i=1}^{t-1}\omega_i)}{\prod_{i=1}^{t-1}\Gamma(\omega_i)} * \prod_{i=1}^{t-1} p_i^{\omega_i-1} * (1-\sum_{i=1}^{t-1} p_i)^{\omega_t-1}$$

where the parameters $\omega_i = n_i+1$, i = 1 to t-1 the i 'th category, and p_i is the probability of outcome E_i. The marginal distributions are beta distributions of the form:

$$f_{P_i}(p_i) = \frac{\Gamma(\sum_{j=1}^{t}\omega_j)}{\Gamma(\omega_i) * \Gamma(\sum_{j\neq i}\omega_j)} * p_i^{\omega_i-1} * (1-p_i)^{\sum_{j\neq i}\omega_j-1}.$$

In order to get a visual feeling for what this distribution is like, we will specialize to the case of a three branch event tree question. Since the probabilities of the three branches must sum to 1.0, there are only 2 degrees-of-freedom in this case and

$$f_{P_1,P_2}(p_1,p_2) = \frac{\Gamma(\omega_1+\omega_2+\omega_3)}{\Gamma(\omega_1) * \Gamma(\omega_2) * \Gamma(\omega_3)} * p_1^{\omega_1-1} * p_2^{\omega_2-1} * (1-p_1-p_2)^{\omega_3-1}.$$

The probability of branch 3 can be expressed in terms of branches 1 and 2 (i.e., $p_3 = 1 - p_1 - p_2$). For the case of $\omega_1 = 2$, $\omega_2 = 3$, and $\omega_3 = 4$, Figure 1 shows a 3-D representation of the distribution and Figure 2 shows a contour plot representation. The peak of the distribution is at the point (.222, .333), the mean probabilities of outcomes 1 and 2, respectively. In order to get a feel for how the shape of the distribution changes, Figure 3 shows the case with the dominant outcome being outcome 1, ω = (4,3,2). As can be seen the peak of the distribution shifts as the mean values shift. Figure 4 shows an example of how increased confidence affects the distribution. In Figure 4 the case is ω = (3,5,7), a doubling of the sample size, and the narrowing of the distribution is apparent.

PRA APPLICATION

The above method can be used to generate coherent Monte Carlo/Latin Hypercube samples for multibranch event tree questions. Interactive software, developed at Sandia National Laboratories, allows an expert to iteratively input the n_i's and view the resulting marginal distributions and their statistics. The expert may then modify his selected parameters until he is satisfied that the set of marginals adequately represents his beliefs. Sandia has also extended the LHS[8] code suite to allow for sampling of the multivariate Dirichlet distribution. Since the probabilities sampled from a Dirichlet distribution are required to sum to 1, the sampled data can be used directly as branch probabilities for multi-branch events in Sandia's EVNTRE[9] event tree analysis code.

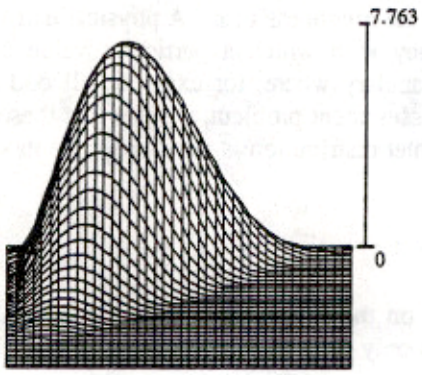


Figure 1. 3-D Dirichlet, $\omega = (2,3,4)$

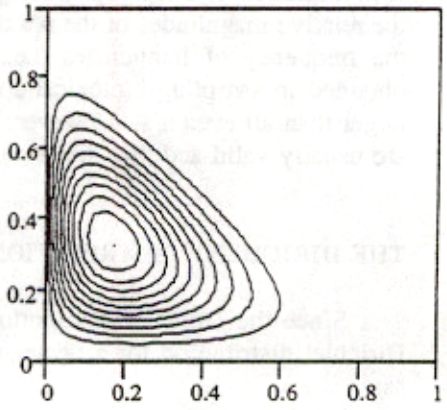


Figure 2. Contour Plot, $\omega = (2,3,4)$

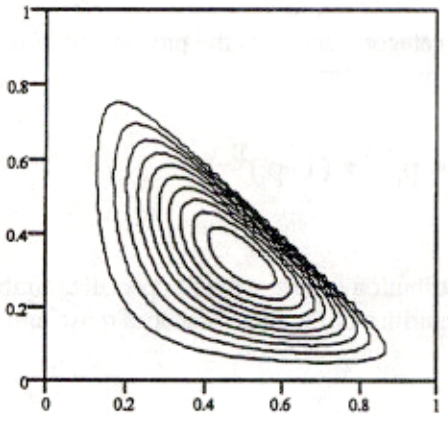


Figure 3. Contour Plot, $\omega = (4,3,2)$

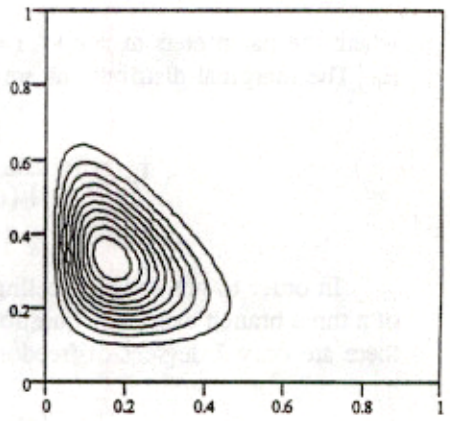


Figure 4. Increased Sample Size, $\omega = (3,5,7)$

The recently completed Level III probabilistic risk assessment of the LaSalle Nuclear Power Plant provides several instances where a Dirichlet distribution might have been useful. The accident progression event tree analysis included several multibranch event tree questions related to phenomena that might occur following a breach of the reactor vessel. For our example, we will use the event tree question, "Does the cavity floor fail from core debris attack?" in the case where a steam explosion occurs in the reactor cavity pool due to a small pour of molten core material from the reactor vessel into a flooded reactor cavity. The objective of the event tree question is to determine whether cavity failure occurs within 30 minutes, one hour, two hours, or after two hours.

A panel of six experts was convened to provide insight into this and other related issues. The panel provided responses in the form of a cumulative probability for the time frames described above. The aggregated results for this case showed the probability of cavity failure in Table 1.

These probability densities were modeled in the LaSalle accident progression event tree using zero/one sampling. While zero/one sampling accurately reflects the probability densities, it does not provide any information regarding the confidence that the panel members placed in their numbers. In other words, the probability that cavity failure would occur in less than 30 minutes is stated as 0.149, but the experts may have only felt confident that the true probability falls somewhere between 0.1 and 0.2. The method used in the LaSalle study, while state of the art at the time, did not allow for this type of uncertainty to be either provided by the experts or modeled in the event tree.

Table 1. Aggregated Probability of Cavity Failure With Time.

Cavity Failure Time	Cumulative Probability	Probability Density
Less than 30 minutes	0.149	0.149 (failure before 30 minutes)
Less than 1 hour	0.327	0.178 (failure between 30 minutes and 1 hour)
Less than 2 hours	0.506	0.179 (failure between 1 hour and 2 hours)
More than two hours	1.00	0.494 (failure, if any, occurs after more than 2 hours)

The estimates of probability density were used as the basis for generating several Dirichlet distributions with differing degrees of confidence. The degree of confidence is related to the total of the parameters in the Dirichlet distribution (i.e., $\Sigma_i \omega_i = N + t$, larger N indicates a greater degree of confidence). The increasing confidence level can be seen by a reduced standard deviation for each marginal distribution as the sum of the distribution parameters increases. In the "Low Confidence Dirichlet Distribution" example shown in Table 2, this would indicate that we could imagine 12 occurrences, $\mathbf{n} = (1, 2, 2, 7)$, of a steam explosion in the reactor cavity pool due to a small pour of molten core material into a flooded reactor cavity, and that one of those occurrences would lead to cavity failure in less than 30 minutes, two between 30 minutes and one hour, and so on. One would naturally expect that having more occurrences upon which to base an opinion would lead to greater confidence in the results, and that behavior is seen in the other two examples in Table 2 (i.e., $\mathbf{n} = (11, 14, 14, 40)$ and $\mathbf{n} = (108, 130, 130, 362)$, respectively). Since the mean values are ratios of integers, the aggregated probability of the three experts can not be reproduced in the low confidence distribution and, in any case, the examples in Table 2 represent the densities pretending the aggregated distribution was obtained from one expert. In the actual case, the distributions from the individual experts would have to be aggregated.

CONCLUSIONS

The use of the asymmetric Dirichlet distribution allows an expert to represent his knowledge about a multioutcome issue using an intuitive and natural model while at the same time enforcing consistency and coherence in the resultant distributions and allowing for Bayesian updating of the distribution if additional knowledge is obtained. Since the marginal probabilities are derived from a multinomial distribution defined on the unit simplex, sampling the resultant distribution guarantees that the set of branch probabilities selected for each observation will sum to one without the use of potentially biasing normalization techniques. The method was demonstrated using an example

from the LaSalle risk assessment study. The use of this technique will allow for the incorporation of uncertainty into risk assessment models in ways that have previously been impossible.

REFERENCES

1. T. D. Brown, A. C. Payne Jr., L. A. Miller, J. D. Johnson, D. I. Chanin, A. W. Shiver, S. J. Higgins, and T. T. Sype, "Integrated Risk Assessment for the LaSalle Unit 2 Nuclear Power Plant," NUREG/CR-5305, SAND90-2765, Sandia National Laboratories, Albuquerque, NM (1992).
2. A. L. Camp, D. M. Kunsman, L. A. Miller, J. L. Sprung, T. A. Wheeler, G. D. Wyss, "Level III Probabilistic Risk Assessment for N Reactor," WHC-MR-0045, SAND89-2102, Westinghouse Hanford Company, Richland, WA (1990).
3. U. S. Nuclear Regulatory Commission, "Severe Accident Risks: An Assessment for Five U. S. Nuclear Power Plants," NUREG-1150, U. S. Nuclear Regulatory Commission, Washington, DC (1990).
4. R. E. Neapolitan, "Probabilistic Reasoning in Expert Systems," Wiley Interscience, New York (1990).
5. W. E. Johnson, "Probability: the deductive and inductive problems (Appendix)," *Mind* 49:409 (Appendix on pages 421-423 ed. by R. B. Braithwaite) (1932).
6. I. J. Good, "A Bayesian Significance Test for Multinomial Distributions," *J. Roy. Statist. Soc. Ser. B* 29:399 (1967).
7. S. L. Zabell, "W. E. Johnson's "Sufficientness" Postulate," *The Annals of Statistics* 10:1091 (1982).
8. R. L. Iman and M. J. Shortencarier, "A FORTRAN 77 Program and User's Guide for the Generation of Latin Hypercube and Random samples for Use With Computer Models," NUREG/CR-3624, SAND83-2365, Sandia National Laboratories, Albuquerque, NM (1984).
9. J. M. Griesmeyer and L. N. Smith, "A Reference Manual for the Event Progression Analysis Code (EVNTRE)," NUREG/CR-5174, SAND88-1607, Sandia National Laboratories, Albuquerque, NM (1989).

Table 2. Example Coherent Probability Densities Generated From the Dirichlet Distribution.

Distribution Type & Parameters		< 30 Min	30 Min - 1 Hr	1 - 2 Hr	> 2 Hr
Experts' Probability Density		0.149	0.178	0.179	0.494
Low Confidence Dirichlet Distribution	Parameter (ω_i)	2	3	3	8
	Mean	0.1250	0.1875	0.1875	0.5000
	Std. Deviation	0.0802	0.0947	0.0947	0.1213
Moderate Confidence Dirichlet Distribution	Parameter (ω_i)	12	15	15	41
	Mean	0.1446	0.1807	0.1807	0.4940
	Std. Deviation	0.0384	0.0420	0.0420	0.0546
High Confidence Dirichlet Distribution	Parameter (ω_i)	109	131	131	363
	Mean	0.1485	0.1785	0.1785	0.4945
	Std. Deviation	0.0131	0.0141	0.0141	0.0184

ANALYSIS OF EXTREME TOP EVENT FREQUENCY PERCENTILES BASED ON FAST PROBABILITY INTEGRATION*

Bevan Staple[1] and F. Eric Haskin[2]

[1]Sandia National Laboratories
[2]University of New Mexico

INTRODUCTION

In risk assessments, a primary objective is to determine the frequency with which a collection of initiating and basic events, E_e, leads to some undesired top event, T. Uncertainties in the occurrence rates, x_t, assigned to the initiating and basic events cause uncertainty in the top event frequency, z_T. The quantitification of the uncertainty in z_T is an essential part of risk assessment called uncertainty analysis. Closely related to uncertainty analysis is sensitivity analysis, which involves the determination of the changes in z_T resulting from changes in the occurrence rates of the initiating and basic events.

In the past, it has been difficult to evaluate the extreme percentiles (such as the 99.9th or the 99.99th percentiles) of output variables like z_T. Analytic methods such as the method of moments do not provide estimates of output percentiles and the Monte Carlo (MC) method can be used to estimate extreme output percentiles only by resorting to large sample sizes. A promising alternative to these methods is the fast probability integration (FPI) methods. These methods approximate the integrals of multi-variate functions, representing percentiles of interest, without recourse to multi-dimensional numerical integration (Hasofer and Lind, 1974; Wu, 1989). FPI methods give precise results and have been demonstrated to be more efficient than MC methods for estimating extreme output percentiles. FPI allows the analyst to choose extreme percentiles of interest and perform sensitivity analyses in those regions. Such analyses can provide valuable insights as to the events driving the top event frequency response in extreme probability regions. These analyses also provide a way of identifying where additional information would be most useful in reducing the uncertainty in the top event frequency.

In this paper, FPI methods are adapted a) to precisely estimate extreme top event frequency percentiles and b) to allow the quantification of sensitivity measures at these extreme percentiles. In addition, the relative precision and efficiency of alternative methods for treating lognormally distributed inputs is investigated. The methodology is applied to the top event frequency expression for the dominant accident sequence from a risk assessment of Grand Gulf nuclear power plant (Drouin et al., 1989).

* This work was performed at Sandia National Laboratories, which is operated for the US Department of Energy under Contract Number DE-AC04-76DP00789.

FAST PROBABILITY INTEGRATION (FPI)

Fast Probability Integration methods are widely used in the field of structural reliability to approximate the integrals of multi-variate functions, representing percentiles of interest, P_z. To illustrate the concept of FPI, consider a function $z(x)$ where x is a vector of random variables with Joint Probability Density Function (JPDF), $f_x(x)$. The probability, P_z, of not exceeding some limiting value of $z(x)$, z_o , is given as

$$P_z = \int_{g(x)<0} f_z(x)dx \tag{1}$$

where $g(x) = z(x) - z_o = 0$ is termed a *limit-state* function and $g(x) < 0$ is the domain of integration. Evaluation of the integral in Eq. (1), in general, is very complicated when $f_x(x)$ is the JPDF of many variables or when the integral domain is irregular. However, with FPI, the random input variables represented by the vector x can be transformed into a probability space represented by the vector u whose components are mutually independent, standardized, and normally distributed. That is, the variables become normally distributed with means zero and variances one. In the *u-space*, Eq. (1) becomes

$$P_z = \int_{g(u)<0} f_u(u)du \tag{2}$$

By transformation, all the uncertainties in the input variables are condensed into a single reliability index, β, called the Hasofer-Lind reliability index. The reliability index defines the minimum distance from a point u^*, called the Most Probable Point (MPP), on the *limit-state* surface to the origin of the coordinates in the *u-space*. Using β, the integral of the multi-variate function can be estimated by approximating the *limit-state* function in the *u-space*, $g(u)$, by a first-order or second-order Taylor series expansion about the MPP. A first-order approximation to Eq. (2), called the first-order reliability method (FORM), was derived by Hasofer and Lind (1974) and is given as

$$P_z \approx \Phi(-\beta) \tag{3}$$

Here Φ is the standard normal cumulative distribution function.

FORMULATION

The Top Event Frequency Equation

The top event, T, can be represented by a union of the minimal cut sets, S_k, which are sums of products of basic and initiating events in Boolean notation:

$$T = \bigcup_{k=1}^{K} S_k = \sum_{k=1}^{K} \prod_{e=1}^{N_E} E_e^{\alpha_{ke}} \tag{4}$$

N_E is the number of basic and initiating events, E_e. K is the number of cut sets, and each cut set S_k is an intersection of initiating and basic events. $\alpha_{ke} = 1$ if cut set S_k contains event E_e; $\alpha_{ke} = 0$ otherwise. Under the rare-event approximation, an upper bound to z_T given independent occurrence rates, is

$$z_T \le \sum_{k=1}^{K} z_k = \sum_{k=1}^{K} \prod_{\ell=1}^{L} x_\ell^{\alpha_{k\ell}} . \tag{5}$$

Here $\alpha_{kt} = 1$ if the event assigned occurrence rate x_t appears in cut set S_k; $\alpha_{kt} = 0$ otherwise. z_k is the frequency of the k-th minimal cut set. When two or more of the occurrence rates are totally correlated they are equal. In this case, α_{kt} is the number of appearances of events assigned occurrence rate, x_t, in cut set S_k.

Two Alternative FPI Quantification Approaches

In FPI evaluations, all non-normal distributions are approximated by normal distributions. If all input distributions are initially normal, the need for approximate distributions in FPI is eliminated. The lognormal distribution is frequently used to characterize the uncertainties in x_t. The lognormal distribution is, however, a modified form of the normal distribution. Consequently, transformation of the top event frequency equation from a space of lognormally distributed inputs to a space of normally distributed inputs, before applying FPI, should increase the precision of FPI-estimated top event frequency percentiles.

In the first approach, the occurrence rates are assumed to be lognormally distributed with mean m_t and error factors EF_t. (EF_t is the ratio of the 95th to the 5th percentile of x_t.) FPI is then applied directly to Eq. (2), approximating the lognormal distributions for the x_t with normal distributions as described by Wu (1989).

In the second approach, the top event equation is transformed to a space of normally distributed independent variables y_t before applying FPI:

$$z_T = \sum_{k=1}^{K} \exp\left[\sum_{t=1}^{L} \alpha_{kt} y_t\right] \qquad (6)$$

The normally distributed variables are $y_t = ln(x_t)$ with means $\mu_t = ln(m_t)-\sigma_t^2/2$ and standard deviation $\sigma_t = [ln(EF_t)/1.645]^{**}$. The relative precision and efficiency of FPI is investigated by comparing the FPI results of the two approaches to the results from a MC sample of size 10,000. A sample size of 10,000 was used as a check as it was deemed adequate to produce good results.

Sensitivity Measures

Four measures are used to investigate the sensitivity of z_T to changes in x_t, at extreme percentiles. The four measures, which are discussed in detail by Haskin et al., (1993), are the partial derivative, PD_t, the normalized partial derivative ηPD_t which measures the contribution of x_t to the gradient of z_T, the risk reduction measure, RR_e, which is the reduction in z_T achieved by eliminating the minimal cut sets containing the event E_e from the Boolean expression of the top event, and the normalized risk reduction, ηRR_e, which divides RR_e by the top event frequency z_T to indicate the fraction (or percentage) of z_T attributable to cut sets containing event E_e.

APPLICATION

The results of the accident sequence analysis for internally initiated events for Grand Gulf Unit 1 (Drouin et al., 1989) indicated that a single accident sequence, which was initiated by a loss of offsite power (LOSP), accounted for 89% of the mean core damage frequency. The sequence, called station blackout sequence 16, contained 1053 minimal cut sets and 110 events. FPI methods are applied to the Grand Gulf dominant station blackout sequence to ascertain the 95th, 99th, 99.9th, and 99.99th percentiles of the accident sequence frequency, and the values of the independent variables at the most probable points corresponding to these percentiles. In the analysis, all occurrence rates based on common data are treated as being totally correlated. The steps taken in applying FPI to analyze the extreme percentiles of z_T and to quantify the four sensitivity measures at these percentiles are as follows:

1. Use the FPI to estimate z_T at the extreme percentiles of interest, for the two alternative

approaches. FPI also provides the most probable values i.e., the MPPs of the independent variables (x_t or y_t) at the selected percentiles of z_T.

2. Compare the FPI estimates of z_T for the two approaches to the estimates from a MC sample of size 10,000. Determine the more precise and efficient of the two approaches.
3. Use the Top Event Matrix Analysis Code (TEMAC, Iman and Shortencarier, 1986) to evaluate the four sensitivity measures at the MPPs corresponding to extreme percentiles.

Results of the Comparisons of FPI Quantification Alternatives

The results of the relative precision of alternative methods for treating non-normally distributed, tailed inputs are presented in Table 1. The best agreements are obtained between the FPI results for the second approach and the 10,000 MC simulations. In addition, the transformation to the normally distributed independent variables, reduces the FPI computation time by a factor of five. Each percentile determined by FPI in the transformed alternative required less than 10% of the run time required for the 10,000 MC sample. Therefore, the second approach is the better approach. The remainder of the results are based on this approach.

Table 1. Descriptive Statistics for Grand Gulf Dominant Station Blackout Sequence.

Quantile	Approach 1 FPI Estimate of $z_T(x)$ (yr^{-1})	Approach 2 FPI Estimate of $z_T(y)$ (yr^{-1})	10,000 MC Estimate of z_T (yr^{-1})
0.05	1.05E-7	1.11E-7	1.12E-7
0.50	6.50E-7	1.25E-6	9.99E-7
0.95	9.95E-6	1.04E-5	1.08E-5
0.99	3.61E-5	3.65E-5	3.66E-5
0.999	1.67E-4	1.68E-4	1.69E-4
0.9999	6.32E-4	6.34E-4	6.36E-4

Partial Derivative Results

Table 2. Partial Derivative Measures at the Extreme Percentiles for the Grand Gulf Station Blackout Sequence.

Event	PD_t-95	Rank	PD_t-99	Rank	PD_t-99.9	Rank	PD_t-99.99	Rank
MOV-CC*	1.31E-3	(1)	3.88E-3	(1)	1.49E-2	(1)	4.74E-2	(1)
MOV-MA*	7.78E-4	(3)	2.65E-3	(2)	1.13E-2	(2)	3.79E-2	(2)
DCP-BAT-LP-CM#	4.70E-4	(4)	5.68E-4	(18)	7.40E-4	(18)	9.17E-4	(20)
ACP-DGN-FS*	4.16E-4	(5)	1.19E-3	(5)	2.16E-3	(5)	1.49E-2	(4)
ACP-DGN-FR*	3.95E-4	(6)	1.21E-3	(6)	4.62E-3	(6)	1.47E-2	(5)
SSW-HTX-PG*	3.77E-4	(7)	1.33E-3	(4)	5.80E-3	(3)	2.02E-2	(3)
SSW-MDP-FS-CM#	3.69E-4	(8)	7.64E-4	(15)	1.87E-3	(17)	3.98E-3	(17)
MDP-FS*	3.58E-4	(9)	1.09E-3	(7)	4.25E-3	(7)	1.36E-2	(6)
DGN-MA*	3.44E-4	(10)	1.05E-3	(8)	4.15E-3	(8)	1.31E-2	(7)
FAN-MA*	2.20E-4	(11)	9.93E-4	(9)	3.95E-3	(9)	1.27E-2	(8)

The results of the partial derivatives and the contributions to the gradient, at the 95th, 99th, 99.9th and the 99.99th percentiles, for 10 occurrence rates, are shown in Tables 2 and 3 respectively. All event that share the same occurrence rate share the same PD_t. For example, the occurrence rates for the events standby service water motor-operated valve #11 fails to open, SSW-MOV-CC-MV11 and RCIC motor-operated valve #46 fails to open, RCIC-MOV-CC-MV46 are

* Denotes totally correlated occurrence rates and # denotes uncorrelated occurrence rates.

totally correlated, and are represented in Tables 2 and 3 by the group name MOV-CC. Event names, such as DCP-BAT-LP-CM (common mode failure of the batteries) are used to denote the corresponding uncorrelated occurrence rates. The occurrence rates in Tables 2 and 3 are ranked according to the magnitudes of PD_t with a rank of 1.0 assigned to the largest partial derivative, a rank of 2 to the second largest, and so on. In the case of a tie, the rank assigned is the average of the ranks that would have been assigned had there being no tie. The results in Table 2 indicate that PD_t at the most probable points increase as the percentile of z_T increases, for all occurrence rates. Thus, the top event frequency of the station blackout sequence becomes more sensitive as the percentiles increase. The contribution to the gradient shows two different trends. First, the results indicate that ηPD_t is dominated by two of the independent occurrence rates; the occurrence rate for motor operated valves failing to open, MOV-CC, and the occurrence rate for motor operated valves being out for maintenance, MOV-MA. Each of these two occurrence rates has a contribution to gradient of over 30% at each extreme percentile. Second, ηPD_t tends to decrease for events having uncorrelated occurrence rates but to increases for totally correlated occurrence rates in moving from the 95th percentile to the 99.99th percentile. This indicate that z_T becomes more sensitive to changes in totally correlated occurrence rates and less sensitive to other occurrence rates at extreme percentiles. For example, ηPD_t for DCP-BAT-LP-CM decreases with increasing percentiles.

Table 3. Normalized Partial Derivative Measures at the Extreme Percentiles for the Grand Gulf Station Blackout Sequence.

Event	ηPD_t-95	Rank	ηPD_t-99	Rank	ηPD_t-99.9	Rank	ηPD_t-99.99	Rank
MOV-CC*	56.6%	(1)	60.2%	(1)	60.4%	(1)	60.4%	(1)
MOV-MA*	33.7%	(3)	41.1%	(2)	46.0%	(2)	48.3%	(2)
DCP-BAT-LP-CM#	20.3%	(4)	8.8%	(18)	3.0%	(18)	1.2%	(20)
ACP-DGN-FS*	18.0%	(5)	18.9%	(5)	19.0%	(5)	19.0%	(4)
ACP-DGN-FR*	17.8%	(6)	18.8%	(6)	18.8%	(6)	18.8%	(5)
SSW-HTX-PG*	16.3%	(7)	20.7%	(4)	24.0%	(3)	25.8%	(3)
SSW-MDP-FS-CM#	16.0%	(8)	11.9%	(15)	7.6%	(17)	5.1%	(17)
MDP-FS*	15.5%	(9)	16.9%	(7)	17.3%	(7)	17.3%	(6)
DGN-MA*	14.9%	(10)	16.2%	(8)	16.7%	(8)	16.7%	(7)
FAN-MA*	13.9%	(11)	15.4%	(9)	16.1%	(9)	16.2%	(8)

Risk Reduction Results

Table 4. Risk Reduction Measures at the Extreme Percentiles for the Grand Gulf Station Blackout Sequence.

Event	RR_t-95	Rank	RR_t-99	Rank	RR_t-99.9	Rank	RR_t-99.99	Rank
IE-T1	1.04E-5	(1)	3.65E-5	(1)	1.68E-4	(1)	6.34E-4	(1)
RA-LOSP-1HR	1.00E-5	(2)	3.60E-5	(2)	1.67E-4	(2)	6.33E-4	(2)
RCI-TDP-FR-TDP1	8.29E-6	(3)	3.24E-5	(3)	1.59E-4	(3)	6.14E-4	(3)
RA-DGHW-1HR	7.50E-6	(4)	3.22E-5	(4)	1.45E-4	(4)	5.70E-4	(4)
ACP-DGN-FS-DG3	7.21E-6	(5)	2.76E-5	(5)	1.37E-4	(5)	5.45E-4	(5)
ACP-DGN-FS-DG2	5.69E-6	(6.5)	2.35E-5	(6.5)	1.23E-4	(6.5)	5.02E-4	(6.5)
ACP-DGN-FS-DG1	5.69E-6	(6.5)	2.35E-5	(6.5)	1.23E-4	(6.5)	5.02E-4	(6.5)
ACP-DGS-FS-CM	1.36E-6	(8.5)	3.58E-6	(8.5)	1.10E-5	(9.5)	2.85E-5	(12.5)
BETA-2DG	1.36E-6	(8.5)	3.58E-6	(8.5)	1.10E-5	(9.5)	2.85E-5	(12.5)
ACP-DGN-FR-DG3	9.99E-7	(10)	3.03E-6	(10)	1.15E-5	(10)	3.63E-5	(8)

The risk reductions for 10 events at the MPPs corresponding to the 95th, 99th, 99.9th, and the 99.99th percentiles are shown in Table 4. The results indicate that the magnitudes of RR_ϵ increase as the percentile of z_T increases, for all events. This is not surprising since the magnitude of z_T available for reduction increases with increasing percentiles. The results of the normalized risk reduction are shown in Table 5. These results indicate that ηRR_ϵ is consistently dominated by seven events; the loss of offsite power (LOSP) initiating event (IE-T1), the failure to recover from an LOSP in one hour (RA-LOSP-1HR), the failure of RCIC turbine driven pump to run (RCI-TDP-FR-TDP1), the failure to recover from the hardware failure of a diesel generator within one hour (RA-DGHW-1HR), the failure of diesel generator #3 to start (ACP-DGN-FS-DG3), the failure of diesel generator #2 to start (ACP-DGN-FS-DG2), and the failure of diesel generator #1 to start (ACP-DGN-FS-DG1). Each of these seven events yields an ηRR_ϵ of over 50%. As expected, ηRR_ϵ for the initiating event is always 100% because the initiating event occurs in every cut set. For the other six dominant events, ηRR_ϵ increase with increasing percentile. In essence, important events become even more important at extreme top event frequency percentiles.

Table 5. Normalized Risk Reduction Measures at the Extreme Percentiles for the Grand Gulf Station Blackout Sequence.

Event	ηRR_ϵ-95	Rank	ηRR_ϵ-99	Rank	ηRR_ϵ-99.9	Rank	ηRR_ϵ-99.99	Rank
IE-T1	100%	(1)	100%	(1)	100%	(1)	100%	(1)
RA-LOSP-1HR	96.6%	(2)	98.8%	(2)	99.6%	(2)	99.9%	(2)
RCI-TDP-FR-TDP1	79.7%	(3)	88.7%	(3)	94.4%	(3)	96.8%	(3)
RA-DGHW-1HR	72.2%	(4)	80.3%	(4)	86.5%	(4)	89.8%	(4)
ACP-DGN-FS-DG3	69.3%	(5)	75.7%	(5)	81.4%	(5)	85.0%	(5)
ACP-DGN-FS-DG2	54.7%	(6.5)	64.4%	(6.5)	73.4%	(6.5)	79.2%	(6.5)
ACP-DGN-FS-DG1	54.7%	(6.5)	64.4%	(6.5)	73.4%	(6.5)	79.2%	(6.5)
ACP-DGS-FS-CM	13.1%	(8.5)	9.8%	(8.5)	6.5%	(9.5)	4.5%	(12.5)
BETA-2DG	13.1%	(8.5)	9.8%	(8.5)	6.5%	(9.5)	4.5%	(12.5)
ACP-DGN-FR-DG3	9.6%	(10)	8.3%	(10)	6.8%	(8)	5.7%	(8)

CONCLUSIONS

Fast probability integration (FPI) can be used for the quantification of extreme percentiles of top event frequencies. In addition, by transforming lognormally distributed occurrence rates to the normal space, improved estimates of the top event frequency are obtained. Normalized risk reduction measures evaluated at the most probable points corresponding to the extreme percentiles tend to provide relatively consistent rankings of the most important events. The contribution to the gradient display more variation, illustrating the tendency for totally correlated occurrence rates to become more important at extreme percentiles. Computationally, the FPI method appears to be competitive with MC with the advantage clearly in favor of FPI at the extreme percentiles.

REFERENCES

Drouin, M. T. et al., 1989, "Analysis of Core Damage Frequency: Grand Gulf, Unit 1 Internal Events," NUREG/CR-4550, USNRC, Washingtion DC.

Haskin, F. E. et al., 1993, "Development and Application of Group Importance Measures," Proceedings PSA, International Topical Meeting, American Nuclear Society, La Grange Park, Il.

Hasofer, A. M. and Lind, N. C., 1974, Exact and Invariant Second Moment Format, *J. Eng. Mech. Div., ASCE*, 100:111.

Iman, R. L. and Shortencarier, M. J., 1986, "A Users Guide for the Top Event Matrix Code (TEMAC)," NUREG/CR-4598, USNRC, Washington DC.

Wu, Y. T., 1989, "Fast Probability Integration (FPI) Theoretical Manual," SWRI, San Antonio, TX.

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)

SAFETY CULTURE:

WHAT IS IT AND HOW CAN IT BE DEVELOPED?

David S. Barnes and Sally A. Brearley

Risk Management Department
AEA Consultancy Services
Thomson House
Risley
Warrington, WA3 6AT
United Kingdom

INTRODUCTION

In an industrial environment, enquiries into the causes of accidents often concentrate on the immediate technical reasons for its occurrence. While these have to be established through examination of all the evidence at the scene of the accident and subsequent technical investigations and calculations, this can often be at the expense of the underlying causes of such incidents. The use of enquiry teams in such a manner can be costly and time consuming and the use of so-called technical experts, while good at apportioning blame can often fail to identify the underlying causes. This can happen because, while they have undoubted technical expertise, their understanding of human factors in accident situations and in safety management issues has been insufficient. This was highlighted in a recent publication from the Advisory Committee on the Safety of Nuclear Installations (ACSNI) in the UK[1].

Recent research work, for example the AEA's Management at Risk Guide[2], has found that the underlying management and organisational failings contributed significantly to the multiple causes of these accidents. As a result of analysing the causes of a number of recent major accidents including Bhopal, Three Mile Island, Chernobyl and some major disasters in the United Kingdom including Flixborough (chemical plant), the Herald of Free Enterprise (ferry accident), Clapham Junction (railway accident), Kings Cross (underground station fire) and Piper Alpha (oil rig fire), the focus on the concept of "Safety Culture" has increased.

DEFINITION OF SAFETY CULTURE

The term "Safety Culture" is now commonly used to refer to the wider management and organisational factors that help to determine human behaviour in an organisational context. There is a lack of common agreement on the exact definition of Safety Culture, but the

importance attached to the concept and its recognition as a prime determinant of safety performance is now well established.

So what is Safety Culture? Safety Culture has been defined by Pigeon[3] as:

> *"the collection of beliefs, norms, attitudes, roles and practices shared within a given grouping".*

In the nuclear safety field, the notion of safety culture was considered by the International Nuclear Safety Advisory Group (INSAG) of the IAEA[4] following analysis of the Chernobyl accident. Their definition of safety culture was presented as:

> *"that assembly of characteristics and attitudes in organisations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance."*

The IAEA document proposed that safety culture has two major components; firstly the framework determined by organisational policy and by managerial action and secondly the response of individuals in working within and benefiting by the framework.

These preceding approaches to safety culture will be discussed in this paper. It will also discuss how safety culture can be measured, assessed and developed within an organisation, and the experience of AEA Technology within the UK regulatory framework will be used for illustration.

COMPONENTS OF SAFETY CULTURE

The Management at Risk Guide, while not making a clear definition, considers that the role of a safety culture is to ensure that every individual in an organisation will make decisions that are in line with the corporate commitment and objectives. Although the commitment is required from the very top of the organisation, it is the culture that will ultimately ensure the attainment of the corporate safety policy objectives. Corporate management must continually develop and maintain the safety culture by demonstrating conviction and commitment through:

- providing a framework of policy and management systems
- implementing the policy
- monitoring the performance of the policy.

Providing The Policy

In the UK it is a requirement of the Health and Safety at Work etc Act[5] for all companies employing five or more persons to provide a safety policy. The provision of a corporate safety policy at a high level within an organisation is therefore a most important activity since it can create a basis for a positive approach to safety management. It is also essential for promotion of a positive safety culture, but it should not merely pay lip-service to concepts of health and safety. It needs to establish the corporate attitude to safety and the framework through which safety objectives can be assured; in addition the policy needs to be regularly reviewed.

It is essential that there is a firm commitment from the top of an organisation; as well as providing the policy, there must be adequate resourcing. Evidence of positive action, involvement and response will also be reflected in the performance monitoring systems. It is well known that the success of organisations in eliminating hazards and accidents results

from applying policies laid down at Board level and progressing them through the successive tiers of management.

In AEA Technology, the provision of safety policy and arrangements has been a regular feature of the company for a number of years. It is described as a statement to all employees on the AEA's policy on safety and a description of the key elements of the company's safety arrangements[6]. The policy includes most of the requirements for a written safety policy including the general principles, responsibilities for safety, policies on workplace and radiological safety, emergency planning, training and the availability of expertise on safety. The safety arrangements include the role of the corporate safety body, occupational health and plant safety, review and consultation, inspection by external bodies, emergency arrangements, incident reporting and investigation, quality assurance and liaison with the local communities.

Implementing The Policy

Implementation of the safety policies within the organisation requires strong lines of authority to be established for safety matters, with clear reporting lines and the minimum number of interfaces. It can be too easy to produce policy statements which are difficult to implement, because of conflicting organisational objectives. They must be compatible with other objectives as they are propagated down the organisation. To ensure the proper communication of objectives and priorities, it is also necessary to set out the responsibilities and accountabilities for the translation of objectives into detailed engineering and operational requirements.

The safety policy must set out clear guidelines as to how the organisation's existing structure will deal with implementing the corporate safety policy. The component parts of an organisation may have different interests, different management styles and different approaches of investment responsibilities. In addition, like AEA Technology they may occupy several different sites. The safety policy thus requires clear identification of responsibilities and lines of communication and control, cutting across internal structures.

Thus on a more detailed level, the safety policy needs to be translated into lower tier documents according to the organisation's requirements taking into account other company policies and relevant legislation. Thus, for example, in the UK a company has a legal responsibility to comply with legislation, notably the Health and Safety at Work Act 1974 and with specific regulations made under that Act and other statutes; in particular the Ionising Radiations Regulations 1985, which forms the basis for the protection of individuals arising from work with radioactivity. There is an onus on both employers and individual employees for the safety of operations under their control.

Policies must also include provision of safe and healthy systems of working through ensuring that plant and equipment are designed, constructed, operated, maintained and decommissioned in a safe manner; this requires taking all reasonably practicable steps in identify, assess and eliminate hazards and, should accidents occur, minimising the consequences.

Lower tier documentation must also reflect the company's commitment to recording, reporting, investigating and analysing incidents to improve safety practices, applying QA procedures to safety arrangements, provision of facilities for treatments of injuries and illness and provision of arrangements for presenting information on safety of operations and health of employees. Arrangements for emergency planning and training are equally important and need to be developed in lower tier documentation.

This covers the organisation itself and the systems the organisation develops. However, there are other features, the so-called "soft" ones that are just as important. Recent research by the USNRC[7-9] has suggested that safety performance is influenced by aspects such as good communications between and within levels in an organisation, good organisational learning, a strong focus on safety by the organisation and by individuals and external pressures.

Empirical evidence[1] has shown that accident rates tend to be lower where resources are devoted to safety, participative relations exist between staff at different levels, management visibility is high in operating areas and appropriate training is given a high profile including management training, formal safety training and safe skills training.

Other factors that affect culture and are linked to safety are perceptions and attitudes of staff, risk awareness and perceptions of staff (including managers), assessment (self assessment and by others), leadership (with the emphasis on more participative styles), the management of stress and violations; the latter concerns the intentional breaching of rules or short-cuts in safety procedures due to conflicts, inadequate understanding of rules, difficulty of implementation or production pressures.

In AEA Technology, the safety policy has been implemented by the production of a series of corporate documents:

- Corporate Safety Directives[10]
- Corporate safety Guidance Notes
- Site Safety Instructions.

The Corporate Safety Directives provide a framework for disseminating the policy; the Guidance Notes provide a major input into the safe operation of the AEA's plants. The series of Site Safety Instructions correspond to the specific site licence conditions for which arrangements are required to be made; the production of these arrangements is necessary for an individual site to be granted a licence by the regulatory body in the UK - the Nuclear Installations Inspectorate.

The above documents are implemented into a wide ranging series of procedures on a business level and ultimately on a plant level as procedural, operating, commissioning, maintenance, testing etc. instructions.

Monitoring The Performance Of The Policy

It has been suggested that the reasons for monitoring safety policy are:

- making sure the policy is happening
- ensuring reinforcement of objectives and commitment
- providing a mechanism to cope with complex, dynamic systems
- demonstrating positive action and response from managers.

The aspects that need to be monitored are the communication from managers, the implementation of the safety policy through working safety programmes and the results from the operation of safety programmes. Performance monitoring can be carried out in two ways; either setting up a system and remaining passive or investigating actively. The latter course can demonstrate commitment and strengthen the culture, whereas the former often only reacts to negative performances.

In the past, conventional measurements of safety performance have included accident statistics such as numbers of accidents, lost time injuries, but these can be misleading or even dangerous. Their weaknesses are well known and they can only provide limited information on the requirements to reduce accidents in the future. Safety is a characteristic that is never appreciated until something goes wrong.

Monitoring performance should reflect all activities in an organisation from the highest management levels to those at the operational level. At the latter level, monitoring performance can be achieved by audits, assessments, incident reporting and investigation; this needs to be translated to a form by which senior managers can appreciate how well the policies are performing and how good the safety culture is.

Again the "soft" issues are of interest. In the monitoring area, organisational learning is important where organisations should be seen to be learning from best practice and accident analysis, should be disseminating new information or information accrued from

reviews and incorporating this into current practices. The attitudes of management are again important for reviewing safety culture, for devising indicators of safety culture and for implementing changes that are necessary in the light of findings from such reviews.

In AEA Technology, individual businesses run audit programmes on a regular basis throughout different departments. These can cover wide ranging issues such as compliance with maintenance and modification procedures, use of respiratory protection equipment, heeding the requirements of basic radiological protection etc. In addition, investigations are carried out into all incident reports, but at the appropriate level to the potential significance of each incident.

Further, since the AEA, like all licenced operators in the UK, come under the jurisdiction of the regulatory authority, the Nuclear Installations Inspectorate, they are also audited by the NII; this occurs more usually when a concern arises within the industry over a particular issue, but can equally happen when a particular area of operations is randomly selected, eg. waste management, permit to work procedures.

SAFETY CULTURE IN AN OPERATING PLANT

AEA Technology, formerly the UKAEA, has developed from the major UK nuclear research and development organisation in the 1950s, to a world class service business, using scientific and engineering skills for the benefit of a wide range of customers. The services are delivered through seven business units, each responsible for particular fields of activity. These operate from six scientific and engineering centres in the UK with smaller offices close to customers in the UK and overseas.

Within some of the business units, AEA Technology still operates a number of nuclear plants, including a prototype fast reactor. Safety considerations have always played a key part in plant operations. This started almost 25 years ago when safety working parties were set up to monitor safety documentation for the facilities and to review the safety of past operations. This has developed over the years as safety assessment methods have evolved, specifically the need for each operating facility to produce a Safety Case for plant operation. These are "living" documents which need to be reviewed periodically.

In AEA Technology in the UK, the responsibility for the safe operation of active facilities is vested in the appropriate Business Directors, but the safe management of individual facilities is delegated to specific Plant Managers who hold the "operational certificate" for the plant, known as the Authority to Operate (ATO). This ATO specifies, through a series of fundamental documents, the operational limits on which the plant must be run. This series of documents is generally limited to the Operational Safety Case, the Maintenance Requirements, the Operational Envelope and the Business Safety Management Procedures.

All of these documents are essential. The Operational Safety Case demonstrates that the facility can be operated in a safe and efficient manner within the company safety policy and criteria and current regulatory criteria. The Maintenance Requirements indicate the engineering (mechanical, electrical etc.) conditions that are required to be satisfied before the plant can be operated.

The Operational Envelope specifies other non-engineering (staffing, discharge limits etc.) requirements which are also needed to be in place before commencement of operations. Finally the Management Procedures are those fundamental administrative requirements which should be adhered to or invoked during the operation of the plant.

The above features, however, merely consider the most direct aspects of the system for operating a plant. Other features are just as important; these include the training of operators, including refresher training, the control of modifications on the plant, the proper use of the permit to work system, the encouragement of reporting of and the appropriate investigation of incidents, the testing of the emergency procedures, the review of all documentation

including operating instructions and the self-auditing of these and other safety characteristics.

The organisation also operates a policy of reviewing plant operations annually; this normally forms the basis of issue of an ATO for a further period of one year. It is important that not only are the direct safety aspects fully covered, but also the apparently indirect or "softer" issues. This can often be assessed from plant management's attitude to safety reviews and their general responsibility and responsiveness to safety issues. A good manager will be active in many areas such as up-to-date documentation, review of incidents etc. but will also have a positive attitude to safety culture on the plant through review of operator and management training, learning from incident investigations and his/her general leadership qualities and presence on the plant.

FURTHER DEVELOPMENTS IN SAFETY CULTURE

The AEA's Management at Risk document[2] suggested there were seven steps in developing and retaining a good safety culture which were:

- demonstration of conviction and commitment at the highest level
- the setting of objectives and standards at the highest level
- propagation of objectives and standards throughout the organisation
- raise awareness and involvement of individuals throughout the organisation
- monitor and audit performance throughout the organisation
- use of proactive follow-up measures to eliminate deficiencies and take new initiatives
- listen to concerns of all staff in the organisation.

As already described the first four components are concerned with policy making and the last three are closing the loop in terms of monitoring and follow-up to sustain the culture.

This paper has attempted to raise the overall issues which can develop an improved safety culture within an organisation. These are all key areas which develop from the organisation's safety policy. There are, in addition, a number of other issues which are important, but which are less easily defined. These are the so-called "soft" issues and include such areas as communications, self assessment, leadership and management of stress.

REFERENCES

1. Advisory Committee on the Safety of Nuclear Installations. ACSNI Human Factors Study Group. Third Report: Organising for Safety. MERELY. 1993.
2. A.M. Jenkins, S.A. Brearley and P. Stephens. Management at Risk. SRDA-R4. AEA Technology. 1991.
3. Pigeon, N, Safety Culture and Risk Management in Organisations, Journal of Cross-Cultural Psychology, 1991.
4. International Atomic Energy Agency. International Nuclear Safety Advisory Group. Safety Culture. Safety Series No. 75-INSAG-4. IAEA, Vienna, 1991.
5. Health and Safety at Work etc Act 1974. MERELY. 1974.
6. AEA Technology. Safety Policy and Arrangements. April 1992.
7. United States Nuclear Regulatory Commission. Human Factors Regulatory Research Program Plan. USNRC-NUREG 1384. 1989.
8. United States Nuclear Regulatory Commission. Influence of Organisation Factors and Performance Reliability. USNRC-NUREG CR-5538. 1991.
9. United States Nuclear Regulatory Commission. Performance Indicators Project, A Summary of Frameworks. USNRC-NUREG CR-5610. 1992.
10. AEA Technology. Corporate Safety Directives. August 1993.

SAFETY CULTURE AND ITS REFLECTIONS IN JOB AND ORGANIZATIONAL DESIGN: TOTAL SAFETY MANAGEMENT

Gudela Grote and Cuno Künzler

Work and Organizational Psychology Unit
Swiss Federal Institute of Technology,
ETH-Zentrum, 8092 Zürich, Switzerland

ABSTRACT

Based on existing models of safety culture, especially the model developed by the International Nuclear Safety Advisory Group (INSAG), and the sociotechnical systems approach an extended model of safety culture termed Total Safety Management is suggested. This model stresses not only characteristics directly related to safety like safety guidelines, training programs, operating procedures etc., but also characteristics of job and organizational design that can be assumed to have an indirect effect on safety as they influence the degree of control over variances and disturbances by the operators in the production process. Some preliminary results from several case studies testing the adequacy of this model are presented.

INTRODUCTION

In recent years, the focus of research into work and production safety has shifted from individual-centered analyses of operator errors, their causes and measures for their prevention to analyses of the sociotechnical system, emphazising factors like safety philosophy and safety management of an organization.

From the viewpoint of the sociotechnical systems approach, work systems consist of a technical and a social subsystem which interact in performing the primary task of the work system, e.g. producing certain goods or services. If safety is defined as a crucial aspect of the primary task, safety measures should penetrate the whole system instead of aiming at isolated human or technical aspects. Instead of focusing on the prevention of accidents, a variety of factors concerning work and organizational design should be considered as influencing a system's safety. Those factors can be understood as expressions of a safety culture.

In the following, current approaches to safety culture and the sociotechnical systems approach are outlined briefly in order to provide some background for the research questions studied. The research design and some results of the ongoing investigations are presented subsequently.

THE CONCEPT OF SAFETY CULTURE

The International Nuclear Safety Advisory Group (INSAG), among others, coined the term safety culture as "that assembly of characteristics and attitudes in organizations and

individuals which establishes that, as an overriding priority, nuclear safety issues receive the attention warranted by their significance" (INSAG, 1991, p. 1). The group also provided a framework for the "measurement" of safety culture by distinguishing characteristics of safety culture on the strategic, management, and individual level of an organization and giving examples of questions to assess these characteristics (Figure 1).

Similar characteristics to those in the INSAG-model have been identified by empirical comparisons between "safe" and "unsafe" organizations (e.g. Cohen, 1977; Zofar, 1980) and through analysis of active and latent failures leading to major accidents (Reason, 1990a/b). Frequently mentioned characteristics are management commitment to safety, safety training and motivation, safety committees and safety rules, record keeping on accidents, sufficient inspection and communication, adequate operation and maintenance procedures, well-designed and functioning technical equipment and good house keeping.

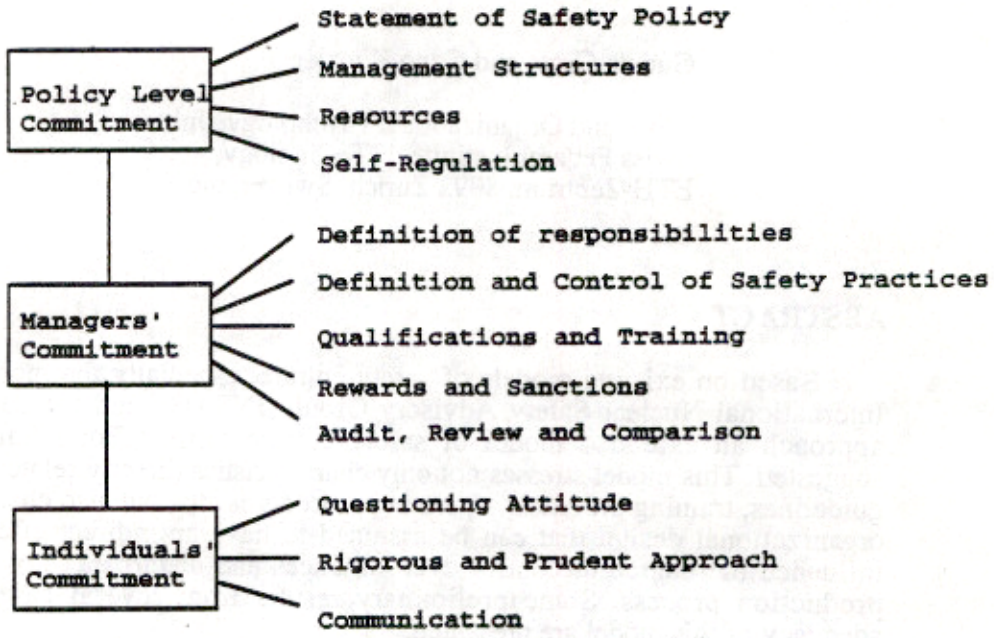


Figure 1. INSAG-Model of Safety Culture (INSAG, 1991)

A major problem with the existing models of safety culture is their lack of integration into general models of organization and of organizational culture, understood as the deeply rooted assumptions about human, societal and ecological categories shared by the members of an organization and their expression in values, behavior patterns, and artifacts found in the organization (e.g. Schein, 1985). Should safety culture be conceived of as a part of a more global organizational culture or is it a specific expression of or type of organizational culture? The definition of safety culture by INSAG refers to safety-related attitutes, but no mention is made of their connection to other norms in the organization. Also, the connection between safety-related characteristics of a system and more general characteristics, like job and organizational design and the use of technology, is missing. Thereby, the impression is furthered that safety can be looked upon and be promoted as something detached from the make-up of the sociotechnical system as a whole.

This view that the promotion of safety is an issue unrelated to questions of technology use and job and organization design, requiring separate norms, organizational resources, and implementation mechanisms, can also be found in industrial practice. Work organization and technology use in everyday operations are rarely planned with explicit reference to safety. Rather, they are planned with respect to production requirements and only afterwards tested against safety standards. The conflict between production and safety is not resolved, however, by pointing to the importance of safety through policy statements, extensive safety regulations, large safety staff, safety training etc. It can be argued even that the conflict is cemented in that way because safety is treated as something separate from everyday business. For the initial establishment of safety issues in an organization, this separation may be useful, but in order to achieve a "safety culture", safety has to become an

integral part of planning and operation. Under the heading of Total Quality Management, such an integral approach has been developed with respect to quality. Similarly, the establishment of a safety culture could be described as "Total Safety Management".

It is argued here that the sociotechnical systems approach can provide the basis for such a Total Safety Management. This approach and the resulting assumptions regarding the promotion of safety culture will be described in the next section.

A SOCIOTECHNICAL SYSTEMS APPROACH TO SAFETY CULTURE

As mentioned already, the sociotechnical systems approach conceives of work systems as having a technical and a social subsystem which together determine how well the primary task of a work system can be accomplished. Only if the two subsystems are jointly optimized, can maximum effectiveness be achieved. The predominant design objective is the provision of a high degree of self-regulation in the sub-units of the work system down to its individual members in order to allow for direct and flexible reaction to or proactive prevention of variances in the production process (cf. e.g. Emery, 1959; Ulich, 1991).

On at least two levels the sociotechnical systems approach can be linked to safety, i.e. the definition of the primary task of a work system and the degree of self-regulation of sub-units in the system. Starting from the assumption that work systems are created and designed with respect to the optimal accomplishment of their primary task, this task should be defined not only in terms of the quantity and quality of products or services, but should contain the safety of their production as well. Only when safety is understood as a central task inseparably linked to production, can one assume that safety measures will penetrate every part of the work system. Secondly, it is widely assumed that a high degree of self-regulation of work teams is beneficial to safety. This assumption has two roots, one is that especially in complex systems immediate reactions to variances and disturbances in the production process as well as anticipatory actions for their prevention necessitate the delegation of control to the lowest, i.e. shop floor, level (e.g. Perrow, 1984). The second root is the motivation model embedded in the sociotechnical approach, i.e. task orientation (Emery, 1959; Ulich, 1991). Tasks that among other things allow for a high degree of autonomy, task completeness and task feedback, will further an indiviual's intrinsic motivation. If, as derived from the definition of the primary task, his or her task includes safety, then motivation should also be directed towards that aspect of the task. Some empirical evidence for this assumption has been provided in studies on the effects of working in semi-autonomous work teams where it could be shown that accidents and unsafe acts decreased (Trist et al., 1963; Trist, Susman & Brown, 1977).

On the basis of these links between sociotechnical systems design and safety, it is suggested that the existing models of safety culture should be extended by characteristics of the work system not directly related to safety, especially characteristics of job and organizational design influencing the degree of self-regulation on the shop floor. Another important design aspect in highly automated systems to be mentioned here - without being able to discuss it further - is the task allocation between operator and technical system, as the often impossible job demands placed on operators of those systems (e.g. Bainbridge, 1982, describing those "ironies of automation") relate quite directly to a system's safety.

Finally, as mentioned earlier, a model of safety culture should be incorporated into a more general model of organizational culture (e.g. Schein, 1985). In addition to elements included in existing models of safety culture, at least two aspects should be looked at: (1) the chosen form of work organization, its underlying assumptions - e.g. regarding the nature of human activity and the necessity of control -, and its consequences for individual work tasks and (2) management philosophies on automation and human reliability and their expressions in the actual division of functions between human operators and machines. Both of these aspects have been pointed out as relevant to the safety of work systems by a number of authors, but they have not yet been linked to the idea of safety culture.

RESEARCH DESIGN

The goals of the research are twofold. Firstly, the assumptions outlined above concerning the relationship between sociotechnical design and safety are tested within the limitations for operationalizing the concept of safety itself. Reason has described these difficulties quite well: "Chance conjunctions and ever-present hazards can bring catastrophe to the best-run organisations. Accidents, significant events and even lost time injuries, having large stochastic components, can only give us a very peculiar sampling of an organisation's strengths and weaknesses" (Reason, 1990b, p. 15). Secondly, the feasibility of safety analysis and design of safety measures based on the extended model of safety culture are investigated.

For the investigation of the various aspects of safety culture and means of their analysis, comparative studies in three chemical companies and one transportation company are carried out. Data are obtained by a variety of methods:

- interviews with safety officers and managers in production and technical support dealing with safety policies, automation philosophy, general principles of work organization etc.
- questionnaires for production workers dealing with their work situation and their views on safety in their company
- observations of production workers during their regular work in different production areas with different degrees of automation in order to describe differences in jobs based on different types of technical conditions
- analysis of documents like organizational charts, safety regulations, descriptions of work procedures, and accident reports.

RESULTS

Only a few results of the ongoing investigations will be presented, given the space limitations of this article.

Comparing the four companies with respect to the definition of their primary task, one finds that safety is an integral part of the primary task mainly in the transportation company. Public transportation, which is the task of this company, has always been linked to safety more than industrial production. In chemical plants, safety has only gradually increased in importance, often as a reaction to major accidents. This basic difference can also be found in the companies' safety organization. In the transportation company, there are few special safety staff, just working on safety matters; instead, the responsibility for safety is integrated into all safety-relevant jobs. In the chemical companies large groups exist whose main job is the design of safety measures, risk analyses, safety training etc.

Table 1 summarizes the answers by chemical shift workers and managers, rail traffic controllers and engine drivers to the question whether in their opinion safety comes first in cases of conflict with immediate production requirements. The scale ranged from 1 to 5, 1 meaning "Safety first". The respondents were also asked to indicate whether they thought improvements necessary in the way conflicts between safety and production were dealt with.

The results show that in general the respondents thought that the Safety First-principle was operating, even though improvements were still possible. However, the rail traffic controllers and engine drivers were more content than the chemical workers. Differences between managers and workers in the chemical plants indicate that the Safety First-principle might be more a dictated than a lived-by norm. Finally, the worst results were found in Company A which experiences the most economic pressure of the three chemical companies.

These results provide some support for the assumption outlined earlier that conflicts between safety and production can more likely be solved in favor of safety in organizations where safety is understood as an integral part of the primary task of the work system.

Table 1. Perception of the Safety First-principle in four companies

Company	Respondents	Agreement to "Safety First"	N	Percentage wanting improvement	N
Transportation	Traffic controllers	1.33	55	17.3	52
	Engine drivers	1.63	32	26.7	30
Chemistry A	Shift workers	2.08	39	58.8	34
Chemistry B	Shift workers	1.59	32	32.0	25
Chemistry C	Shift workers	1.76	46	33.3	39
Chemistry All	Shift workers	1.82	117	41.8	98
	Managers	1.52	93	25.3	91

Questionnaire data on job perception ("Subjektive Arbeitsanalyse", Udris & Alioth, 1980; Table 2) were obtained from rail traffic controllers and chemical plant operators. They were asked to describe their jobs with respect to a number of characteristics linked to the task orientation model presented earlier. Scales ranged from 1 to 5, 5 indicating a high level of that characteristic. Despite all differences in production requirements, job conditions, degree of automation etc., the two groups perceived their jobs quite similarly, possibly because both jobs predominantly require production surveillance. Generally, the traffic controllers rated their jobs slightly higher, however. Both groups perceived low autonomy in their jobs, restrictions originating from time tables and operating procedures respectively. The largest difference was the higher demands the traffic controllers experienced as compared to the chemical workers. These demands are also expressed in the higher qualification required for traffic control. These employees all went through a three year apprenticeship while the chemical workers are often trained on the job over a few months.

Table 2. Job perceptions by traffic controllers and chemical workers

Job characteristic	Respondents	
	Traffic controllers N = 52	Chemical workers N = 113
Autonomy	2.89	2.98
Task variety	4.60	3.96
Task transperence	4.31	3.88
Social transparence	4.10	3.61
Task demands	4.88	3.94
Chances for development	3.94	3.57
Social support	4.22	3.70
Cooperation	4.06	3.72
Respect from supervisors	4.16	3.58
Adequate quantity of work	3.29	3.64
Adequate work difficulty	3.93	3.60

Analyzing the daily work activities of these two groups, again a number of similarites were found, especially some effects of automation were very similar: with higher degrees of automation, control tasks decreased while surveillance tasks increased; experience gained in less automated systems seemed crucial for operating automated systems because of a general understanding for production processes that is gained much better in manually operated systems. Other effects varied, depending on the chosen work organization, e.g. in chemical plants splitting the responsibility for working in the central control room and in the plant versus having workers do both jobs or requiring written protocols even in automated plants versus requiring protocols only in manually operated plants.

The analysis of the job situation for traffic controllers and chemical workers has not been completed. However, the opportunities for self-regulation can be considered quite low, especially in the chemical plants, given e.g. ever-present written procedures, strict hierarchical structures in decision-making, and strong organizational divisions between planning, manufacturing, and quality control. Also, the low qualification level of most chemical workers restricts the potential for self-regulation.

CONCLUSION

The results provide some first support for the assumptions underlying the proposed model of safety culture termed Total Safety Management. Discussions with safety experts and production managers in the companies studied have also shown that they readily acknowledge the link between safety and job and organizational design, especially with respect to problems arising from high levels of automation. At the same time very little has been done so far to put this knowledge into practice. It is hoped that the analysis and design instrument based on the extended model of safety culture, which will be the practical outcome of the research presented, can be helpful in establishing this link in industrial safety practice.

REFERENCES

Bainbridge, L. (1982). Ironies of automation. In G. Johannsen & J.E. Rijnsdorp (Eds.), Analysis, design and evaluation of man-machine-systems (pp. 129-135). Oxford: Pergamon.

Cohen, A. (1977). Factors in successful occupational safety programs. Journal of Safety Research, 9, 168-178.

Emery, F.E. (1959). Characteristics of socio-technical systems. London: Tavistock Document No. 527.

INSAG (1991). Safety culture. Safety Series No. 75-INSAG-4. Wien: International Atomic Energy Agency.

Perrow, C. (1984). Normal accidents. Living with high-risk technologies. New York: Basic Books.

Reason, J. (1990a). Human error. Cambridge: Cambridge University Press.

Reason, J. (1990b). Managing the management Risk: New Approaches to organisational Safety. Draft paper for Workshop on Managing New Technologies, Bad Homburg.

Schein, E.H. (1985). Organizational culture and leadership. San Francisco: Jossey-Bass.

Trist, E.L., Higgin, G.W., Murray, H. & Pollock, A.B. (1963). Organizational choice: The loss, redicovery and transformation of work tradition. London: Tavistock.

Trist, E.L., Susman, G. & Brown, G.R. (1977). An experiment in autonomous working in an american underground coal mine. Human Relations, 30, 201-236.

Udris, I. & Alioth, A. (1980). Fragebogen zur subjektiven Arbeitsanalyse (SAA). In Martin, E., Udris, I., Ackermann, U. & Oegerli, K., Monotonie in der Industrie (S. 61-68 und 204-207). Schriften zur Arbeitspsychologie (Hrsg. E. Ulich), Band 31. Bern: Huber.

Ulich, E. (1991). Arbeitspsychologie. Zürich: Verlag der Fachvereine; Stuttgart: Poeschel.

Zohar, D. (1980). Safety climate in industrial organizations: Theoretical and applied implications. Journal of Applied Psychology, 65, 96-102.

ASSESSING ORGANIZATIONAL IMPACT ON REACTOR SAFETY

Wei G. He[1]

[1]PLG, Inc.
4590 MacArthur Boulevard, Suite 400
Newport Beach, CA 92660-2027

ABSTRACT

This paper discusses a backward approach to evaluating quantitatively the role of organizational factors in reactor safety. This approach assumes that the conventional probabilistic risk assessment (PRA) models have implicitly included organizational factors when plant-specific experience have been inputted to the model. The approach starts with the determination of the core damage frequencies (CDF) for the interested nuclear power plant (NPP) and the population from which the NPP comes. The CDF differences between the plant and the population are identified, and the contributors are determined. The approach continues to assess the contributors to determine if specific plant practices are the cause. These plant practices are traced back to the plant management systems. Finally, the role of organizational factors can be evaluated to determine how these factors shape the management practices, which, in turn, yield the interested differences. It is found, by using this approach, that organizational factors impact the numerical values of basic variables, accident sequences, and CDF. The results indicate that organizational impact on CDF would not be much larger than a factor of 10.

INTRODUCTION

Considerable evidence has been accumulated in the last two decades to suggest that organizations who run NPPs might have impacts on reactor safety that are much more direct than the risk assessment community had realized. The NPP performance comparisons, and severe accidents studies have shown some direct influences of organization and management.[1,2,3] The U.S. Nuclear Regulatory Commission (NRC) concurred that "no level of technical safeguards can make a nuclear facility safe unless it has a good management." Attempts have been made within and outside the PRA community to link organizational factors to reactor safety, and considerable progress has been made. These investigations have been successful in identifying the general structure of NPP organizations.[4] Hundreds of organizational factors that are potentially related to reactor

safety have been identified.[5] Several pathways or mechanisms through which organizational factors impact nuclear safety have been proposed. [6,7]

Most of these approaches postulate the existence of direct organizational impact on the performance of NPP. Based on this consideration, researchers take the following three steps:

- Identifying organizational factors or organizational characteristics.
- Specifying pathways of organizational factors on reactor safety.
- Estimating the quantities of organizational impact.

It is usually assumed that organizational factors affect nuclear safety through its effect on the personnel performance. Therefore, the rates of human errors can be modified[4] or the likelihood of system in a wrong alignment after maintenance might be increased due to organizational factors[7].

Considerable insight has been gained due to these efforts. However, no credible methods have been established on how to determine the quantity of modifications that will be applied to human error rate or maintenance unavailability. Furthermore, the logic between the specific organizational factors and the impacted parameters, such as maintenance, is not clear. To fill a gap for organizational factor study, this paper outlines a method for estimating the magnitude of the modifications due to organizational factors by using the PRA framework and using CDF* as the NPP risk parameter.

USE PRA TO ASSESS ORGANIZATIONAL IMPACT

The conventional PRA model has specified a function or algorithm, F, that relates the CDF, through intermediate variables of accident sequences or minimum cutsets, CDF_i, to a series of elemental input variables, x_j, representing initiating events frequencies, failure rates of equipment, human error rates, and maintenance unavailabilities. The function can be written as

$$CDF = F(x_1, x_2,...x_j,...x_n) = \sum CDF_i$$

where j = 1,2,...n is the number of the basic variables included in the PRA model, and i = 1,2,...m is the number of accident sequences. The function F here can be referred to as the PRA model.

If we now consider organizational factors, OF, as an independent variable, OF can affect CDF only through its effect on the parameters x_j, accident sequences CDF_i, or the form of the function F. The effect of organizational factors can therefore be determined by computing functions $x_j(OF)$, $CDF_i(OF)$, and F. Thus, the basic question of (quantitative) organizational impact can be broken into the following questions:

- What is the effect of organizational factors on the parameters x_j that are already in the PRA model?
- What new parameters, x_{n+J}, where J = 1,2,...N, should be included in the function F to represent the organizational factors?
- What additional accident sequences, CDF_{m+I}, where I = 1,2,...M, should be added to the PRA model to represent organizational effects?
- What is the net effect of the organizational impact on CDF?
- What is the quantitative relationship between these new parameters/accident sequences and organizational factors?

The above approach breaks a difficult task into a number of manageable subtasks. The questions also specify a step-by-step method to measure the quantitative impact of

---

*As biased PRA practitioners, we use reactor CDF as the NPP risk parameter. The desirability of CDF to represent NPP risk is due to its comprehensiveness and its direct impact on public safety.

organizational factors. However, the above approach is based on a very important hidden assumption: the construction of the plant PRA model and the specification of its input are isolated from NPP's organizational factors; therefore, the effects need to be added.

This assumption might not be true since some of the organizational impact must have been captured by the input to the PRA model. For a NPP of long operating experiences, input data reflect the history of the operating characteristics. These operation characteristics should be influenced by organizational factors. If the PRA model is correct and the data analyses are performed rigorously, these characteristics that are shaped by organizational factors are inputted into the model through the plant-specific PRA structure and input data.*

BACKWARD APPROACH FOR ASSESSING ORGANIZATIONAL FACTORS

If impacts of organizational factors are implicitly included in the calculation of CDF, the task of assessing organizational impact becomes to separate the impact from other factors. For this purpose, the following backward approach is proposed:

1. Estimate the CDFs for the interested NPP and its population.
2. Determine the CDF differences between the interested NPP and the population.
3. Find the contributors of the differences.
4. Determine plant practices that are behind the contributors.
5. Link the plant practice to organizational factors.

This backward approach does not commit itself to the task of searching for new variables, x_{n+J}, and new accident sequences, CDF_{m+I}, as was outlined in Section 2. These parameters and sequences have not been observed with the worldwide experience of several thousand reactor-years. Furthermore, these parameters and sequences have not been revealed by hundreds of state-of-the-art PRAs. Therefore, even if they existed, their frequencies would not be much higher than 10E-4.

ESTIMATE THE CDFs FOR POPULATION AND-THE INTERESTED NPP

If reactors, about 108 in the U.S. today, are all the same, the task of determining the population CDF distribution is straightforward. Conventional statistics can be used to calculate the mean and to determine other attributes. However, for the current generation of reactors, it is rather a formidable task to estimate the population CDF since most NPPs are custom designed and operate in a somewhat different natural environment. Calculated CDFs range from 10E-3 to 10E-6, and, so far, there is no evidence to suggest that the NPP with a CDF about 10E-3 has worse organizational characteristics than NPPs with a CDF about 10E-6. Therefore, for assessing organizational impact, the population CDF distribution should be determined differently.

If we admit that all reactors are different and each from a unique population, some working assumptions are needed to develop engineering approximations for population CDF. The approach discussed in this study uses the following assumptions:

- Components, such as pumps, valves, switches, etc., used in NPPs are from the same population. Therefore, following equation can be used:

  $$x_{0j} = \sum_i x_{ij}$$

  where x_{ji} is the variable representing the performance of ith component in ith plant, and x_{oj} is the variable representing industry-average performance.

*One exception might be human error rates.

- The CDF obtained by input industry average data in the PRA model constructed for an NPP can be approximated as the population risk. Mathematically, this assumption can be expressed as follows:

$$F(x_{01}, x_{02}, \ldots x_{0j}, \ldots x_{0n}) = \frac{1}{m} \sum_{i=1}^{m} (x_{i1}, x_{i2}, \ldots x_{ij}, \ldots x_{in})$$

where i = 1 to m is the number of NPPs.

The assumption of components from one population is based on observations and studies of past PRA practices. This assumption is used implicitly by many organizations. For instance, INPO's safety system performance comparison is based on compatibility at the system level. The NRC safety system actuation indicators implicitly assume compatibility. With few exceptions, this assumption can be satisfied by continuously seeking similarity at the low level of components.

The other assumption used to obtain the population CDF is hard to prove analytically but it is intuitively appearing. Furthermore, it is a widely used method for deriving the base risk inherent in the design of the reactor. If the validation of this assumption becomes an issue, the French 900 MWe series PWRs might be a reasonable sample to examine its applicability.

Once these two assumptions are established, it is straightforward to determine the population and the interested NPP CDF. We simply use the same PRA model constructed for the interested NPP but input industry-average and plant-specific performance data.

DETERMINE THE CDF DIFFERENCE BETWEEN POPULATION AND THE INTERESTED NPP

CDF differences between the plant and its population can be readily determined by the following equation:

$$\delta CDF = CDF_p - CDF_0$$

where subscript 0 represents industry average and subscript p represents plant-specific parameter.

To study organizational factors, we would like to break the δCDF into its functional contributors. Differential parameters that are directly related to NPP functional activities such as maintenance, personnel (human error), and hardware can be defined to use the same format. For instance, the following parameter can be used to compare the NPP maintenance (m) impact on the CDF:

$$\delta CDF_m = CDF_{pm} - CDF_0$$

where CDF_{pm} is the CDF with industry-average data except maintenance-related input. Plant-specific maintenance data are inputted.

More detailed information can be obtained by specifying a lower level parameter such as maintenance on a particular system.

The above δ-parameters are not very convenient if the purpose is to compare NPPs across the board. As discussed previously, the CDF differs by several magnitudes, and this might also be true for different populations. Thus, δCDF may not be a good indicator for comparing organizational impact on plant safety. To assess and compare the impact of organizational factors, the ratio or fractional difference of NPP and population CDF should be defined as following:

$$M = CDF_0/CDF_p$$

$$\delta M = \delta CDF/CDF_p$$

Since $M = CDF_p/CDF_0$, M could be used to compare the risks of all NPPs. For instance, if M = 0.1, the plant would have a risk 10 times less than the average plant or M = 4 would

be 4 times more risky, regardless of CDF_0 values. Other parameters that are related to the NPP function can be defined the same way.

FIND THE CAUSES OF CDF DIFFERENCES

Due to the potential existence of one-of-a-kind customized design and unique external environment, some differences between the plant and population may not be contributed by NPP practices. Identified CDF differences between the NPP and population need to be screened to determine if factors other than NPP practices are responsible.

As was pointed out previously, the system uniqueness usually can be accommodated by seeking the standard components of lower levels. In practice, it may take an extra effort for an existing PRA model since the model might treat the equipment as one piece. If this is the case, sound engineering judgment may be more efficient in attributing the causes of CDF differences.

External environment may also cause some variations in CDF. For instance, one NPP is located in the East Coast, and its particular location is prone to coastal winter storms. These winter storms typically cause a loss of offsite power for the NPP. The corresponding frequency of loss of offsite power and CDF due to station blackout is substantially high. This phenomenon is not caused by plant practice, and is population related. Therefore, the population risk needs to reflect this external factor.

After technical and external contributors are screened out, the balances are more likely to be caused by plant management systems. The next step is to determine the plant-specific practices that contribute to the differences. For instance, plant poor maintenance strategies such as maintenance coordinations, spare parts stock, maintenance crew trainings, etc., cause long maintenance duration.

DETERMINE ORGANIZATIONAL FACTORS

Many works have been conducted in determining organizational characteristics and important organizational factors as were discussed earlier in the paper. This backward approach focuses the NPP practices that are direct causes of CDF deviations. The individual NPP-oriented approach is based on the observation about the nuclear industry shared by many researchers:[8]

> Organizational structure and characteristics of nuclear power plants vary according to their technological and institutional environments, to their life cycles and productions cycles.

After risk differences are identified, plant practices that contributed to these differences are determined. Plant-specific organizational factors that help to shape the management practices are then identified as contributors. The determination of organizational factors responsible for the CDF deviation can be difficult since the search is an inductive process.

APPLICATION AND RESULTS

The above method has been applied to three NPPs.[9] The primary results by using the above method indicate organizational factors have impact on CDF, and the method outlined above can measure the impact of organizational factors. The findings corresponding to the remaining three questions posed in Section 2 by using this method are as follows:

- Organizational impact changes the numerical values of x_i.
- Organizational impact changes the numerical values of accident sequences CDF_i.

- Organizational impact changes the ranking of the risk importance of parameters and accident sequences already included in the PRA model.
- The magnitude of organizational impact appears to be in the range of about of 0.1 to 10.

Other interested findings include:

- δM, appropriately corrected by a study of its contributors, can be used as an estimate of organizational impact.
- δM can be decomposed into its contributors.

Furthermore, it is found that several organizational factors are contributing to CDF differences. Among them, the activity ownership (who is responsible for the problem), line of communication (coordination of work across several functional areas), and maintenance crew and operator training seem to have direct impact on reactor safety. The application and results of this approach are discussed in Reference 9.

REFERENCES

1. R.N. Osborn and D.H. Jackson, "Leaders, Riverboat Gamblers, or Purposeful Unintended Consequences in the Management of Complex, Dangerous Technologies," *Academy of Management Journal*, Vol. 31, No. 4 (1988).
2. R.N. Osborn, et al., "Organizational Analysis and Safety for Utilities with Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington, D.C. (1983).
3. A.A. Marcus, et al., "Management, Organization, and Safety in Nuclear Power Plants (Draft Report)," NUREG/CR-5437, U.S. Nuclear Regulatory Commission, Washington, D.C., (1989).
4. "Influence of Organizational Factors on Performance Reliability," NUREG/CR-5538, U.S. Nuclear Regulatory Commission, Washington, D.C. (1991).
5. Organizational Factors Research Contractors Second Annual Meeting, University of Pennsylvania (1991).
6. V. Joksimovich, etc., "Organizational and Management Influences on the Safety of Nuclear Power Plants: Modeling and Measurements Using a Job Sampling Approach," NUREG/CR-5752, U.S. Nuclear Regulatory Commission, Washington, D.C. (1991).
7. G. Apostolakis, etc., "Quantification of Influence of Organizational Factors on Risk at Nuclear Power Plants," Organizational Factors Research Contractors Second Annual Meeting, University of Pennsylvania (1991).
8. "The MIT International Program for Enhanced Nuclear Power Plant Safety Progress Report," Cambridge, Massachusetts (1993) .
9. H.G. Wei, "A Method for Estimating Organizational Impact on Reactor Safety," Ph.D. Thesis, Nuclear Engineering Department, Massachusetts Institute of Technology (1992).

CONCEPT SAFETY REVIEW OF A SOCIOTECHNICAL SYSTEM

Geoff Wells and Christina Phang

Dept of Mechanical and Process Engineering
University of Sheffield
England.

AIMS OF THE SOCIOTECHNICAL SYSTEM CONCEPT REVIEW

The Concept Safety Review of a Sociotechnical System is recommended as a review procedure for a new plant at the conceptual or preliminary engineering stage. A keyword approach can be adapted as a means of generating discussion on the major elements affecting a system. These have been classified into the following subsystems:

- System climate
- External systems
- Organisation and management
- Site and plant facilities
- Communication and information
- Management control
- Procedures and practices
- Working environment
- Operator performance
- Equipment integrity

These systems have been further subdivided by keyword attached to each of which are selected preconditions for failure.

A study of such elements, backed by subsequent improvement, results in an overall reduction of risk on a plant which is impracticable to quantify but is acknowledged to be of considerable importance in practice, leading to order of magnitude changes in individual and societal risk. Subsequently the results from the analysis can be used in conjunction with other safety reviews to develop a safety schedule for the plant, modify risk assessments, and upgrade and improve the safety management system at the location.

The Procedure

The general procedure is outlined in Table 1. Each subsystem is reviewed by applying keywords which are specifically directed at key safety issues, usually specific parts of an incident scenario. The keywords are used in a similar way to those in a Concept Hazard Analysis; see Wells[3]. They enable the analyst to focus on major variances or deviations of the system from the ideal state. They also give guidance for exploring various facets of the sociotechnical system's character and expectations.

Table 1. Steps for concept safety review of a sociotechnical system

- ❒ Collect information on the main characteristics of the process system and its environment. This should include data on:
  - general information on the organisation and site
  - information on the safety management system
  - plant information and the main inputs and outputs
  - main incident scenarios
- ❒ Use keywords to identify preconditions for failure for each subsystem
- ❒ Note the main variances and how they affect system safety
- ❒ Record the discussion

Application of the Methodology

For new plants our system involves three stages of hazard identification: Concept Hazard Analysis, Preliminary Hazard Analysis and HAZOP. During a Concept Sociotechnical System Review, it has been found important to always refer when discussing a particular plant to specific postulated incident scenarios. This prevents the discussion becoming too general and leads to actions being more specific. Any general problem can be investigated later as part of a safety improvement programme, possibly involving the use of audits. Hence the main study is normally carried out on various incident scenarios when these are available i.e. following Preliminary Hazard Analysis. However earlier studies can be undertaken to tackle general points at the time of project review. As with all such methods it is a matter of setting aims and selecting keywords. Table 2 lists examples of keywords for the various subsystems.

The method can be used when carrying out the regular study of an existing plant and is particularly suitable for a rapid investigation of a near-miss incident. The approach is illustrated by a study of a major incident although it is stressed that the root causes identified do not necessarily relate to the particular accident.

The 'preconditions for failure' represent the root causes of incidents. These latent failures are often present in the system for a period of time and in combination with other factors can lead to a serious incident. They are usually listed separately on a proforma which has a column for the results of the initial discussion. The analyst can highlight the preconditions of failure identified in the review and may note down observations or follow-up actions which need further investigation or study.

The preconditions for failure are not intended to be comprehensive. The aim is to generate ideas and discussion. The main studies for a proposed plant should be carried out at an early stage of the project, at a time when the Concept or the Preliminary Hazard Review have been completed. The use of a specific incident scenario on which to focus attention is useful as the discussion can start by asking if an accident were to happen on this plant what factors would be identified as being deficient. This approach leads to a more structured discussion which relates to the specific problem rather than descending to a general gossip about company ills and problems.

The work can subsequently be extended by its use to help develop the safety schedule. The way that it changes the values of equipment failures, loss of control, reduction of protective and mitigation systems should be noted. It is also particularly useful if ways can be suggested for appropriate system defences and appropriate performance indicators to monitor.

Table 2. Root cause categories, keywords and preconditions for failure

System Climate	External Systems
Technical adsorption Legislation/regulations Political climate/pressure groups Economic climate/business factors Business focus Corporate culture Safety culture	Governmental bodies Industrial bodies Contractors/consultants General public External emergency facilities
Organisation and Management	**Site and Plant Facilities**
Decision-making hierarchy Commitment to safety Resource provision Interaction with internal/external systems Production resources	Site and its layout Preliminary engineering and process design Detailed engineering Commissioning and realisation of plant Transport, storage, use and disposal of material
Management control	**Working environment**
Resource allocation and development Monitoring, quality control and appraisal Management of change Competence/capability of management Management responsibility and accountability Supervision and control Safety responsibilities Handling emergencies	Working environment Welfare Safety culture Immediate supervision and support
Communication and Information	**Procedures**
Information quality Safety information Channels Media interface/exchange Emergency response information Emergency communication	Working practices and procedures Safety studies Quality control Emergency procedures Incident reporting
Operator Performance	**Engineering Integrity**
Recruitment Personnel capabilities Training Inadequate working disciplines	Quality of plant Availability Maintenance Plant upgrading/modifications Standards and codes Safety and operating margins

FURTHER STUDIES

The Concept Sociotechnical System Review can be combined with the Concept Hazard Analysis and the Preliminary Hazard Analysis to set up a Safety Schedule which is to be developed for the plant. Such a schedule contains specific information on material hazards and inventory, incident scenarios, the immediate causes of incidents and the engineered protection and mitigation systems. The extension within this schedule of some reference to root causes is possible. This should if possible refer to specific factors and indicate how deficiencies can be measured using performance indicators and where specific engineered defences can be instigated. This document can be built up over the life of a plant and can be used to demonstrate

in an auditable form the quality assurance measures carried out on the project. The focus on the development of incident scenarios is vital. It emphasises what the study is about and stops it becoming perceived by workers at the sharp end as yet another exercise and demonstration of management efficiency. The schedule is further backed by monitoring that adequate change procedures are in place and that the updating of documentation and training is conducted.

The study of the sociotechnical system can be used to modify generic values of risk. For an excellent well-run plant the values of risk will be improved. However for a worse case the risk is increased. The way the risk on a plant which is not being properly maintained with defences intact will not be wasted on those who are familiar with major incidents such as occurred at Bhopal and Piper Alpha. Any deficiencies noted either now or in the future can be prioritised according to risk for immediate action.

CASE STUDY OF A REFINERY INCIDENT

We have based the following study on an actual incident[1] which occurred at Grangemouth, Scotland in March, 1987. In this incident a fire of flammable liquids, unexpectedly (although foreseeably) present, released during maintenance of a refinery flare system, killed two men and seriously injured two others. We are not in a position to state that the root causes which we have identified actually were those responsible. Consequently the study must be treated either as referring to a similar incident or as fiction.

The Flare Line System

Briefly the flare line at the refinery consisted of a complex system of pipework which passed through the refinery. It was discovered that a crossover valve (V17) was not providing effective isolation and would need to be removed for overhaul. As stated in the report, HMSO[3], the senior operations and engineering staff held discussions to plan a scheme for the isolation of the flare system at valve V17. They concentrated on the operational and safety requirements of the refinery and the flare system. The procedures and safety precautions necessary for the removal of the valve V17 were left to those who would eventually be responsible for the work.

A simplified version of the system of interest, indicating the valves to be closed for isolation of valve V17, is shown in Figure 2.

The Development of the Incident

Following due discussion and taking of precautions such as provision of respiratory equipment, fire protection etc. a cold work permit was issued and work was started on removing the valve by loosening a flange so that a spade could be inserted. Work continued although there was a persistent loss of flammables occurring from the initial break of the joint. This loss provoked considerable concern by the fitters such that the process shift supervisor checked the situation and reassured the fitters that it was safe for work to continue. Despite efforts to take care when lifting, as the last bolt was undone the crane increased its lift and the spacer suddenly sprang upwards. Gallons of liquid were suddenly released and a cloud of flammable vapour formed from the rapidly spreading pool of liquid on the ground. This was ignited at the compressor which was supplying the airline of the breathing apparatus of the workers. Fire flashed back around the working area. A fitter and a rigger could not escape from the scaffold and were killed. Further information is available in the report and can be discerned by study of Table 3. The model of incident scenario used here is based on work by Wells et.al.[2]

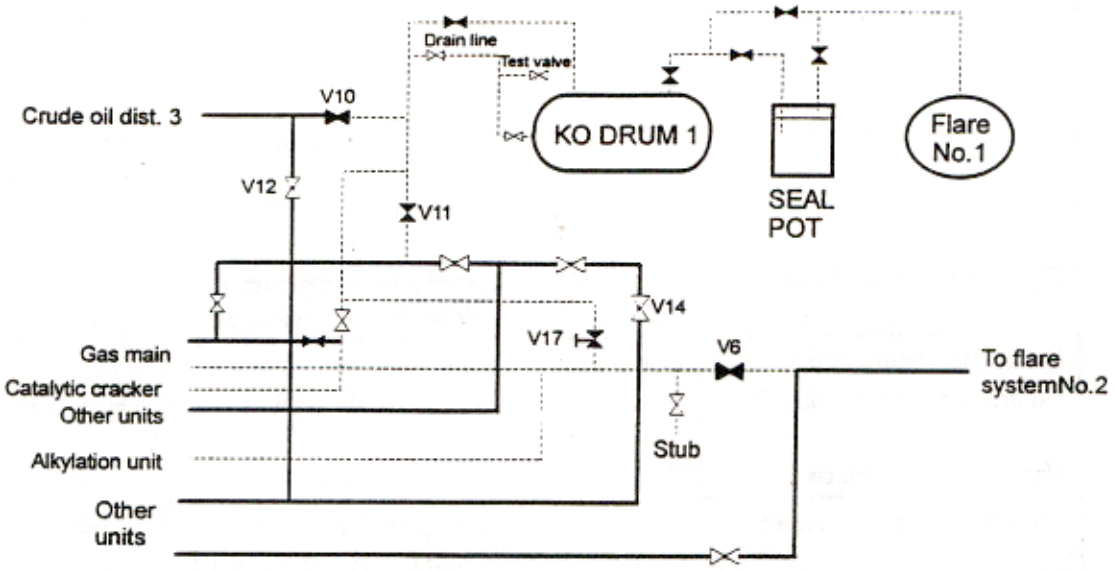


Figure 2. The section of the flare system to be repaired

Root Causes

This incident has been studied by various groups of safety specialists. In no way can their comments be said to represent the conditions applying at the time this incident occurred. Nevertheless using the keywords supplied plus peoples experience it was possible in under two hours to generate the root causes given in Table 3. The first part of Table 3 refers to the hazard scenario. The root causes were not mentioned as such in the report of the incident. It is interesting to note that they are considerably greater in number than the events describing the incident scenario from immediate causes. Somewhere there is a lesson in this when one consider that the latter represents the activities of all the hazard studies normally carried out on a plant. The safety experts in general felt some sympathy towards the need to cope with production pressures. They also were aware that the release of some flammable when such systems are repaired is not a rare experience. However it was felt that the design was inadequate, that procedures and practices needed considerable improvement particularly with respect to isolation, and that the level of management control was unacceptable. Attention to any of these factors did not need hindsight and should have been implemented.

ACKNOWLEDGEMENT

Christina Phang is sponsored by the Health and Safety Executive whose assistance in this project, particularly from Dr Nick Hurst, is gratefully acknowledged.

REFERENCES

1. HMSO 1988 *The fires and explosions at BP Oil ((Grangemouth) Refinery Ltd. A report of the investigations of the Health and Safety Executive into the fire and explosion at Grangemouth, Scotland, 13 March 1987.* HMSO, London
2. Wells, G.L. and Phang C.M.C. 1992. *A demonstration of the use of HAZCHECK and a systems example by an analysis of a recent refinery line accident.* Loss Prevention Bulletin 105. pp 25-34.
3. Wells, G.L., Wardman, M.J. and Whetton, C.W. 1993. *Preliminary safety analysis.* Journal of Loss Prevention in the Process Industries., Vol.6, No.1, p47-60.

Table 3. The incident scenario and suggested causes of pipe line release

Impact of the incident	Flash fire caused 2 fatalities and 2 people injured
Escalation of the release	Escalation by fire; failure to prevent upstream plants fuelling fire; inadequate emergency response; failure of fire protection; failure to exclude a source of ignition; inadequate escape procedures ; inadequate protection of personnel.
Significant release of material	Release of large flow of flammables through opened flange forming a liquid pool which vaporised; no means of attenuating the release.
Dangerous disturbance	Opening made in plant.
Failure to control the situation	Failure to stop the job on initial release of process material; inadequate monitoring of line.
Hazardous disturbance	Escape of material as flange loosened.
Immediate cause of incident	Loosening of flange whilst isolation of system is incomplete; task not completed properly with failure to stop the flange springing open.
Inadequate engineering integrity	Unable to isolate plant section; no spark arrestor on compressor; inadequate flare system, probably due to sending material outside design specification to stack; faulty reading of line pressure indicator; valves not closing properly and poor maintenance schedule; valve positioners needed; failure to upgrade piping system to company standards; failure to reconsider design when system deposits became excessive; drain line of poor design; general condition of valves and line poor.
Inadequate operator performance	Contract labour unskilled in process work; suspicious spindle positions ignored; crane operated incorrectly.
Inadequate working environment	Excessive pressure to complete the job; production needs dominant; overload and work pressure on supervision; lack of technical back-up; inadequate access and egress from location.
Inadequate communication and information	Absence of communication; engineering staff did not inform fitters of hazards; insufficient documentation of plan; no feedback on failures; failure to get advice from plant manager on release; failure to communicate emergency details to upstream plant; inadequate checking of isolation.
Inadequate practices and procedures	Inadequate procedures for closing valves and instruction of operators; failure of permit to work system; inadequate maintenance procedure in using crane and no flange spreader; work during flammable release.
Inadequate management control	Inadequate planning for task with roles and responsibilities inadequately defined; decisions on plan left to supervisors and maintenance team; operators left to own devices; fitters not involved in discussions on isolation; no system in place to deal with any problems which arise; poor emergency planning.
Inadequate organisation and management	Roles and responsibilities poorly defined; inadequate maintenance resources; lack of commitment to safe working practices; inadequate safety studies and hazard identification; no safety management system in place.
Inadequate site and plant facilities	Design of line and valves inadequate; location of valve inadequate for maintenance; inadequate assessment of risk of release; inadequate disposal of materials to stack.
Inadequate external systems	Inadequate know-how and safety awareness of outside contractors.
Inadequate system climate	Production pressures allowed to outweigh safety needs; complacency by originators of valve replacement job.

MANAGING HUMAN INDUCED RISK INVOLVING TECHNOLOGICAL SYSTEMS AND PROCESSES[1]

Thomas G. Ryan, Lee T. Ostrom, and
David I. Gertman

INEL/EG&G Idaho Inc.
P.O. Box 1625
Idaho Falls, ID 83415-3855

Key words: Human Factors, Human Reliability Analysis, Probabilistic Risk Assessment, Function/Task Analysis, Human Vulnerability Analysis, Data Management, Configuration Management

ABSTRACT

Maintaining a safe operating environment is "Job 1" in complex high reliability systems involved in manufacturing, military, and energy development. New and better tools for managing risk and thus achieving and maintaining safe operations are continually being sought. One potential risk management tool is the probabilistic risk assessment (PRA). To date, PRA has been used primarily to provide a snap-shot of the risk associated with a system's current operating configuration. A major component of the PRA is an assessment of the human-in-the-system contribution to risk by means of human reliability analysis (HRA). In order for PRA to become a practical risk management tool, it must become a "living" rather than a "static" characterization of risk, including risk attributable to the human-in-the-system.

This paper addresses two primary human-in-the-system issues that must be resolved if "living HRA" is to be used as a tool for managing person-induced risk in technological systems and processes of the types associated with Department of Energy (DOE) reactor and nonreactor nuclear facilities. The first issue involves dynamic pictorial and descriptive analyses of human action sequences with potentials for impacting risk, achieved by means of dynamic function, task and human vulnerability analyses. The second issue involves configuration management of data emerging continuously or at regular intervals from the HRA, including changes in the human action sequences, usable for benchmarking and trending human performance, and achieved by means of a dynamic Personnel Data System (PDS).

---

1. The views expressed herein are solely those of the authors and do not necessarily represent those of EG&G Idaho, Inc. or the U. S. Department of Energy.

INTRODUCTION

Increasingly, managers and operators of complex high reliability technological systems and processes (e.g., aerospace, military, nuclear) are being required to demonstrate that their safety margin, or safety envelope, is sufficient to justify risks that might accrue to the general public and the worker. The most commonly used method for assessing the safety margin is the probabilistic risk assessment (PRA); an element of which is HRA.

Until recently, HRA segments of PRA have developed static indices for benchmarking human performance impacts on the safety margin, where impact is defined as contribution to core damage frequency, injury to workers, or off-site release. Presently, DOE and other Federal agencies such as the Nuclear Regulatory Commission (NRC), are searching for ways of making HRA dynamic or "living." Specifically, HRA techniques are being sought that are capable of continuously tracking changes in the safety margin due to shifts in the human operating configuration (e.g., staffing, operating procedures, training, human-machine interfaces, physical environment, management oversight).

REQUIREMENTS OF LIVING HRA

Changes are required in the way HRA is carried out and documented, to achieve a dynamic or living HRA whose results are near realtime, and are (1) more credible and auditable, (2) capable of supporting causal factor identification and repeated measurement, and (3) capable of combination with results of other analyses to provide risk management of issues that transcend any one analysis.

Credibility

Defensible HRA results require an experienced HRA analyst carefully using accepted human reliability analysis and quantification techniques. More specifically, defensible estimates of uncertainty require careful, standardized, conscientious, applications of the accepted techniques by experienced HRA practitioners well trained in the behavioral sciences, and armed with the appropriate contextual information (Reason, 1991). As a minimum, the HRA should account for human performance as a potential initiator and mitigator in all accident sequences analyzed in the PRA. More specifically, the HRA should include base case (current conditions) and best case (optimum conditions) estimates of human performance as potential initiators, and as potential mitigators either recovering an accident or initiating error, or conversely exacerbating an otherwise recoverable condition.

Auditability

An HRA must be well documented and traceable for the results to be practical and defensible. All steps, assumptions, information, and methods relevant to the analysis must be presented in detail, to allow a reviewer to understand the origin, understand the specific context, and assess the meaning of the results.

Support Analysis of Contributing Factors To Risk

The HRA must contain appropriate information to extend the identification and analysis of contributing factors to risk.

The HRA must produce results, quantitative or qualitative, that can be meaningfully compared to results from other HRA efforts. Such comparisons facilitate examination of HRA related issues of possible relevance across systems or facilities not originally included in a single analysis. To achieve such results, the HRA process, assumptions, and methodologies employed must also be carefully considered to determine valid comparisons of HRA results.

Achieving credible and auditable HRA results on a near-realtime basis, involves primarily (1) implementing dynamic function, task, and human vulnerability analyses capable of pictorially and descriptively mirroring changes in the personnel mission occurring continuously or at regular intervals, and (2) adopting a mechanism for configuration management of those function, task, and human vulnerability analysis changes, and other HRA input data changing continuously or at regular intervals.

DYNAMIC FULL SCOPE FUNCTION/TASK AND HUMAN VULNERABILITY ANALYSES

Appropriately detailed and well documented function, task, timeline, link, and human vulnerability analyses are the linchpin of a highly traceable and renewable HRA, provide the minimum information to determine the validity and meaningfulness of HRA results, and provide a basis for comparing these results with other HRAs.

Although some forms of function and task analyses are performed as part of current HRA, their updating is not usually pursued after the HRA is completed, unless a specific update to the HRA is required. In order for HRA to be used as a living risk management tool, dynamic full scope function and task analyses must be constructed and updated continuously or at specified intervals. They must be developed from detailed reviews of system documentation, operating experience, interviews with system personnel, walk-throughs/talk-throughs, and direct observations of system operations and maintenance activities. For a review of task analysis refer to Kirwan and Ainsworth (1992) or Drury, Paramore, Vancott, Grey and Corlett (1987). Function and task analyses must be updatable and describe in detail, on a near realtime basis, changes in the what, why, when, where and by whom of both human and hardware actions during system or process startup, normal operation, accident mitigation, accident recovery, and shutdown. They must continually provide the user with a credible and up-to-date technical basis for: (1) providing human factors inputs to logic or facility models used as a general framework for estimating overall system unreliability and risk, (2) identifying safety-related human tasks and task sequences needing probabilistic assessments, (3) specifying endogenous factors (e.g., personal ability, psychophysical state of health, motivation, mind set) and exogenous factors (e.g., person- to-person, supervisory, organization, external environment) believed to influence human performance on each task action and task action sequence, and (4) acting as a criterion for scaling the nature of those influences from positive to negative. Later, as part of a continuous HRA process, function and task analysis must provide the context for benchmarking and trending, on both quantitative and qualitative bases, the degree to which human performance is contributing in a progressively more positive or negative manner to: (1) system and process reliability and risk, and (2) system and process accident prevention and recoverability (Meister, 1985).

An iterative process of collecting function, task, timeline, link and human vulnerability analysis data provides a sound technical base for responding to each of the HRA requirements outlined in the previous section of this paper. The document review

gives the analyst an overview of the facility and an understanding of the human actions and action sequences that are actually used by the staff. The open-ended interviews, along with the facility's operating procedures are of great help in developing an outline of the functions, tasks, and subtasks that should be performed as part of each operating procedure. Once the outline of the functions, tasks, and subtasks has been completed, directed interviews help fill in any gaps in the understanding of the human actions and action sequences that make up the function/tasks/subtasks and help the analyst to understand the performance shaping factors (PSFs) that measurably impact either positive or negative performance of the functions/tasks/subtasks. Direct observations and table-top discussions are very useful in showing the interactions between individuals responsible for each function/task/subtask and furthering the understanding of the PSFs. Organizing resulting function/task/subtask information on a time grid, and presenting pictorially the interfaces among personnel, actions, and equipment, and their frequency, help the analyst visualize circumstances where institutional factors (e.g., management, organizational culture) might have their greatest impact on performance. Finally, screening for error vulnerability provides the analyst a rank ordering of human task actions and action sequences for consideration during later segments of the HRA.

Information for these analyses is sought from a wide variety of sources to ensure a complete and accurate picture of how functions and tasks are actually performed. Frequently, facility documentation is incomplete or out of date, and/or personnel have differing perceptions of how the functions and tasks of interest are supposed to be executed. Only by sampling all, or at least a representative mix of facility information sources, can credible representations of these functions and tasks be achieved.

DYNAMIC PERSONNEL DATA SYSTEM FOR CONFIGURATION MANAGEMENT

A dynamic Performance Data System (PDS) of the type described in draft NUREG/CR-5534 (1991), is required as an on-line repository, processor, and clearinghouse for dynamic function and task analysis information, human error probability source data, and HRA results continually being developed and trended based on the facility's ongoing experience. As such, PDS must be capable of serving two functions in a "living" HRA: the first as a data management system, the second as a configuration management system,

As a data management system, PDS must be part of the facility's larger configuration management and documentation control programs. This will ensure that all changes in the facility's operating configuration down to the system and component level will be screened and processed by PDS, and the updated quantitative and qualitative results will be systematically organized such that they can be: (1) communicated continuously among PDS users and HRA analysts, (2) fully audited, and (3) used as a technical basis for risk management by facility managers and oversight agencies such as DOE.

As a configuration management system, PDS must provide users and HRA analysts with up-to-date information in order for them to direct ongoing and planned HRA activities in a timely and cost effective manner. PDS must be capable of providing ready access to information and data to monitor progress in achieving each of the benchmarking and trending milestones of the living HRA. PDS must also be capable of flagging changes in function/task analysis and other source data, and trigger recalculations of risk.

In a living HRA environment, this monitoring, compiling, flagging, and triggering process allows PDS managers to: (1) conduct comprehensive reviews (quality, completeness, timeliness) of each continuing HRA activity, (2) allocate or reallocate resources including human factors expertise, facility personnel supporting the HRA, and

subject matter experts, based on progress being made on each continuing HRA activity, (3) coordinate and direct activities among the various human factors participants and between human factors and systems engineering participants, and (4) provide comprehensive and continuous outputs and reports to risk managers and Federal agencies such as DOE and NRC overseeing the operation of the facility.

CONCLUSIONS

This paper has examined the potential contributions that dynamic function, task, and human vulnerability analyses, along with a Performance Data System (PDS) can make in achieving "living" quantitative and qualitative HRA results which are: (1) credible, in that they minimize uncertainty, (2) auditable, in that they link quantitative results and qualitative information from which the results are derived, (3) capable of supporting contributing cause analyses on human reliability factors determined to be major contributors to risk, and (4) capable of repeated measures and being combined with similar results from other HRAs to examine issues transcending individual systems and facilities.

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

Drury, C.G., Paramore, B., VanCott, H.P., Grey, S.M. and Corlett, E.N., 1987, *in "Handbook of Human Factors,"* Wiley Interagencies, New York.

Kirwan, B., and Ainsworth, L.K. (editors), 1992, "A Guide to Task Analysis," Taylor and Francis, London.

Meister, D., 1985, "Behavioral Analysis and Measurements Methods," John Wiley & Sons, New York.

NUREG/CR-5534, 1991, "Task Analysis Linked Evaluation Technique (TALENT): Procedures for Implementing Human Factors Expertise into the Probabilistic Risk Assessment Process," U.S. Nuclear Regulatory Commission, Washington, DC: (Draft).

Reason, J., 1991, "Human Error," Cambridge University Press, New York.

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)

QUANTITATIVE RISK ASSESSMENT OF THE LOS ALAMOS NATIONAL LABORATORY TA-55 PLUTONIUM FACILITY

M. Kent Sasser and Dean Sanzo

Engineering and Safety Analysis Group
Probabilistic Safety Assessment Section
Los Alamos National Laboratory
Los Alamos, NM 87545

INTRODUCTION

Much of today's probabilistic safety assessment (PSA) methodology has been developed for nuclear reactors; however, it currently is being applied to nonreactor facilities. Government research, processing, and production facilities are under increasing emphasis to perform risk-based prioritization and use the results of quantitative risk analysis in decision-making. Although reactor risk assessments have concentrated on offsite health effects, numerous other consequences, including worker health effects and environmental impact, play a significant role in the management of these facilities. This paper describes a quantitative risk assessment of the Los Alamos National Laboratory TA-55 Plutonium Laboratory Complex currently being undertaken with the support of the US Department of Energy (DOE), Office of Engineering and Operations Support (DP-62).

FACILITY DESCRIPTION

TA-55 is a DOE facility supporting DOE defense research and development activities. The functional purpose of the facility is to perform basic special nuclear materials (SNM) research to develop, demonstrate, and exchange technology in support of national defense and energy programs. Both nuclear and nonnuclear are included in the facility inventory. There are several hundred hazardous chemicals, including a large inventory of nitric acid and various physical and chemical forms of plutonium, uranium, and other radionuclides. The laboratory is large, comprised of over 150,000 ft^2 of floor space and hundreds of gloveboxes in various laboratories housing specific processes.

The complex consists of a large main research building, the Plutonium Facility (PF-4), and a number of other administrative and support buildings.

- TA-50, the Central Liquid Waste Treatment Plant, handles relatively low-level radioactive wastes from many technical areas; it is located approximately 1200 ft east of TA-55. This area also includes TA-50-37, the Treatment Development Facility, which is located approximately 500 ft east of TA-55 and conducts R&D on radioactive waste management processes.
- TA-35, an extended area, begins about 1500 ft east-northeast of TA-55.

- TA-48, beginning 900 ft west of TA-55, is the site of radiochemistry studies and the Central Guard facility.

PF-4 is a reinforced concrete building designed and built to provide a high degree of safety and physical security. It was one of the first "modern" structures built within the DOE complex specifically designed to withstand severe seismic events and tornadoes. During the design process, attempts were made to incorporate the lessons learned from the first generation of plutonium facilities designed and built during the 1940s and 1950s at Los Alamos, Rocky Flats, Hanford, and Savannah River and to build a facility that could withstand all credible design-basis accidents, including severe seismic events (0.38 g), tornadoes (107 mph), and large-scale internal fires.

PF-4 is a single structure with approximately 151,000 ft^2 of total floor area built to Safety Class 1 standards. The outer walls and roof are of reinforced concrete; the walls are 14 in. thick and the roof is 10 in. thick. The building consists of a laboratory operating floor with a full basement level beneath. The basement contains both room air ventilation systems and electrical equipment. The basement clear ceiling height is 17 ft and the column spacing averages 20 ft. A service area containing ventilation ductwork is located above the laboratory corridors.

The building is divided into two halves by a 4-h fire-resistant wall. Each half is further divided into two compartments on the main process floor separated by a 2-h fire resistant wall. The compartments are referred to as the 100, 200, 300, and 400 Areas. Ventilation is independent for the two halves of the building. Support areas inside PF-4 include storage rooms, health physics offices and personnel decontamination facilities, process offices, etc. Support staff offices, management offices, and cold laboratories are all located within the other buildings at the TA-55 site. The north half of PF-4 houses the 100 and 200 Areas; the south half houses the 300 and 400 Areas.

The basement of PF-4 is divided into two areas separated by a 4-h fire wall and houses the critical support equipment for all of PF-4. This equipment includes the electrical switchgear, the uninterruptible power supply (UPS), and the HVAC equipment for the building. SNM shipping and receiving activities and waste management staging for transportation also are carried out in the basement. The storage vault for intermediate and long-term storage is located in the basement. The vault is divided into 13 compartments, each with a Class C fire door.

Several chemicals used in large quantities for PF-4 operations are stored in tanks both inside and outside the facility. Concentrated nitric acid is stored in a tank outside the building and is piped to bulk acid dispensers inside PF-4. Other chemicals used in large quantities are prepared in separate tanks within a separate facility and delivered to PF-4 through dedicated lines to selected areas.

The Facility Operations Center (FOC), which is of Class 1 construction, is also part of PF-4 and is immediately adjacent to the Support Building (PF-3). The remainder of the support building contains change rooms, cold support laboratories, and a machine shop. PF-5 is a warehouse.

Other buildings in the TA-55 complex include an Administration Building; a Support Office Building; a Generator Building (PF-8), which contains three air compressors, an auxiliary generator, switchgear, and batteries; a Utility Building (PF-6); and a Calcium Grinding Building (PF-7). The Generator Building is designed to Class 1 structural criteria; all facilities other than PF-4 and the FOC are Class 2.

There are four ventilation zones in building PF-4. Zone 1, the lowest pressure zone in the building, operates at -0.8 in. of water. It is a once-through system supplied by forced air blowers in the basement and services the glovebox lines. Supply air is drawn through a high efficiency particulate air (HEPA) filter, and each glovebox exhaust point is filtered by an 8-in. glovebox HEPA filter unit. The exhaust from the lines pass through three stages of HEPA filtration (four for ^{238}Pu lines).

Zone 2A consists of the corridors and mezzanines in the operating portions of the facility. It is supplied with HEPA-filtered air by a dedicated supply system and is maintained at a slightly higher pressure than Zone 2 so that Zone 1A air is drawn into Zone 2, the facility laboratory rooms and the basement vault. Air is bled out of Zone 2 to maintain a set pressure. This bleedoff air is exhausted from the building through two stages of HEPA filtration. Zone 2 air also is recirculated continuously through two-stage HEPA filter banks in the facility basement.

Zone 3 is the basement. It has a HEPA-filtered air supply system and an internal recirculation unit. Zone 3 exhaust air passes through two stages of HEPA filtration.

RISK ASSESSMENT METHODOLOGY

In addition to providing a traditional measure of facility risk, this study was designed to meet several other objectives.

1. Demonstrate the necessary level of detail with associated time and costs required to be useful for applications to numerous facilities or projects competing for approval and funding in a risk-based prioritization decision process. Not every facility or process is a candidate for a full-scope PSA.
2. Apply different measures of risk and consequences in addition to the traditional measures, which are based solely on risks to the public. This leads to a multiattribute description of the consequences.
3. Combine the various attributes to arrive at an overall utility measure for risk-based prioritization of upgrades within the facility.

To meet the first objective, the study has started with a qualitative preliminary hazard analysis (PHA) to identify hazards and potential consequences. Using the facility understanding developed through research into the systems and processes and the PHA results, a more quantitative assessment will be performed using techniques drawn from hazards and operability study (HAZOPs) and the failure modes and effects (FMEA) methods. Limited fault-tree modeling has been performed for critical safety systems. These more quantitative methods helped identify accident initiators and accident sequences, which then were quantified.

To meet the second objective, attributes considered potentially important to decision makers were identified. These included onsite and co-located worker health effects resulting from normal operations, accidental releases, and remediation activities. In addition, various types of environmental impacts were analyzed, including the extent of surface contamination with associated costs for remediation efforts (soil excavation, treatment, and disposal), the effects on resources such as effects on endangered wildlife species, and restrictions on land use (national parks, recreation areas, and private lands). Also included were measures to address programmatic, political, and community effects. Using the dominant accident sequences developed in meeting the first objective, a defined set of these attributes will be analyzed and quantified.

The relationships between the various steps required in meeting the first two objectives are shown in Fig. 1. For the multiattribute case in this analysis, the source term and consequence analysis quantities C1, C2, ... are vectors.

The third objective follows from the first two objectives. Using an assessed utility function for laboratory-wide risk-based prioritization and the safety assessment results as input, an overall utility value will be calculated. This value will be used by decision makers in allocating resources for safety-related work. The difference in the baseline utility value and that resulting from proposed system modifications will be used as the basis for decision making.

RESULTS TO DATE

To date, effort has been concentrated on performing a PHA in support of the first objective. In tandem, the defined set of attributes to be included in meeting the second objective is being developed. As work progresses, proposed system modifications are expected and will be used as one input required for meeting the third objective.

In performing the PHA, the following steps are being taken.

1. Preparing for the review
2. Performing the review
3. Documenting the results

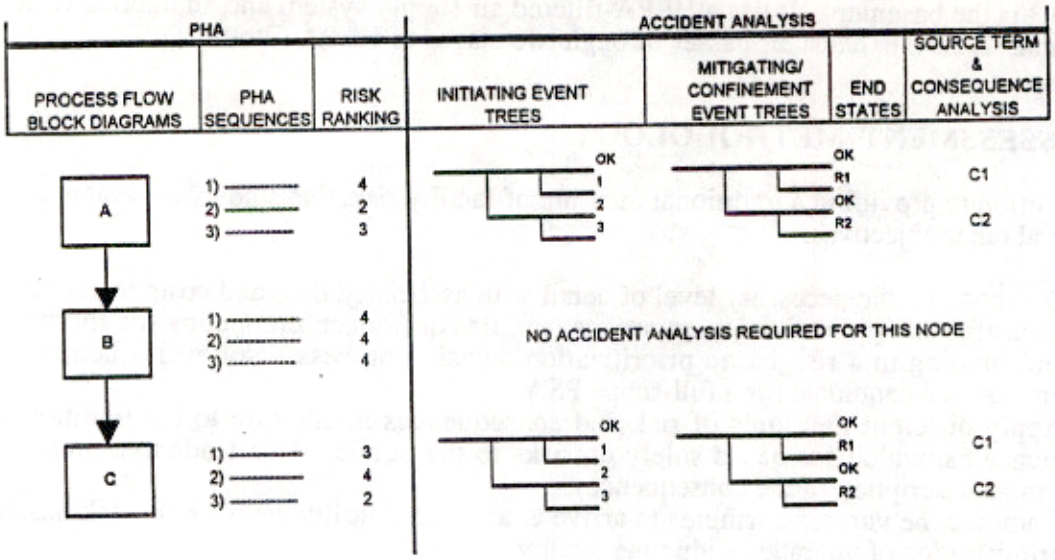


Figure 1. The relationship of preliminary hazard and accident analyses.

Each of these steps is composed of several tasks.

1. Selecting a team of risk assessment specialists and engineers and operators familiar with the process.
2. Gathering information on the subject process and similar processes. This encompasses information about chemicals, process parameters, major equipment, component interfaces, operating environments, available procedures, the facility layout, and safety-related equipment.
3. Establishing a recording medium for evaluation that specifies the format and methods of recording information.
4. Obtaining the required documentation to prepare the review. This includes P&IDs, process flow diagrams, a compilation of hazardous properties of materials used or generated in the process, plant equipment lists, facility layout diagrams, and electrical and mechanical component interface information.

In review we perform the following tasks.

1. An area and/or process is selected for evaluation.
2. The associated hazards are identified .
3. Hazard causes are identified.
4. Major effects of accidents are identified.
5. Safeguards are identified for hazard mitigation.
6. Assign hazard severity category.
7. Assign hazard likelihood.
8. Assign hazard risk.
9. List recommendations for mitigating hazard.
10. Assign severity, likelihood, and risk with recommendation.

Tables 1, 2, and 3 are used to carry out steps 6, 7, 8, and 9.

The final step, documenting results, requires that a format be specified for sorting and prioritizing the results for follow-up.

Table 1. Consequence severity categories ("S" Column).

Category	Maximum Possible Consequences			
	Public	Co-Located	Worker	Environment
A	Immediate health effects.	Immediate health effects.	Loss of life.	Onsite and offsite contamination.
B	Long-term health effects.	Long-term health effects.	Severe injury or disability.	Onsite only contamination.
C	Irritation or discomfort but no permanent health effects.	Irritation or discomfort but no permanent health effects.	Lost-time injury but no disability.	Significant facility contamination.
D	No significant offsite effect.	No significant onsite effect.	Minor or no injury and no disability.	Minor or no facility contamination.

Table 2. Consequences likelihood categories ("L" Column).

I (1 to 0.1)	Normal operations; frequency as often as once in 10 operating years or at least once in 10 similar facilities operated for 1 year.
II (0.1 to .01)	Anticipated events; frequency between 1 in 100 years and 1 in 10 operating years or at least once in 100 similar facilities operated for 1 year.
III (10^{-2} to 10^{-4})	Unlikely; frequency between 1 in 100 years and 1 in 10,000 operating years or at least once in 10,000 similar facilities operated for 1 year.
IV (10^{-4} to 10^{-6})	Very unlikely; frequency between 1 in 10,000 years and once in 1 million years or at least once in a million similar facilities operated for 1 year.
V	Improbable; frequency of less than once in a million years.

Table 3. Assignment of risk rank risk matrix ("R" Column).

Severity of Consequence	Likelihood of Consequence				
	I	II	III	IV	V
A	1	1	2	3	3
B	1	2	2	3	4
C	2	3	3	4	4
D	3	4	4	4	4

Risk Decision Criteria	
Risk Rank	**Recommendation**
1	Unacceptable - Should be mitigated to risk rank 3 or lower as soon as possible.
2	Undesirable - Should be mitigated to risk rank 3 or lower within a reasonable time period.
3	Acceptable with Controls - Verify that procedures, controls, and safeguards are in place.
4	Acceptable As Is - No action necessary.

QUANTITATIVE RISK ANALYSIS OF A BUTANE STORAGE FACILITY

L. F. S. Oliveira[1], J. D. Amaral Netto[2], R. A. Pinto[2], J. C. A. Lima[3]

[1]PRINCIPIA Ltda. and Federal University of Bahia, Brazil.
Fax: (55-71) 231-5332
[2]PRINCIPIA Ltda. - Brazil Fax: (55-21) 220-6663
[3]Refinaria Duque de Caxias - PETROBRÁS - Brazil
Fax: (55-21) 580-0376

INTRODUCTION

An existing butane pressurized storage facility formed by two 750 m^3 and two 1,600 m^3 spheres had been deactivated for some years. Recently a decision was taken to partially activate the facility by using the two smaller spheres. A safety review was undertaken which revealed that several aspects of the facility were not in accordance with the standards presently used by PETROBRAS, particularly, those related to the physical layout of pressurized hydrocarbon storage facilities and minimum separation distances to other storage tanks. As a result the preparation of a quantitative risk analysis (QRA) was requested by the Industrial Safety Division of REDUC and endorsed by the Refinery upper management. The proposed QRA had the following objectives:

1. assess the risks imposed to the external public and to the Refinery workers by the operation of the facility as it's;
2. compare the results to existing international acceptability criteria;
3. propose and evaluate risk reduction measures;
4. evaluate whether after implementing risk reduction measures, the facility could be operated where presently located or should it be transferred to a recently refurbished LPG storage facility.

In this work we describe the approach, the methodology and the software used to perform the analysis and discuss its main results.

METHODOLOGY AND SOFTWARE USED

A full quantitative risk analysis was performed following the typical approach of responding to the following questions: "what can go wrong?", "how likely is this to happen?", and "what are the expected consequences?"[(1)]. Risks were then firstly

expressed as a set of triplets: {scenario, frequency, consequences}, and then transformed to and presented as individual risk contours, cumulative complementary distribution functions (F-N curves), and average societal risk figures.

To answer the first question, a historical accident analysis and a preliminary hazard analysis (PHA) were performed. The first used two different data bases, namely, MHIDAS (over 5,000 accidents) from the Safety and Reliability Directorate[2] and ACCIDATA (over 1,500 mostly in Brazil) from PRINCIPIA[3]. The PHA was performed by a team of engineers and technicians from REDUC and PRINCIPIA. About 170 basic initiating events (involving ruptures of pipes, flanges, valves, spheres, pumps and human actions) were grouped into 12 initiating event groups (IEG), based on the equivalent diameter, pressure, flow type and rupture location.

The frequency of each IEG was quantitatively evaluated using international failure rates for the basic initiating events. A single fault tree was constructed to calculate the expected frequency of sphere rupture, which was evaluated using the fault tree program FTW[4] developed by PRINCIPIA.

Accident scenarios were assembled using event trees involving failure or success of existing protection systems, daytime and nighttime conditions, wind speed and direction, and ignition sources. A total of 1,474 different accident scenarios were evaluated, involving BLEVE's, flash and pool fires and unconfined vapor cloud explosions[5,6]. The expected effects and consequences of each scenario were calculated for two different types of population, namely, the public and Refinery workers.

A special risk assessment program named VULNER+[7] was developed by PRINCIPIA to perform extensive integrated scenario frequency and consequence calculations. The accident scenarios are automatically generated by the program from basic information fed by the user. Also in this program, the population is distributed on a square cell grid, which also serves to locate the specified ignition points, lines and areas. Each cell is further subdivided in a refined square grid to improve the resolution of the calculations. The effects of each scenario are calculated in the center of the refined cells and used to produce the corresponding consequences by means of pertinent probit relations[8].

Fatality conditional probability at each cell center is coupled to the associated scenario frequency to produce the value of the individual risk at that cell. The program goes through an interpolation process to yield the contours of individual risk around the facility. Societal risks (F-N curves and average societal risks) are obtained by coupling the above results to the population distribution in the cell grid, producing automatically the points for the curve plotting.

A ranked listing of the scenarios of larger frequencies, of larger consequences and of those which contribute the most to the average societal risk is also produced, being of invaluable help to the process of proposing risk-reduction measures by the analysts. The development and use of VULNER+ made it possible to perform the calculations referred above within a reasonable time period and with much less human resources than what we used in previous works of this kind.

MAIN RESULTS

Contours of individual risks of 10^{-4}/year, 10^{-5}/year, and 10^{-6} /year were obtained, respectively, for approximated radii of 200, 500 and 700 meters around the facility (Figure 1). The F-N curve for the public revealed that the frequency of accidents with 10 or more deaths is about 2×10^{-4}/year, and that of the accidents with 100 or more deaths is about 7×10^{-5}/year, with a maximum number of about 275 fatal victims.

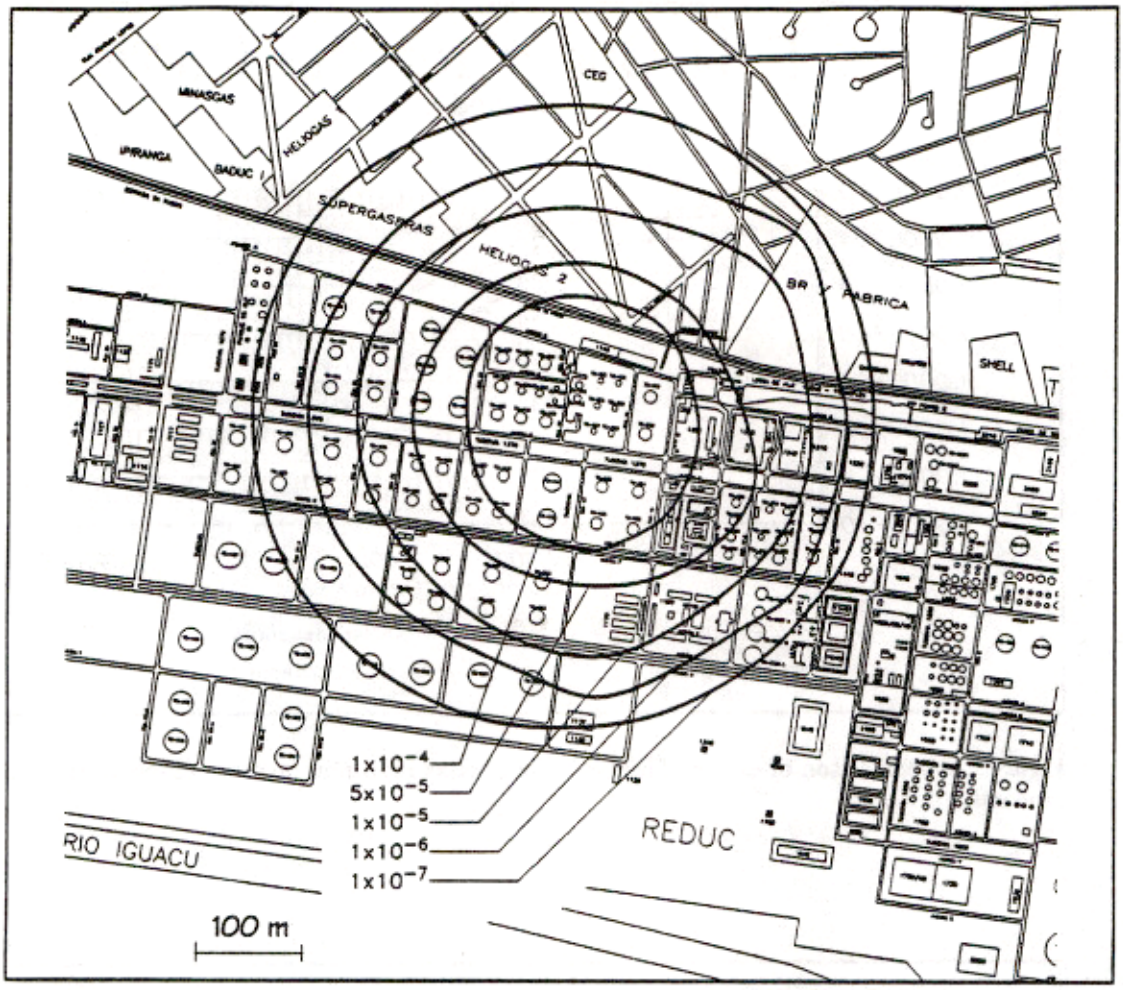


Figure 1 - Contours of individual risks for the existing facility

Since risk acceptability criteria for the public have not yet been established in Brazil, we compared our results to international existing criteria such as those of Holland and Denmark. This comparison showed that the risks of operation of the existing butane storage facility would be considered as "unacceptable" in both of those countries (Figures 2 and 3).

Individual risks for the workers of various affected units inside the refinery were converted to "fatal accident rates", with values ranging up to 10 for the butane storage facility operators. These values were then compared to the average FAR value for the Brazilian chemical industry, which is about 8.0. Therefore, the obtained FAR values for the butane facility were considered too high for the most affected workers.

Eight risk-reduction measures were proposed by the working group, ranging from removal of presently unused components, establishment of test procedures for valves, up to sloping the ground under the spheres to eliminate the accumulation of liquefied gas under the spheres and removal of neighboring liquid fuel tanks. The risks were reevaluated assuming that all measures would be implemented by the Refinery, and compared again to the acceptability criteria. Although a significant reduction was obtained, the results are still partly in the high side of both criteria, as shown by Figures 2 and 3.

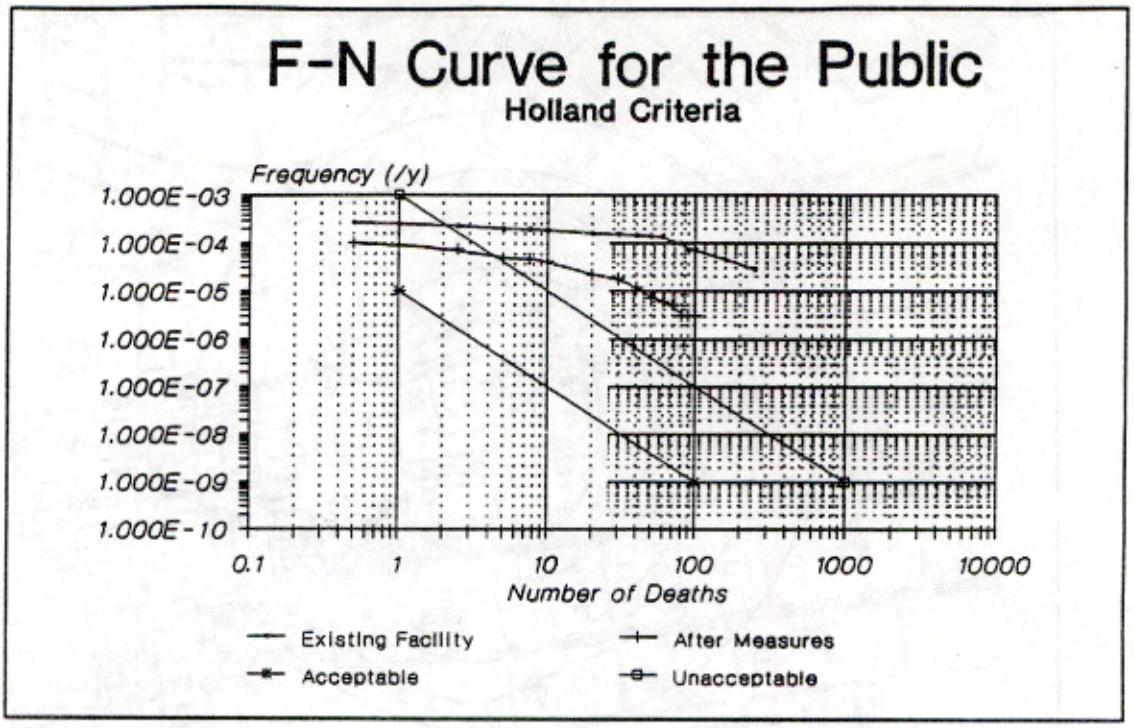


Figure 2 - Comparison of existing facility and after risks reduction measures F-N curves to the Holland criteria

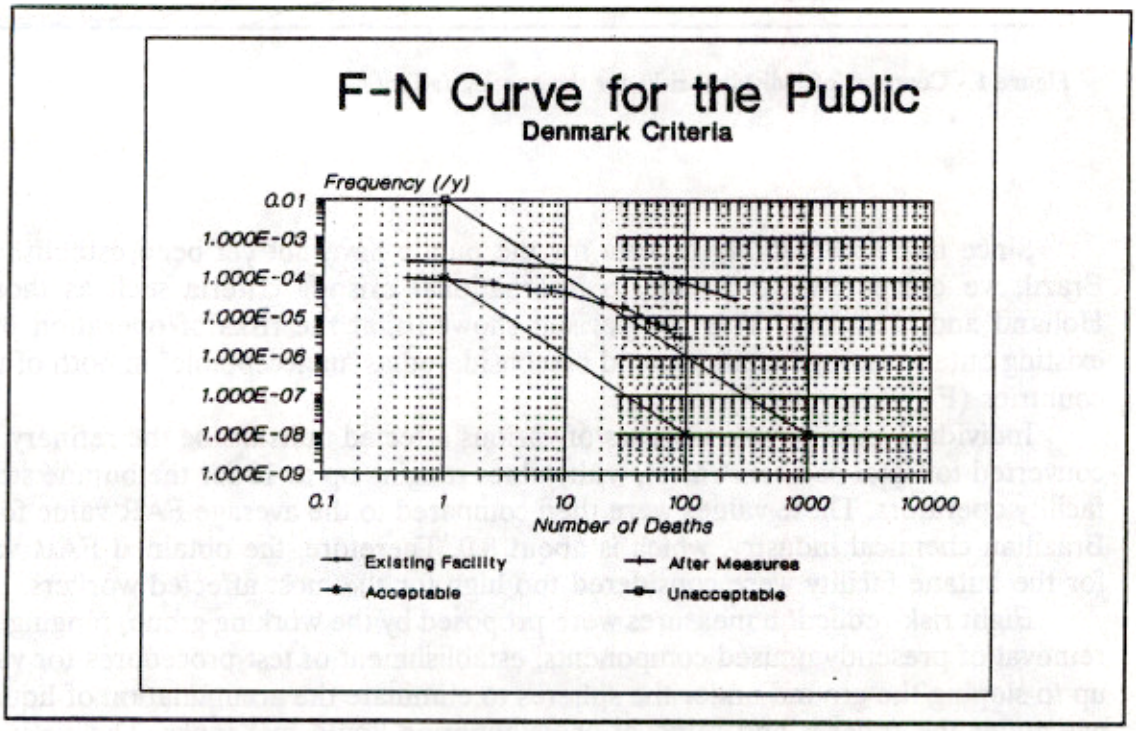


Figure 3 - Comparison of existing facility and after all risk-reduction measures F-N curves to the Denmark criteria.

Table 1 shows the impact of each risk-reduction measure over the public social risk, the total cost, the annual cost for ten years extension life of the facility and the cost per death averted. From this table, with exception of measure 8 (high cost), all the other measures could be considered for implementation, depending of financial resources availability.

Table 1 - Relation between risk reduction and associated costs for each measure

Existing facility average societal risk for the public = 2.14e-02 deaths/year				
Measure	Risk reduction (death/year)	Total Cost (US$)	Annual Cost (US$)	Cost/Death Averted (US$/death)
1. Test of liquid blockage three action valves each three months.	5.10e-05	0.00e+00	-	-
2. Water injection directly in the manifold, eliminating a valve and reducing the size of the valve for drainage execution.	3.34e-03	2.80e+04	3.8e+03	1.14e+06
3. To elevate and slope the ground under the spheres.	1.25e-02	4.55e+05	6.18e+04	4.95e+06
4. Valves removal at the pump discharge.	1.29e-04	1.00e+04	1.36e+03	1.05e+07
5. Explosion proof control room and operator always present in the control room.	1.07e-03	1.00e+05	1.36e+04	1.27e+07
6. Use of only one product receiving line, removing the other.	1.11e-04	1.12e+04	1.52e+03	1.37e+07
7. Nafta pipeway relocation.	6.33e-03	9.45e+05	1.28e+05	2.03e+07
8. Removal of neighboring liquid fuel tanks.	4.10e-05	3.09e+06	4.20e+05	1.02e+10
All risk-reduction measures.	2.44e-02	4.64e+06	6.30e+05	2.58e+07

From the results obtained, it was concluded:

1. The operation of existing facility imposes an unacceptable social risk to the public according to Holland and Denmark criteria.

2. After the implementation of all risk-reduction measures, the social risk would not be totally acceptable (Denmark criteria), mainly due to low frequencies/high consequences (highly populated area). After this measures, the area of the public submitted to levels higher than 1.0e-05 (maximum value for acceptability in England) is relatively small, reaching mainly employees of adjacent companies, as illustrated by Figure 4.

3. As the risks weren't reduced, after implementation of all risk-reduction measures, to an acceptable level, the butane storage in refurbished LPG facility would be an attractive alternative to be considered by REDUC upper management.

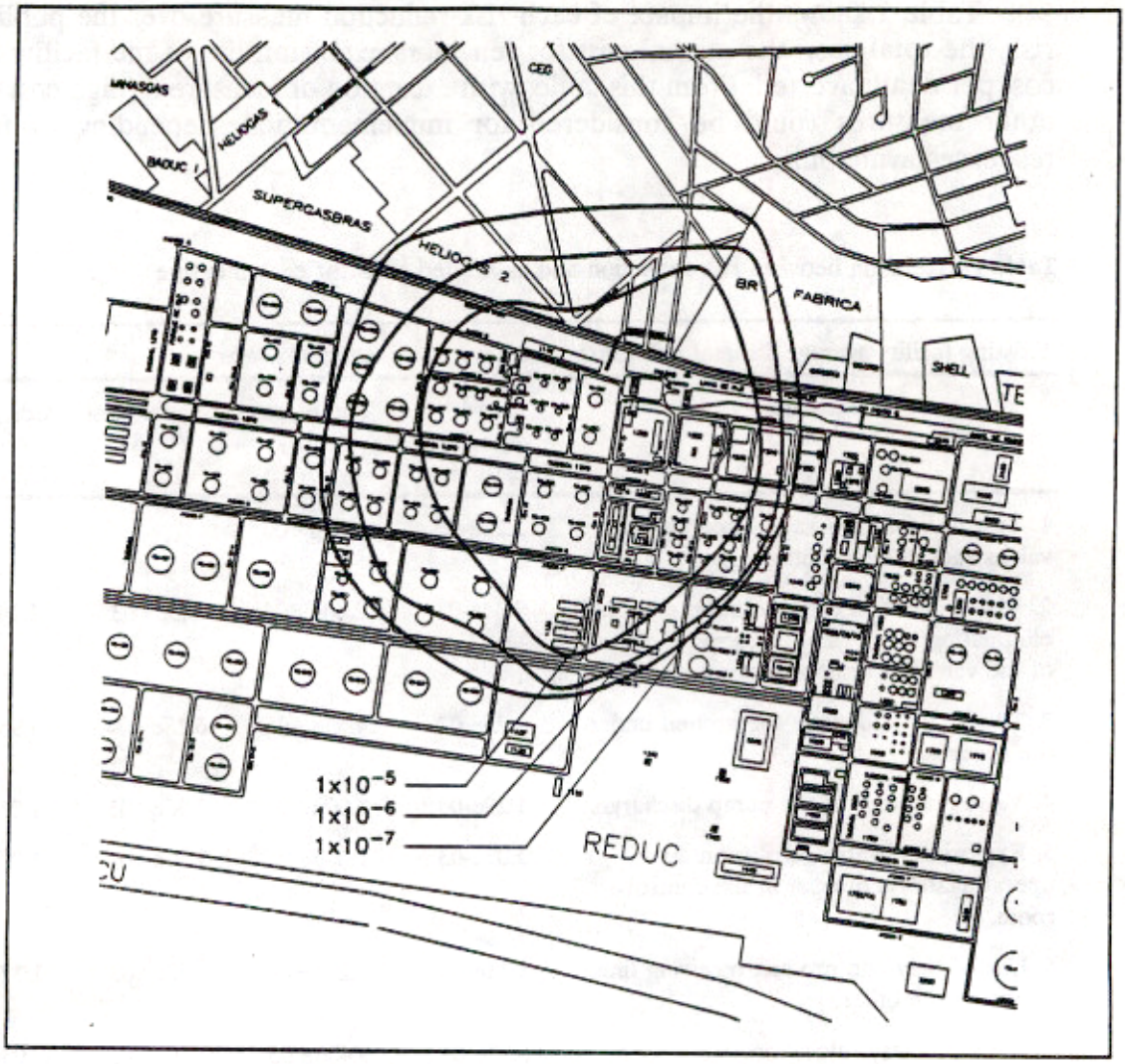


Figure 4 - Contours of individual risks after all risk-reduction measures implementation.

REFERENCES

1. L. F. Oliveira, C. Leal, J.E Lima, J. Amaral Netto, M. Contarini, P.F. Melo and P.V. Fleming, "Risk assessment of a Marine Terminal for Hazardous Chemicals, *International Probabilistic Safety Assessment and Management Meeting*, Beverly Hill, (February 1991).
2. *MHIDAS*: Major Hazard Incident Data Service, Safety and Reliability Business, United Kingdom Atomic Energy Authority, Distributed by Silverplate Information Inc., UKAEA, (1992).
3. *ACCIDATA*: Accident Data, PRINCIPIA Engenharia de Confiabilidade e Informática Ltda, (1992).
4. *FTW*: Fault Tree Workstation, PRINCIPIA Engenharia de Confiabilidade e Informática Ltda, (1991).
5. *TNO* "Methods for the Calculation of the Physical Effects of the Escape of Dangerous Materials: Liquids and Gases", Directorate General of Labour, Holland, (1980).
6. G. W. Colambrander and J.S. Puttock, Dense gas dispersion behaviour: experimental observations and model developments, *International Symposium on Loss Prevention and Safety Promotion in the Process Industries*, Harrogate, England, (September 1983).
7. *VULNER+*, PRINCIPIA Engenharia de Confiabilidade e Informática Ltda, (1992).
8. N.A. Eisenberg, C. J. Lynch and Breeding, Vulnerability model: a simulation system for assessing damage resulting from marine spills, U.S. Coast Guard, Department of Transportation, CG-D-136-75, (June 1975).

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)

SITE-WIDE SEISMIC RISK MODEL FOR SAVANNAH RIVER SITE NUCLEAR FACILITIES

S. A. Eide[1], R. S. Shay[1], and W. S. Durant[2]

[1]Los Alamos Technical Associates, Inc.
P. O. Box 51688
Idaho Falls, ID 83405-1688

[2]Westinghouse Savannah River Company
1991 S. Centennial Ave.
Building 1
Aiken, SC 29803

INTRODUCTION

The 200,000 acre Savannah River Site (SRS) has nearly 30 nuclear facilities spread throughout the site. The safety of each facility has been established in facility-specific safety analysis reports (SARs). Each SAR contains an analysis of risk from seismic events to both onsite workers and the offsite population. Both radiological and chemical releases are considered, and air and water pathways are modeled. Risks to the general public are generally characterized by evaluating exposure to the maximally exposed individual located at the SRS boundary and to the offsite population located within 50 miles.

Although the SARs are appropriate methods for studying individual facility risks, there is a class of accident initiators that can simultaneously affect several or all of the facilities. Examples include seismic events, strong winds or tornadoes, floods, and loss of offsite electrical power. Overall risk to the offsite population from such initiators is not covered by the individual SARs. In such cases multiple facility radionuclide or chemical releases could occur, and offsite exposure would be greater than that indicated in a single facility SAR.

As a step towards an overall site-wide risk model that adequately addresses multiple facility releases, a site-wide seismic model for determining off-site risk has been developed for nuclear facilities at the SRS.[1] Risk from seismic events up to the design basis earthquake (DBE) of 0.2 g (frequency of 2.0E-4/yr) is covered by the model. Present plans include expanding the scope of the model to include other types of initiators that can simultaneously affect multiple facilities.

METHODOLOGY

Development of the SRS seismic risk model involved four steps:

1. Identification of all nuclear facilities at the SRS

2. Review of seismic accident analyses (radionuclide and chemical releases and air and water pathways) in facility SARs

3. Updating of air dispersion and dose calculations for seismic accidents to obtain up-to-date and consistent results (1992 offsite population and ICRP-30 dose model)

4. Integration of individual facility results to obtain a site-wide risk model.

Nuclear facilities at the SRS were identified by a review of existing SARs and a review by cognizant safety personnel. The SRS has 29 different facilities historically classified as nuclear. This list does not include storage and waste facilities with very small amounts of radionuclides and whose classification is presently undecided. Such facilities would not significantly contribute to the offsite risk.

Once the nuclear facilities and SARs were identified, the seismic accident analyses were reviewed. Several cases were encountered in the SARs:

- Single seismic accident analysis for the DBE (for facilities that do not release significant quantities of radionuclides or chemicals for earthquakes significantly weaker than the DBE)

- Multiple seismic accident analyses for the DBE to cover different sources of radionuclides or chemicals or different accident phenomena

- Multiple seismic accident analyses covering a spectrum of earthquakes up to the DBE (for facilities that can release significant quantities of radionuclides or chemicals for earthquakes weaker than the DBE)

- Multiple seismic accident analyses covering a spectrum of earthquakes up to and beyond the DBE (for some of the newer SARs).

Of the 29 nuclear facilities, 12 were chosen for inclusion in the seismic risk model based on their seismic-initiated offsite risk (as indicated in their SARs). These 12 facilities contribute over 99% of the site-wide seismic risk to the offsite population. All seismic accidents (up to the DBE) for these facilities were then included in the model. The 12 facilities contributed a total of 15 seismic accidents to the model.

Because the atmospheric dispersion calculations for the 12 facilities had been performed over a period of 10 years (1983 to 1993), inconsistencies existed with regard to the offsite population assumed and to the dose model used. All of these dispersion calculations were rerun using the most up-to-date SRS atmospheric dispersion code, AXAIR89Q.[2] Therefore, all analyses were standardized using the 1992 offsite population, the ICRP-30 dose model, and SRS meteorological conditions based on the period 1982 through 1986.

The final step in developing a site-wide seismic risk model involved integrating the individual facility seismic risks. The two main measures of off-site population radiological risk used at the SRS are the following:

- Risk to the maximally exposed individual located at the SRS boundary (dose in rem, multiplied by the accident frequency)

- Risk to the offsite population located within 50 miles of the site (dose in person-rem, multiplied by the accident frequency).

The location of the maximally exposed individual at the site boundary varies with facility location with the SRS, as shown in Figure 1. Because of this and because a single site boundary location is needed for the site-wide model, the individual facility doses and risks to the site boundary individual are not additive. At a given instance in time, the wind direction across the site is relatively uniform. This implies that release plumes from certain facilities may not overlap at the site boundary. Therefore, the location of the maximally exposed individual at the site boundary for the dominant risk facility was chosen as the location for the site-wide model. Then releases only from facilities whose release plumes overlap this location were included for the site-wide calculation of risk to the individual located at the site boundary.

In contrast, all facility results can be added to determine the site-wide risk to the offsite population located within 50 miles.

Also desired were the exposures for the maximally exposed individual at the SRS boundary and the offsite population. To obtain these doses, only the DBE accidents from each facility were used. (To include other seismic accidents from weaker earthquakes would result in overestimation of the integrated dose. This problem of overestimation does not occur when risk measures are calculated, because the frequencies of the accidents are factored into the calculation.) Otherwise, the dose results were combined in a manner similar to what was done for risk results.

RESULTS

The resulting seismic risk model for the SRS appropriately integrates individual facility radiological risks to obtain the site-wide risk to the maximally exposed individual at the site boundary and to the offsite population. Both radiological and chemical releases and air and water pathways were initially considered in the development of the model. However, only air dispersion of radionuclides turned out to be significant with respect to risk to the offsite population.

Final site-wide risk and dose results were approximately twice the results from the most dominant SRS facility. However, the site-wide results could have been much higher if facility locations at the SRS had been different or if none of the facilities had been dominant with respect to risk.

ACKNOWLEDGEMENT

This work was supported by the U.S. Department of Energy under Contract Number DE-AC09-89SR18035.

REFERENCES

1. J. C. Huang and C. R. Lux, AXAIR-89: An Improved Version of the AXAIR Code, Westinghouse Savannah River Company, WSRC-RP-89-1197, 1989.

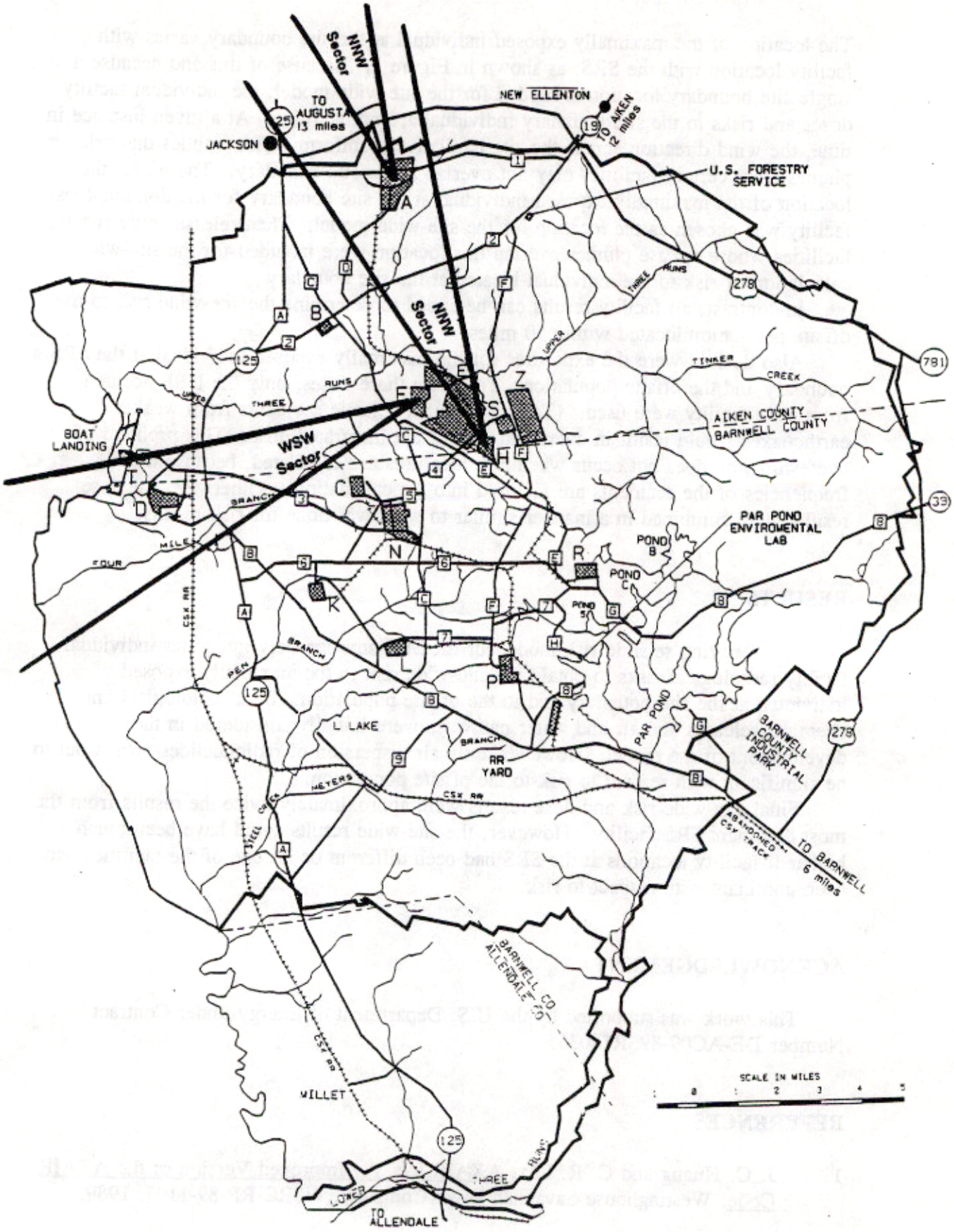


Figure 1. This figure shows the Savannah River Site facility locations and site boundary. Also indicated are the locations of the maximum exposed individual at the site boundary for various facilities.

TORNADO IMPACT ANALYSIS FOR USE IN QUANTITATIVE RISK ASSESSMENT

Jatin N. Shah[1]

Senior Engineer
Four Elements Ltd.
450 W Wilson Bridge Rd
Columbus, OH 43085
(614) 431-6330

INTRODUCTION

Public awareness of the potential danger from accidental releases of hazardous chemicals has increased over the years. Major industrial accidents have led to promulgation of governmental safety regulations throughout the world. In the United States, government agencies at all levels have passed regulations that are geared to protect the public and the environment from accidental releases of hazardous materials.. The evaluation of risks from chemical releases that are induced by events such as tornados, earthquakes, and other natural phenomena are required by California's Risk Management and Prevention Program (RMPP) and may also be required by the pending federal Risk Management Program (RMP) regulation. Although most industrial facilities are designed to withstand high wind speeds, there is always potential for violent storms, such as tornadoes, that can damage buildings and process equipment. The possibility of a tornado strike in most regions of the United States is remote; however, in the some regions (Panhandles of Texas and Oklahoma, and Kansas) the probability of a tornado strike is significant. This paper describes a methodology to estimate the likelihood of a tornado impacting a facility and causing damage. Although there are other published methodologies for the quantification of a tornado strike[1-3], the analysis presented in this paper provides a more detailed, site specific calculation that can be used to determine potential chemical release probabilities. The results of this analysis can be easily incorporated into an overall risk analysis and used to partly fulfill regulatory requirements.

---

[1] This analysis was primarily developed while the author was an employee at DNV Technica. I would also like to thank the contributions of Kevin J. Mitchell who provided invaluable assistance during the analysis. Additionally, I would like to thank Dr. Krishna Mudan and Philip M. Myers of Four Elements for their outstanding review of this paper.

BACKGROUND

The quantification of risk using an appropriate methodology can provide a reliable and realistic estimate of risks from an industrial facility. The Center for Chemical Process Safety (CCPS) of the American Institute of Chemical Engineers (AIChE) have published guidelines for Quantitative Risk Assessment (QRA). The underlying basis of a QRA is to offer means to estimate the answers to the following questions:

- What causes the potential events ?
- How likely are these events ?
- What are the potential consequences of these events?

The first question can generally be answered through the use of hazard identification techniques such as HAZOP, "What If", "What-If"/Checklist, and Checklists to name just a few. These techniques provide only qualitative information regarding the likelihood and consequences of an event. Due to the very strong winds associated with tornadoes it is obvious that a tornado strike may cause equipment damage which result in a release of hazardous material. A detailed methodology to determine the likelihood of a damaging tornado strike can be used in conjunction with equipment failure rates to obtain the overall likelihood of releasing hazardous material from process equipment at a given site.

TORNADO IMPACT ANALYSIS

The primary objective of a tornado analysis is to estimate the likelihood of a process unit being struck by a damaging tornado and the resulting effects. The likelihood depends on the frequency of tornado occurrences in the region, the area in which wind velocities exceed the critical damaging velocity, and the size of the process unit. Instead of determining the likelihood of exceeding design wind speeds for each critical process equipment, it is more expedient to determine a wind speed profile. This profile can be used for each piece of equipment to determine appropriate damage levels. The following terms are used in this analysis:

Ft	=	expected number of tornados per year in a given area
A	=	given area
L	=	the mean length of "swept area"
W	=	the mean width of "swept area"
P_{ti}	=	conditional probability a that tornado will be of given intensity.
E_z	=	tornado exposure zone
F_o	=	Occurrence frequency of a tornado of given intensity
P_w	=	conditional exposure probability to various "F-Class" wind speeds for a tornado of given intensity

A critical assumption of this analysis is that the touch-down point of a tornado is uniformly distributed over the given area, "A". This allows for application of tornado occurrence data collected for a larger region (like counties) to a smaller area (like a process unit).

For most regions in the United States, historical data on tornado strike frequencies can be obtained, from the National Weather Service's Severe Storms Center. These frequencies are normalized on both an annual and an area basis. Since the winds associated with tornadoes vary, the severity of damage along the potential strike area also varies. The extent and area of tornado damage increases with increasing wind speed. Dr. T. Theodore Fujita, Professor of Meteorology at the University of Chicago devised the "F scale" to classify tornados by their severity [4].

The intensity of the tornadoes is not measured directly, but rather, indirectly by the type of resultant damage caused. Dr. Fujita devised a qualitative scale, coarse by design, such that the damage observer should not have to choose from between more than two intensity classes. For example, an F1 tornado may be expected to cause moderate damage (topple mobil homes, snap trees, and damage roofs), while an F2 tornado is expected to cause considerable damage (such as lifting roofs from homes), and an F5 tornado causes incredible damage (completely destroying strong, well-built structures). In general, the frequency of tornado occurrence decreases with increasing intensity (i.e. F1 tornadoes are more prevalent than F5 tornadoes). Table 1 presents the F-scale along with the associated wind speed ranges, damage intensities, mean length, mean width of tornadoes and a national average of conditional occurrence probability for different intensity tornadoes. It should be noted that the conditional probability of having a tornado of given intensity (P_{fi}) varies by region; therefore, a site specific analysis should be conducted to derive results similar to the ones shown in Table 1.

Table 1. Tornado classification by F-scale, wind speeds, and intensities.

F-SCALE	Wind Speed (MPH)	Prob. Occ. (%)	Mean Length (miles)	Mean Width (miles	Intensity
F0	40-72	26	1.2	0.028	Light Damage (broken branches, mobil home damage)
F1	73-112	37	2.6	0.062	Moderate Damage (snap trees, roof damage)
F2	113-157	27	5.4	0.185	Considerable Damage (blow away roofs, uproot trees)
F3	158-206	8.0	10.0	0.366	Severe Damage (blow away roofs, damage and destroy walls)
F4	207-260	1.7	27.2	0.457	Devastating Damage (leave most buildings as rubble)
F5	261-318	0.3	35.5	0.487	Incredible Damage (destroy buildings to their foundation)

The greatest extent of damage caused by any given tornado is used to characterize its intensity. Therefore, a tornado may be classified with a certain F-scale, but only a fraction of the damaged area will have experienced wind speeds of that F-class. Twisdale [5] gave the conditional probability of observing various class wind speeds for a tornado of given intensity. These probabilities are presented in Table 2.

Table 2. Damage class distribution in tornadoes

Tornado Class	Wind Speed Class Probability						
	F0	F1	F2	F3	F4	F5	Total
F0	1						1
F1	0.55	0.45					1
F2	0.22	0.35	0.43				1
F3	0.09	0.24	0.32	0.35			1
F4	0.12	0.16	0.26	0.22	0.24		1
F5	0.12	0.11	0.17	0.25	0.17	0.18	1

Tornado Exposure Zone

When calculating the tornado exposure zone the process unit area can be considered in conjunction with the mean width (W) and length (L) of the tornado which is dependent upon its intensity. The tornado strike area varies for each class of tornado and is determined by multiplying the mean length and mean width of the tornado (given in Table 1). Since only a portion of the process unit needs to be struck by a tornado to cause damage the tornado mean length and width are generally modified by the dimensions of the process unit. In most cases, the tornado dimensions are much larger than the process unit dimensions, so this modification is not significant. The exposure zone (E_z) is calculated for each tornado intensity category .

Frequency of Exceeding Specific Wind Speeds

The occurrence probability of a given F-class tornado is calculated for a process unit by using equation (1).

$$F_o = [F_t (E_z) P_{ti}] / A \quad (1)$$

The frequency of observing a given class of winds is obtained by multiplying the occurrence probability (F_o) by the conditional probability of observing that class of wind speed (P_w) as given in Table 2. The frequency versus wind speed profile is obtained by calculating this for each tornado intensity class and summing the frequencies for each class tornado. An example of a frequency versus wind speed profile is provided in Figure 1.

RISK ANALYSIS

The estimation of risk involves estimating the likelihood of possible events, determining the consequences, and integrating the consequences with the likelihood. A methodology for determining the frequency of exceeding given wind speeds is provided above. A methodology for the determination of failure sizes and the assessment of consequences is provided below.

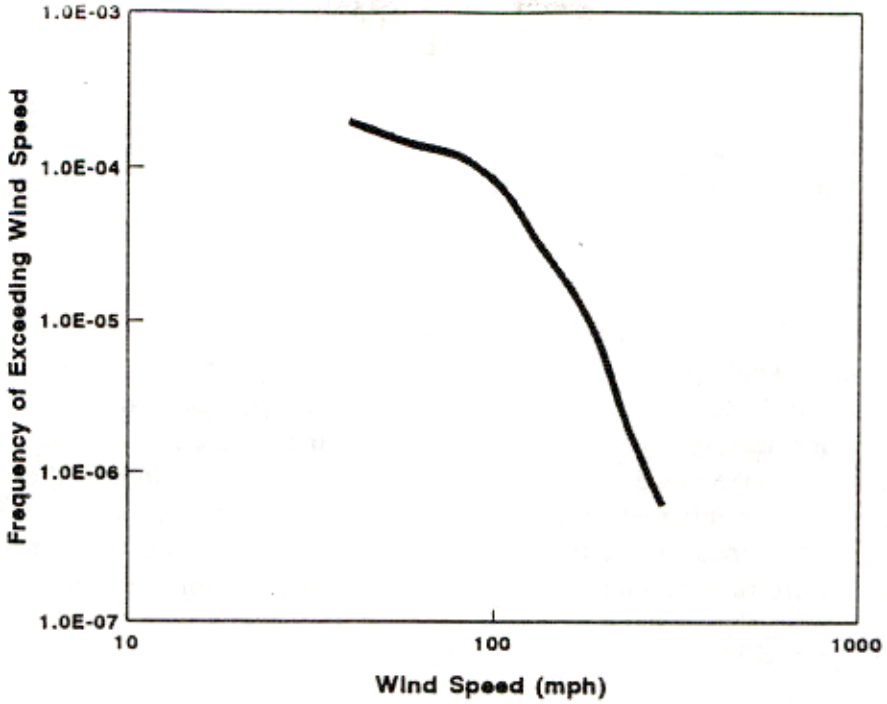


Figure 1. Frequency of exceeding various wind speeds.

Release Size Determination

The size of potential releases caused by a damaging tornado depends upon the extent the design wind speed is exceeded by the tornado winds. Although a structural component or a building is designed to withstand a certain wind speed, construction, age, and prevailing condition will affect the extent of damage. Since the actual building or structures can be more or less resistant than the design specification, it is preferable to use a distribution of design wind speeds rather than a single design wind speed. Thus, the probability of a building withstanding a specific wind speed can be determined by using a log-normal distribution. In typical analyses, the design wind speed distribution is represented by using several discrete critical wind speeds. To illustrate, take the simplest of examples, a structure designed to withstand winds of 100 mph with a standard deviation of 20 mph could use 80, 100, and 120 mph as the critical wind speeds to represent the design wind speed distribution. The damage, can then be correlated with exceedence of the discrete critical wind speeds. For tornado wind speeds within one standard deviation above the critical wind speed, the expected damage is moderate and would probably result in small leaks. For wind speeds between one and two standard deviations, considerable structural damage is likely to occur, potentially resulting in large leaks. Above two standard deviations, damage is expected to be catastrophic. For each damage category, the frequency of observing the winds required to cause the damage is obtained form a graph like Figure 1. The frequency for various releases is determined by first multiplying the probability that the structure can withstand a specified critical wind speed by the frequency of observing the various wind speeds required to cause each damage category (moderate, considerable, and catastrophic) and then summing them.

Once hazardous material is released, its consequences are dependent on several important factors such as: the type of release, type of material, material inventory, prevailing meteorological conditions, ignition sources, etc. Except for the meteorological conditions all of these factors would be addressed in the same manner as in a typical quantitative risk analysis and are not discussed further here.

Initially, releases that are induced by tornadoes quickly diluted affected by the associated high wind speeds. However, tornados usually pass the area in a brief period of time (usually less than five minutes) and the meteorological conditions after passage could vary considerably. Additionally, the tornado may cause severe structural damage, but a release may take place later. One should also exercise care in how the consequence of multiple releases initiated by a common cause, like a tornado strike, are evaluated. Therefore, caution must be exercised in modeling releases arising from tornadoes. The equipment failure rates should thus be increased to account for the tornado strike.

CONCLUSIONS

This paper has outlined the procedures for a detailed tornado analysis that can be incorporated in a QRA study. A separate curve can be developed for each facility, giving the frequency for various wind speeds. This can then be applied to various critical process equipment and buildings. This approach provides an efficient method to evaluate releases from process equipment with different design characteristics. A detailed tornado analysis can also be used as input for a comprehensive structural analysis, to evaluate potential options for reducing the likelihood of damage. The procedures outlined in this paper result in a high quality site specific study that is fundamentally sound and defensible.

REFERENCES

1. Thom, H. C. S., "Tornado Probabilities," Monthly Weather Review , Vol. 91, 1963, pp. 730-736.

2. Wen, Y. K., and Chu, S. L., "Tornado Risks and Design Wind Speed," Journal of the Structural Division, ASCE, Vol. 99, No. ST12, Proc. Paper 10249, December, 1973, pp. 2409-2421.

3. Rutch, C., Anselmo, K., Linney, R.E., and Sheesley, J.H., "Tornado Risk Analysis," Plant Operations Progress, Vol 11., No.3, July, 1992.

4. Fujita, T. T., "Proposed Characterization of Tornadoes and Hurricanes by Area and Intensity," SMRP Research Paper No. 91, Department of Geophysical Sciences, University of Chicago, Feb., 1971

5. Twisdale, L. A., "Tornado Data Characterization and Wind Speed Risk", Journal of the Structural Division, ASCE, Vol. 104 No. ST10, October, 1978.

AIRCRAFT CRASH ANALYSIS OF THE PROPOSED SIZEWELL B CONTAINMENT VESSEL

Y.F. Al-Obaid

Faculty of Technological Studies, PAAET,
P.O.Box 42325 Shuwaikh,
70654 KUWAIT

ABSTRACT

This paper attempts to examine the behaviour of the proposed sizewell B containment vessel under aircraft crash. A three-dimensional time dependent crash analysis is carried out which incorporates, direct integration concept. The final results obtained include displacement, velocities, accelerations, concrete scabbing, perforation and general cracking. The final damage is shown in a specially prepared postmortem diagram. The paper has an appendies summarizing the constitutive equations and flow of cracks for the proposed numerical model.

INTRODUCTION

In the process of design of containment vessels for nuclear power plants special emphasis is placed on matters which guarantee their integrity against hazards within and without these vessels. They cause extreme stresses, plasticity, rupture and cracks in the vessels. The integrity analysis demands to evaluate a complex interaction of many parameters caused by aircraft crash which include types of aircraft and their loading functions, the non-linear behaviour of materials and the local crashed zone, energy absorbing characteristics of component system and dynamic modes of failure and damage. In addition to that the integrity analysis is directly dependent on special modeling and analytical techniques.

This paper attempts to examine the behaviour of the proposed sizewell B containment vessel under the crash of a multi-role combat aircraft such as Tornodo and Phantom RF-4E. A 60 section of the containment vessel is analyzed using three dimensional 20 nodded isoparametric finite elements adopted in program OBAID. The crash area under consideration is 28 m^2 which is evaluated

from the data obtained from these two aircraft. The vessel is assumed to have unbonded tendons both in the dome and in the barrel wall. The influence of the liner is included in evaluating resistance to the crash.

A STEP-BY-STEP DYNAMIC ANALYSIS

The non-linear dynamic finite element analysis is reported in [1-4] for aircraft crash. The current analysis reported in this paper takes into consideration on the strength of the liner intact initially with concrete by means of Lugs and other anchoring devices. The dynamic coupled equations are interpreted step-by-step and the response history of the vessel is divided into time increments Δt. If [M] is the mass, [C] and [K] are the damping and stiffness matrices, the equation of motion with specified material properties at time are established.

The equation of motion may be written in increment form with modified [C] and [K]

(1) $[M]\{\ddot{\delta}(t)\} + [C_o]\{\dot{\delta}(t)\} + [K_o]\{\delta(t)\} = \{R(t)\} + \{F(t)\}$
where $\{F(t)\}$ is the initial load = $\{[\Delta C]*\{\dot{\delta}(t)\}+[\Delta K]*\delta(t)\}\}$
(* indicates time $0 \rightarrow t$).

Solution at $t + \Delta t$

(2) $[M]\{\ddot{\delta}(t+\Delta t)\}+[C_o]\{\dot{\delta}(t+\Delta t)\}+[K_o]\{\Delta R(t+\Delta t)\}+\{\Delta F(t+\Delta t)\}$
$\Delta F(t+\Delta t)$ represents the non-linearity during time increment Δt and is determined by interaction using the stress approach.

(3) $\{\sigma\} = [D_T](\{\varepsilon\}-\{\varepsilon_o\})+\{\sigma_o\}$

The constitutive law is used with the initial stress and constant stiffness approaches throughout the non-linear and the dynamic iteration. For the iteration

(4) $\{\delta(t+\Delta t)\}_i = [K_o]^{-1}.\ \{R_{TOT}(t+\Delta t)\}_i$

The strains are determined using

(5) $\{\varepsilon(t+\Delta t)\}_i=[B]\{\delta(t+\Delta t)\}_i$

where [B] is the strain displacement. The stresses are computed as

(6) $\{\sigma(t+\Delta t)\}_i = [D_T]\{\varepsilon(t+\Delta t)\}_i +\{\sigma_o(t+\Delta t)\}_{i-1}$

where $\{\sigma_o(t+\Delta t)\}_i$ is the total initial stress at the end of each iteration. All calculations for stresses and strains are performed at the Gauss points of all elements. The initial stress vector is

(7) $\{\sigma_o(t+\Delta t)\}_i = f\{\varepsilon(t+\Delta t)\}_i =[D_T]\{\varepsilon(t+\Delta t)\}_i$

Using the principle of virtual work, the change of equilibrium and nodal loads $\{\Delta F(t+\Delta t)\}_i$ are calculated as

(8) $$\{\Delta F(t+\Delta t)\}_{TOT} = \int_{-1}^{+1}\int_{-1}^{+1}\int_{-1}^{+1} [B]^T\{(\Delta\sigma_o(\Delta t+t))\}_i\, d_\xi\, d_\eta\, d_\zeta$$
$$\sigma_o(t) = \{\sigma_o(t+\Delta t)\}_i = 0$$

where d_ξ, d_η, d_ζ are the local co-ordinates.

The integration is performed numerically at the Gauss points. Effective load vector F(t) is given by

(9) $\{\Delta F(t+\Delta t)\}_{TOT} = -[\Delta\sigma(t)_o](\{\delta(t+\Delta t)\}_i * \{\delta(t)\})$
$= -[\Delta C(t+\Delta t)_i\{\delta(t+\Delta t)\}_i[\Delta K(t)_o(\{\delta(t+\Delta t)\}_i\{\delta(t)\}_i)$
$= -[\Delta K(t+\Delta t)_i\{\delta(t+\Delta t)\}_i$

Von Mises criterion is used and together with transitional factor f^*_{TR} form the basis of the plastic states such that

$$(10)\quad f^*_{TR} = \frac{\sigma_y(t) - \sigma_{y-1}(t)}{\sigma(t+\Delta t)_i - \sigma(t+\Delta t)_{i-1}}$$

The elasto-plastic stress increment will be

(11) $\{\Delta\sigma_i\} = [D]_{ep}\{\sigma(t+\Delta t)_{i-1}(1-f^*_{TR})\{\Delta\varepsilon\}$

If $\sigma(t+\Delta t)_i < \sigma_y(t)$, it is an elastic limit and the process is repeated. The equivalent stress is calculated from the current stress state, where stresses are drifted they are corrected from the equivalent stress-strain curve.

The residual load vector is calculated as

(12) $\{R\} = \{F_q\} - \int_v [B]^T\sigma(t+\Delta t)_i \, d\,vol$

Stresses are checked against cracking criteria to find new cracks. A new secant [D] is built which takes into account the new cracks for changes in modulus of elasticity due to higher compression and also due to additional crushing of concrete. Stresses existing normal to cracks or crushing are released from the new stresses $\sigma^*(t+\Delta t)_i$

(13) $\sigma^R(t+\Delta t)_i = \sigma(t+\Delta t)_i - \sigma_{CR}$

LOADINGS AND VESSEL PARAMETERS

The load time functions is reported in [see ref.5] for Phantom and Tornado multirole combat aircraft are summarized in Fig.1. Table 1 gives the material properties. Table 2 shows the vessel parameters given initially for the Sizewell B inquiry [6]

APPLICATION TO SIZEWELL B

Figure 2 shows linear and non linear displacements of the vessel with the final post-mortem given in Figures 3 and 4 for both aircraft.

SUMMARY AND CONCLUSIONS

Dynamic analysis under aircraft crash has been carried out using the proposed analysis. The evaluation of the criticality of the containment vessel with the reactor embedded equipment involved a complex interaction of numerous parameters. Upon crash the aircraft can produce two types of effect on the vessel, namely, the local effects and the overall effects. The local effects are characterized by penetration, perforation and backface spalling or scabbing of the vessel material. The overall effects of the aircraft crash on vessel stability are commonly evaluated in terms of the flexural and shear behaviour of the vessel. The aircraft impact or crashes produces a stress wave which is a transient stress disturbance which travels a finite

velocity from the level of application of load. The wave can be longitudinal or dilational parallel to the direction of the crash and transverse or distortional perpendicular to the direction of the crash. Using the Sizewell B parameters and the load-time functions for two aircraft the proposed analysis has been carried out and the results are plotted. During crash the liner in the local area has ruptured. The studs in the local area under impact load have been ruptured. In other areas they have buckled.

REFERENCES

1. Y.F. Al-Obaid, Three-dimensional cracking analysis of concrete containment vessels under external impacts, Journal of the university of Kuwait (Science), 19: 17-34, (1992).

2. Y.F. Al-Obaid, The finite element analysis of crack growth in zircalogy tubing under extreme temperature, Int. J. of Engng. Fracture, 23 (5): 875-82, (1986).

3. Y.F. Al-Obaid, Dynamic crack propagation in PWR tube, Pressure Vessel and Piping Conference (ASME), June 17-21, Houston, Texas, U.S.A., (1984).

4. K. Dritler, P. Gruner, Calculation of the total force acting upon a rigid wall by projectiles, Int. J. of Nuclear Engng. and Design 37: 231-44 (1976).

5. H. Kamil, N. Krutzik, G. Kost & R.L. Sharper, An overview of major aspects of aircraft impact problem, Int. J. of Nuclear Engng. and Design 46 (1): 109-21 (1977).

6. A case for the Size-well B Nuclear Power Station. HMSO 1985.

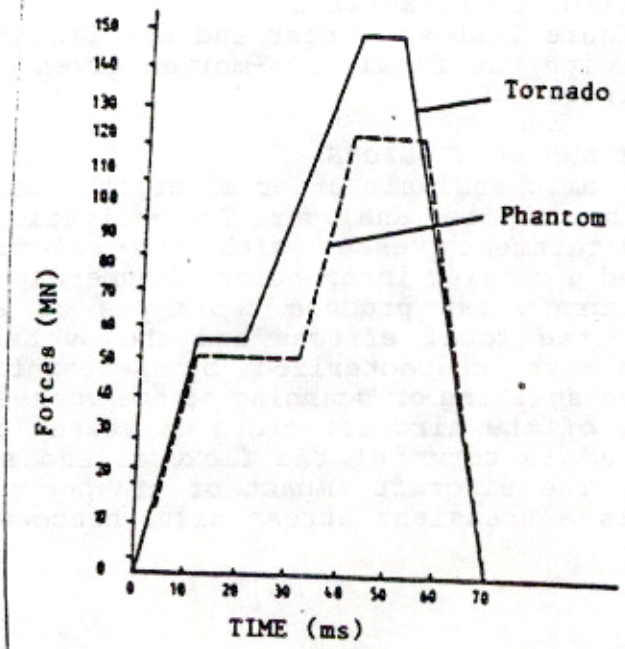


Fig. 1 Load time impact function

Table 1 - Design Stress Data

Conventional Steel	4516 MN/mm^2
σ_y - yield strength	
Ep = 0.1 E	
Liner 6 mm to 12 mm thickness	10 μM/m°C
Coefficient of linear expansion	41.6 W/m°C
thermal conductivity	0.0035
-ultimate strain	200 x_3 10^3 MN/m^2
E(steel)	38x10^3 MN/m^2
E(concrete) - short term	20.7x10^3 MN/m^2
long term	0.74 E
E(soft zones)	0.47 E
Ep - plastic moulus	0.15 (concrete)
Poissons Ratio	1.3 (Steel)
Coefficient of Thermal-	
Expansion of Concrete	
Short term specific creep	10x10^{-6}/°C; 12x10^{-6}/°C(*)
Long term specific creep	1830x10^{-9} MN/m^2 °C
Minimum crushing strength at	2407x10^{-9} MN/m^2 °C
28 days.	

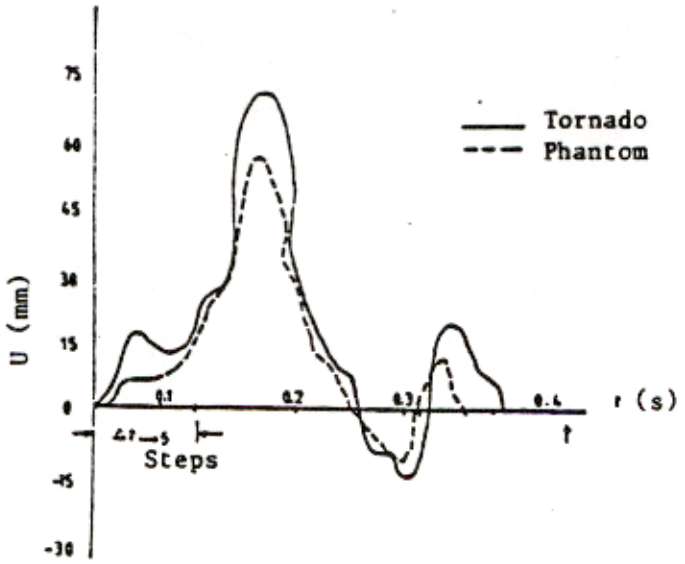
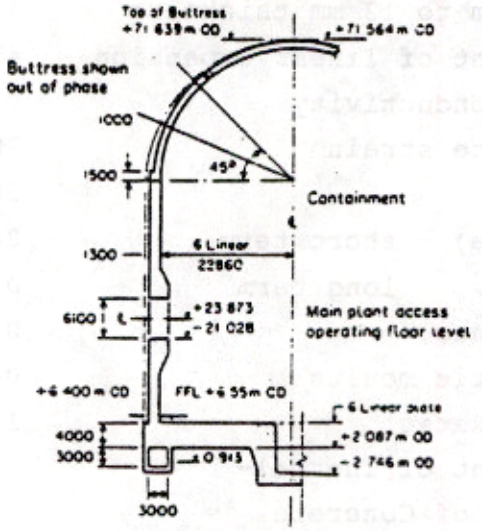
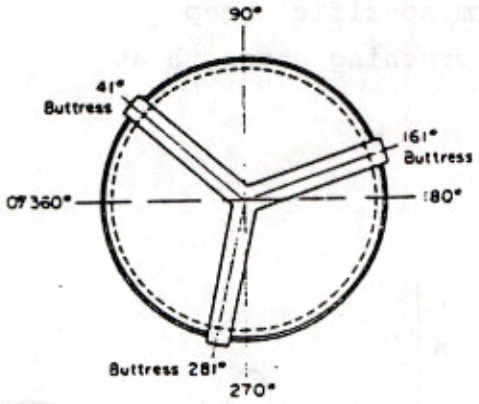


Fig. 2 Load Displacement as a Function of Time

Table 2 - Containment Vessel Parameters



Vertical section through main plant access



Plan of dome

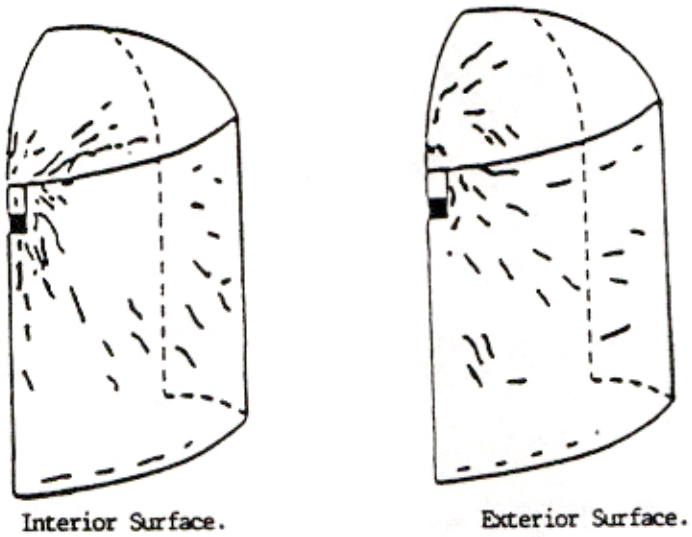


Fig. 3 Aircraft Phantom Post-Mortem.

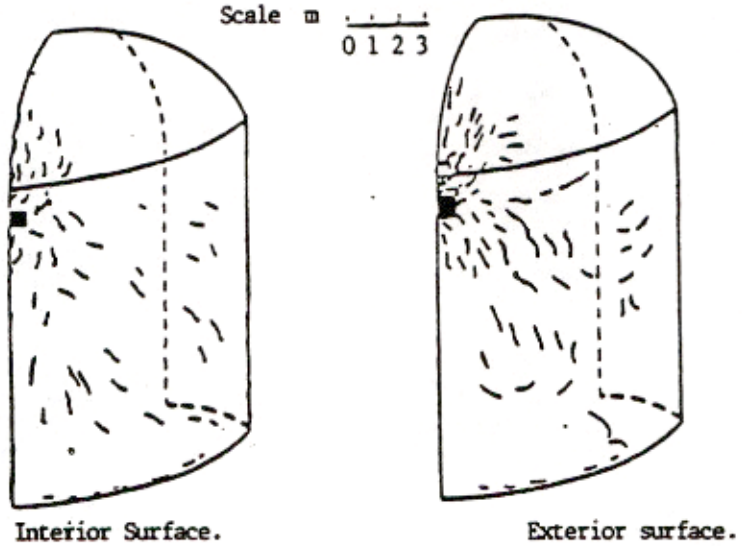


Fig. 4 Aircraft Tornado Post-Mortem.

050 Risk Management in DOE (III)

Chair: R.R. Fullwood, BNL

Fully Integrated Risk Management

R.J. Doyle, K. Beierschmitt, (Battelle Pantex)

FULLY INTEGRATED RISK MANAGEMENT

R. J. Doyle, Ph.D., K. J. Beierschmitt, Ph.D., P.E.

Risk Management Department
Battelle Pantex
P. O. Box 30020
Amarillo, TX 79177

INTRODUCTION

Risk management is a process that cuts across disciplines, and uses information from a variety of sources. Each element in a risk management program must be viewed jointly with all other elements because all are required for effective risk management. Too often, however, risk management programs consist of a series of disjoint elements. For example, quality assurance is a vital element of risk management; it mitigates risk by ensuring that standards and criteria are maintained. But quality assurance is usually independent of the risk management program. The same is true of maintenance management, however, maintenance management ensures that reliability assumptions that affect risk are maintained. Understanding of interactions such as these by management and line personnel is essential to managing risk.

An effective risk management program empowers those responsible for affecting risk by ensuring effective interaction of all program elements, by providing training on the elements of the program and their interactions, and by providing management endorsement and support for the program.

Full integration of all the elements of a risk management program produces a whole far greater than the sum of the parts. Information contained in one element of the program, but required by other elements is more readily available and more easily transmitted among functions. In some cases, this integration means that contradictory regulatory and procedural guidance is discovered, resolved and eliminated.

The Integrated Risk Management Program (IRMP) was established to describe and provide oversight for the diverse activities and programs that are being undertaken to satisfy new Environment, Safety and Health (ES&H) requirements. The IRMP mission is to identify areas for improvement in existing programs, prioritize needs, assure consistency among program interfaces, and develop transition strategies to accommodate new regulatory guidance from DOE.

The IRMP supports ES&H upgrade activities that satisfy changes in regulations and DOE orders. The IRMP supports these functions by: integrating ongoing programs, interpreting regulatory requirements, evaluating consistency between programs and

requirements, assuring consistency among program interfaces, tracking program progress, developing transition strategies, and prioritizing needs of programs.

A fully integrated risk management program assures the proper definition, control, maintenance, and assessment of the safety envelope.

DEFINE THE SAFETY ENVELOPE

The Safety Analysis Report (SAR) is a vital element of controlling the risk of facility operations--it provides the technical justification that the facility can be operated safely. The SAR describes the criteria against which the facility was designed, establishes design bases for safety-related systems, describes the actual configuration of the facility, describes how operations are to be performed in the facility, and demonstrates through analysis the level of safety that has been or is expected to be achieved.

The facility "safety basis" is the information presented in the SAR, including aspects of design, engineering analyses, and administrative controls, that are vital to the control of hazards of the facility. The safety basis is the basis on which both the contractor and the DOE determine that it is safe to operate the facility. Approval to operate the facility is granted by the DOE with the understanding that the contractor will operate the facility within the "safety envelope", the boundary of acceptable conditions that are consistent with the safety basis.

For a new facility, the development of the safety basis can be divided into two phases: preliminary design, and final design and construction.

(i) Preliminary Design Phase

The Preliminary Safety Analysis Report (PSAR) provides documentation of the safety basis that is developed during conceptual and preliminary design. If the hazard level of the facility is very low, a safety assessment may first be performed and submitted to the DOE to determine whether a Safety Analysis Report is warranted. Approval of the PSAR is required prior to construction of a facility.

DOE Order 5480.23, Nuclear Safety Analysis Reports, describes requirements for safety analysis reports prepared for nuclear facilities. Design criteria are provided for DOE facilities in DOE Order 6430.1A, General Design Criteria. The criteria depend upon the type of facility being designed. Within the SAR, all of the applicable federal, state, and local criteria are identified and the degree of compliance with the criteria is presented. A key step in establishing the safety basis of the facility is the selection and analysis of design basis accidents. The capability of the design to withstand natural phenomena, as required by DOE 6430.1A, is currently evaluated according to UCRL-15910. A new Order, DOE 5480.NPH, is in preparation to provide guidance in this area.

Another key step is the performance of failure modes and effects analyses to identify which system failures could lead to critical or catastrophic consequences, to categorize safety-related systems, and to establish the level of Quality Assurance required. To evaluate the level of safety provided by the design, a risk analysis is performed and documented in the PSAR.

Safety is included in the facility design by compliance to a number of DOE Orders, including: Human Factors Engineering (DOE 6403.1A & DOE 5480.23); Fire Protection (DOE 5480.7A), Criticality Safety (DOE 5480.24), and Quality Assurance (DOE 5700.6C).

(ii) Final Design and Construction Phase

During final design and construction, the PSAR for the facility is updated to become the Final Safety Analysis Report (FSAR). At this stage, configuration management becomes an important aspect of risk management. As the basis for approvals, the information in the SAR must be controlled. The analyses performed and documented in the SAR must reflect the design and what is ultimately constructed.

Intimately associated with configuration management is quality assurance. Quality assurance provides confidence that the level of safety of the constructed facility is consistent with the level of safety analyzed in the FSAR. The Quality Assurance Program provides an umbrella under which the architect-engineer performs design, the constructor performs construction, and the Final Safety Analysis Report (FSAR) is prepared.

The approval of the DOE for the operation of a facility is based not only on the safety characteristics of the design, but also on how the facility will be operated. In particular, assurance must be given in the FSAR that the operation of the facility will not extend outside the safety envelope. The SAR analyses support the derivation of operational requirements including safety limits, limiting safety system settings, limiting conditions for operation, surveillance requirements, and administrative controls.

For a nuclear facility, a stand-alone Technical Safety Requirements (TSR) document is prepared (in accordance with DOE 5480.22), which contains the operational requirements that, if violated, could result in off-site consequences. The entire SAR represents a contract with the DOE regarding how the facility will be operated.

Before a facility can be operated, operating procedures must be developed, according to requirements in DOE 5480.19, and personnel must be trained, as specified in DOE 5480.18A and DOE 5480.20 for nuclear facilities. An Emergency Management Program must also be established, as required by the DOE 5500 series of Orders. The Emergency Management Program must identify organization and responsibilities, develop procedures for emergency response, provide appropriate facilities and equipment, and prepare emergency response plans.

In its review and approval process for the FSAR, the DOE prepares a Safety Evaluation Report (SER) which examines the safety basis provided in the FSAR. After approval of the FSAR, the contractor must perform an Operational Readiness Review to assure that all of the commitments made in the FSAR have been satisfied and that the facility is ready to operate. In turn, the DOE performs an Operational Readiness Evaluation (ORE). Operation of the facility can then begin.

MAINTAIN THE SAFETY ENVELOPE

The manner in which facilities are operated is at least as important to the risk as the safety characteristics of the design. The changes that are being imposed on this aspect of the management of DOE facilities are perhaps the most challenging because they require not only major financial resources, but a change in the safety culture and attitudes of operating personnel.

DOE Order 5480.19 provides requirements for the conduct of operations at DOE facilities. These requirements are largely based on those developed by the Institute for Nuclear Power Operations (INPO) for commercial nuclear facilities and can be implemented on a graded approach according to the hazard level of the facility. Conduct of operations covers a variety of areas including

- Operations organization and administration
- Shift routines and operating practices
- Control area activities
- Communications

- On-shift training
- Investigation of abnormal events
- Notifications
- Control of equipment and system status
- Lockouts and tagouts
- Independent verification
- Logkeeping
- Operations turnover
- Operations procedures
- Postings
- Labeling.

Conduct of operations is primarily human oriented. Increased formality in the conduct of operations in all of these areas is essential to reducing the human error contribution to risk. It is also important to control the status of the facility and equipment. The analysis of risk performed in the SAR relates to a new facility with equipment that operates within design specifications. In-service testing and surveillance are necessary to assure that materials have not degraded with age and that equipment has not been unacceptably modified or worn out.

Similarly, the maintenance management program, as required by DOE 4330.4A, assures that equipment does not degrade as the result of lack of maintenance. Safety-related instrumentation must be kept calibrated to be reliable. The evolving philosophy within the nuclear industry and the DOE is that an older facility should pose no difference in risk or reliability from a new facility. Preventive maintenance is an important element of this philosophy.

CONTROL CHANGES TO THE SAFETY ENVELOPE

The DOE approves operation of a facility according to the design and procedures described in the SAR. During the lifetime of the facility, changes will be required in facility design and operating procedures. In the past, SARs were not updated to reflect changes in DOE facilities and, typically, changes were made to facilities with little analysis of the impact on the approved safety basis.

Improved configuration management (a draft Order, DOE Order 5480.CM, is in preparation), like improved conduct of operations, requires a major cultural change in the operation of DOE facilities. It also requires a major investment to make the transition from facilities with unmanaged configuration to managed configuration. In some cases, the cost of transition cannot be justified based upon the remaining lifetime of the facility. In other cases, upgrading of configuration management can be limited to critical safety systems that have a direct impact on the safety basis.

Configuration management affects many different aspects of facility management including document control, maintaining drawings that reflect as-built and as-modified construction, controlling changes in procedures, obtaining appropriate approvals before making modifications, and updating documents to reflect changes.

DOE Order 5480.21 identifies requirements for addressing Unreviewed Safety Questions (USQ) in nuclear facilities. USQ's arise when changes are made in facilities, when a test or experiment is to be performed that was not explicitly considered in the SAR, when an error is discovered in the SAR, or when new data result in questioning the validity of an assumption in the SAR.

The purpose of the USQ process is to identify changes or conditions that may be outside the envelope of the authorization basis on which DOE approved operation of the

facility. The implementation of a USQ program is intimately related to the state of configuration management and the existing authorization basis of a facility. A USQ program must be phased into existence as the authorization basis and configuration management are established.

ASSESS THE SAFETY ENVELOPE

The final risk management function is to assess the safety envelope. Programs have been undertaken to control risk by developing a safety envelope, controlling a safety envelope, and modifying a safety envelope, as described in the preceding sections. It is not enough to implement programs, however--it is also important to measure their effectiveness. Assessment includes both the evaluation of the condition of the physical plant, and a self-assessment that focuses on the management system that is controlling plant safety.

The Quality Assurance Program, as required by DOE 5700.6C, addresses:

- **Management:** Contractors are required to develop a Quality Assurance Program that describes organizational structure and responsibilities, to assure proper training of staff, to establish processes for maintaining and upgrading quality, and to control records.

- **Performance:** Contractors are required to establish technical standards, administrative controls, and approved procedures; to incorporate applicable design requirements and criteria in facility design; to procure items and services according to established specifications; and to perform inspections and acceptance tests.

- **Assessment:** Contractors are required to assess their own performance periodically and to obtain periodic independent review.

The functions of surveillance and in-service testing were mentioned under "Controlling the Safety Envelope" as a means of assuring that conditions are not deteriorating. Other indicators can be used to determine whether risk is being properly controlled. It is critical that performance indicators be established and tracked. Examples of such performance indicators are lost workday incidence rate, equipment outages, and maintenance backlog to identify safety-related or risk-related problems in the plant or in the management system that is being used to control risk. It is also necessary to monitor abnormal occurrences, which may be an indication of a deterioration in risk management to identify and correct the root cause of those occurrences.

SUMMARY

Risk management programs today are generally considered to be discrete, stand-alone programs, as are quality assurance, configuration management, maintenance management, waste management, human factors, fire protection, industrial hygiene, and many others. However, the fact is that all these elements comprise a risk management program, and a risk management program cannot exist without taking all these elements into account in a fully integrated fashion. Once fully integrated, these elements provide us with a system that enables us to define, maintain, control and measure the safety envelope. This has effectively been achieved through the IRMP.

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)

ORGANIZATION OF PERFORMANCE ASSESSMENTS CONDUCTED FOR THE WASTE ISOLATION PILOT PLANT

J. C. Helton,[1] D. R. Anderson,[2] and M. G. Marietta[2]

[1] Arizona State University, Tempe, AZ 85287
[2] Sandia National Laboratories, Albuquerque, NM 87185

INTRODUCTION

The Waste Isolation Pilot Plant (WIPP) in southeastern New Mexico is being developed by the U.S. Department of Energy (DOE) as a disposal facility for transuranic waste.[1-3] In support of this project, Sandia National Laboratories is conducting an ongoing performance assessment (PA) for the WIPP.[4-9] The ordered triple representation for risk proposed by Kaplan and Garrick[10] is used to provide a clear conceptual structure for this PA. This presentation describes how the preceding representation provides a basis in the WIPP PA for (1) the definition of scenarios and the calculation of scenario probabilities and consequences, (2) the separation of subjective and stochastic uncertainties, (3) the construction of the complementary cumulative distribution functions (CCDFs) required in comparisons with the U.S. Environmental Protection Agency's (EPA's) standard for the geologic disposal of radioactive waste (i.e., 40 CFR Part 191, Subpart B),[11] and (4) the performance of uncertainty and sensitivity studies. The organization of this discussion follows the structure previously used in Refs. 12 and 13. Results obtained in preliminary PA for the WIPP completed in December of 1992 are used for illustration.[14,15]

CONCEPTUAL BASIS FOR WIPP PERFORMANCE ASSESSMENT

As proposed by Kaplan and Garrick,[10] the outcome of a PA can be represented by a set $\mathcal{R}$ of ordered triples of the form

$$\mathcal{R} = \{(S_i, pS_i, \mathbf{cS}_i), i=1, ..., nS\} , \quad (1)$$

where S_i is a set of similar occurrences, pS_i is the probability that an occurrence in the set S_i will take place, $\mathbf{cS}_i$ 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. This representation formally decomposes the outcome of a PA 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 S_i are typically referred to as "scenarios" in radioactive waste disposal. Similarly, the pS_i are scenario probabilities, and the vector $\mathbf{cS}_i$ contains environmental

releases for individual isotopes, the normalized release defined by the EPA,[11] and possibly other information associated with scenario S_i.

Although the representation in Eq. (1) provides a natural conceptual way to view risk, the set $\mathfrak{R}$ by itself can be difficult to examine. For this reason, the risk results in $\mathfrak{R}$ are often summarized with CCDFs, which provide a display of the information contained in the probabilities pS_i and the vectors $\mathbf{cS}_i$. With the assumption that a particular consequence result cS in the vector $\mathbf{cS}$ has been ordered so that $cS_i \leq cS_{i+1}$ for i=1, ..., nS-1, the associated CCDF is shown in Fig. 1. A consequence result of particular interest in PAs for radioactive waste disposal is the EPA normalized release to the accessible environment.[11,16] As indicated in Fig. 1, the EPA places a bound on the CCDF for normalized release to the accessible environment. Regulatory considerations associated with the WIPP PA are discussed by Anderson and Marietta (these *Proceedings*) and in more detail in Ref. 14.

In practice, the outcome of a PA depends on many imprecisely known variables. These imprecisely known variables can be represented by a vector

$$\mathbf{x} = [x_1, x_2, ..., x_{nV}], \tag{2}$$

where each x_j is an imprecisely known input required in the PA and nV is the total number of such inputs. As a result, the set $\mathfrak{R}$ is actually a function of $\mathbf{x}$:

$$\mathfrak{R}(\mathbf{x}) = \{[S_i(\mathbf{x}), pS_i(\mathbf{x}), \mathbf{cS}_i(\mathbf{x})], i=1, ..., nS(\mathbf{x})\} . \tag{3}$$

As $\mathbf{x}$ changes, so will $\mathfrak{R}(\mathbf{x})$ and all summary measures that can be derived from $\mathfrak{R}(\mathbf{x})$. Thus, rather than a single CCDF for each consequence value contained in $\mathbf{cS}$, there will be a distribution of CCDFs that results from the possible values that $\mathbf{x}$ can take on.

In the WIPP PA, the uncertainty characterized by the probabilities pS_i in Eq. (1) is referred to as stochastic uncertainty and results from the fact that the system under study can behave in many different ways. The uncertainty associated with $\mathbf{x}$ is referred to as

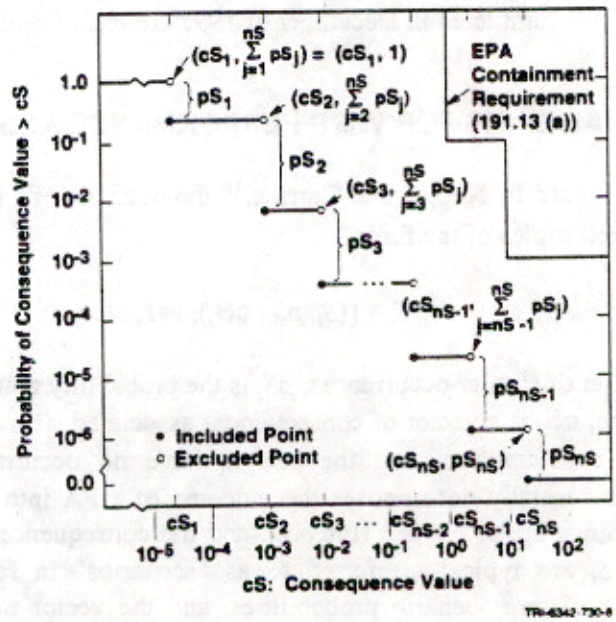


Figure 1. Estimated CCDF for Consequence Result cS.

subjective uncertainty and results from a lack of knowledge on the part of the analysts conducting the WIPP PA. The importance of maintaining a distinction between stochastic and subjective uncertainty has been emphasized by a number of authors.[10,17,18]

The uncertainty in $\mathbf{x}$ can be characterized by probability distributions

$$D_1, D_2, ..., D_{nV}, \tag{4}$$

where D_j is the distribution for the variable x_j contained in $\mathbf{x}$. The definition of these distributions may also be accompanied by the specification of correlations and various restrictions that further define the relations between the x_j. These distributions and other restrictions probabilistically characterize where the appropriate input to use in a PA might fall given that the analysis has been structured so that only one value can be used for each input variable. The development of such distributions for the WIPP PA is discussed by Tierney (these *Proceedings*) and in more detail in Vol. 3 of Ref. 14.

Once the distributions in Eq. (4) have been developed, Monte Carlo techniques can be used to determine the uncertainty in $\mathcal{R}(\mathbf{x})$ that results from the uncertainty in $\mathbf{x}$. First, a sample

$$\mathbf{x}_k = [x_{k1}, x_{k2}, ..., x_{k,nV}], k=1, ..., nK, \tag{5}$$

is generated according to the specified distributions and restrictions, where nK is the size of the sample. The PA is then carried out for each sample element $\mathbf{x}_k$, which yields the sequence of results

$$\mathcal{R}(\mathbf{x}_k) = \{[S_i(\mathbf{x}_k), pS_i(\mathbf{x}_k), \mathbf{cS}_i(\mathbf{x}_k)], i=1, ..., nS(\mathbf{x}_k) \tag{6}$$

for k=1, ..., nK. For the 1992 WIPP PA, nV = 49 (Table 3-1, Ref. 15) and nK = 70 (Table C-2, Ref. 15). Each set $\mathcal{R}(\mathbf{x}_k)$ is the result of one complete PA carried out with a set of inputs (i.e., $\mathbf{x}_k$) that the review process producing the distributions in Eq. (4) concluded was possible. For a particular consequence result, a CCDF will be produced for each set $\mathcal{R}(\mathbf{x}_k)$ shown in Eq. (6). This yields a distribution of CCDFs of the form shown in the left frame of Fig. 2, which can be summarized with mean and percentile curves as shown in the right frame. In addition, the expression in Eq. (6) generates a mapping from analysis input (i.e., $\mathbf{x}_k$) to analysis results (i.e., $\mathcal{R}(\mathbf{x}_k)$) that can be explored with regression-based sensitivity analysis techniques.[9,15,18]

STRUCTURE OF 1992 WIPP PERFORMANCE ASSESSMENT

Scenarios constitute the first element S_i of the ordered triples contained in the set $\mathcal{R}$ shown in Eq. (1) and are obtained by subdividing the set

$$S = \{x: x \text{ a single 10,000-yr history beginning at decommissioning of the WIPP}\}. \tag{7}$$

Each 10,000-yr history is complete in the sense that it includes a full specification, including time of occurrence, for everything of importance to PA that happens in this time period. In the terminology of Cranwell et al.,[19] each history would involve a characterization for a specific sequence of "naturally occurring and/or human-induced conditions that represent realistic future states of the repository, geologic systems, and

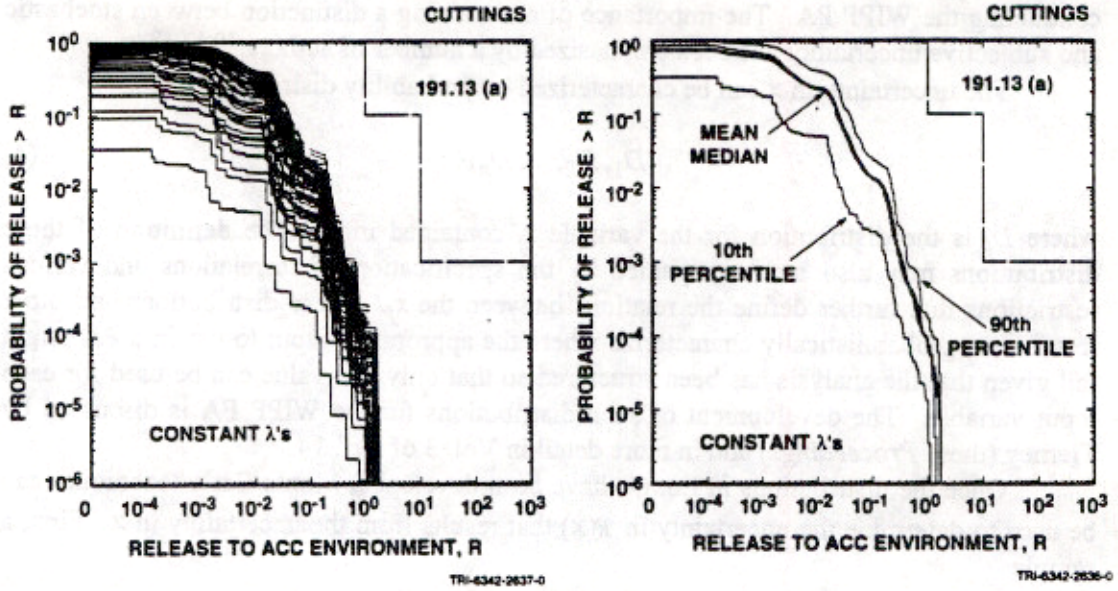


Figure 2. Distribution of CCDFs for normalized release to the accessible environment over 10,000 yr for cuttings removal (Fig. 8.2-3, Ref. 15).

ground-water flow systems that could affect the release and transport of radionuclides from the repository to humans."

The development of scenarios for the 1992 WIPP PA led to a set S of the form shown in Eq. (7) in which all credible disruptions were due to drilling intrusions (Ref. 14, Vol. 2, Ch. 4). As a result, scenarios were defined to provide a systematic coverage of drilling intrusions. Specifically, scenarios were defined on the basis of (1) number of drilling intrusions, (2) time of the drilling intrusions, (3) whether or not a single waste panel is penetrated by two or more boreholes, of which at least one penetrates a pressurized brine pocket and at least one does not, and (4) the activity level of the waste penetrated by the boreholes.

The construction of scenarios started with the division of the 10,000-yr time period appearing in the EPA regulations into a sequence

$$[t_{i-1}, t_i],\ i=1, 2, \ldots, nT, \tag{8}$$

of disjoint time intervals. These time intervals lead to scenarios

$$S(\mathbf{n}) = \{x:\ x \text{ an element of } S \text{ for which exactly } n(i) \text{ intrusions occur in time interval } [t_{i-1}, t_i] \text{ for } i=1, 2, \ldots, nT\} \tag{9}$$

and

$$S(\mathbf{l},\mathbf{n}) = \{x:\ x \text{ an element of } S(\mathbf{n}) \text{ for which the } j^{th} \text{ borehole encounters waste of activity level } l(j) \text{ for } j=1, 2, \ldots, nBH\}, \tag{10}$$

where

$$\mathbf{n} = [n(1), n(2), \ldots, n(nT)],\ \mathbf{l} = [l(1), l(2), \ldots, l(nBH)],\ nBH = \sum_{i=1}^{nT} n(i). \tag{11}$$

Additional scenarios involving penetrations of pressurized brine pockets were also defined. For cuttings removal in the 1992 WIPP PA, $nT = 6$ and the individual time intervals were [100, 150 yr], [150, 200 yr], [200, 500 yr], [500, 1500 yr], [1500, 4500 yr] and [4500, 10,000 yr]. Scenarios of the form $\mathcal{S}(\mathbf{l},\mathbf{n})$ were used as the basis for the CCDFs for normalized release to the accessible environment presented in the 1992 WIPP PA (e.g., as shown in Fig. 2) (Ref 15, Ch. 2; Ref. 20).

Probabilities for scenarios were determined under the assumption that the occurrence of boreholes through the repository follows a Poisson process with a rate constant λ (Ref. 15, Ch. 2; Refs. 20, 21). The probabilities $pS(\mathbf{n})$ and $pS(\mathbf{l},\mathbf{n})$ for the scenarios $\mathcal{S}(\mathbf{n})$ and $\mathcal{S}(\mathbf{l},\mathbf{n})$ are given by

$$pS(\mathbf{n}) = \left\{ \prod_{i=1}^{nT} \left[\frac{\lambda^{n(i)} (t_i - t_{i-1})^{n(i)}}{n(i)!} \right] \right\} \exp\left[-\lambda (t_{nT} - t_0) \right] \tag{12}$$

and

$$pS(\mathbf{l},\mathbf{n}) = \left(\prod_{j=1}^{nBH} pL_{l(j)} \right) pS(\mathbf{n}), \tag{13}$$

where $\mathbf{n}$, $\mathbf{l}$ and nBH are defined in Eq. (11) and pL_l is the probability that a randomly placed borehole through a waste panel will encounter waste of activity level l. Table 2.5-4 of Ref. 15 provides an example of probabilities $pS(\mathbf{n})$ calculated as shown in Eq. (12) with $\lambda = 3.78 \times 10^{-4}$ yr^{-1}, which corresponds to the maximum drilling rate suggested for use by the EPA.[11] Related expressions were also developed for the probability of scenarios that involve penetration of pressurized brine pockets (Ref. 8, Vol. 2, Chs. 2 and 3; Refs. 20, 21).

As indicated in Fig. 3, the following computer models were used to estimate scenario consequences in the 1992 WIPP PA: CUTTINGS, BRAGFLO, PANEL, SECO2D and SECOTP. Descriptions of these models are given in Marietta et al. (these

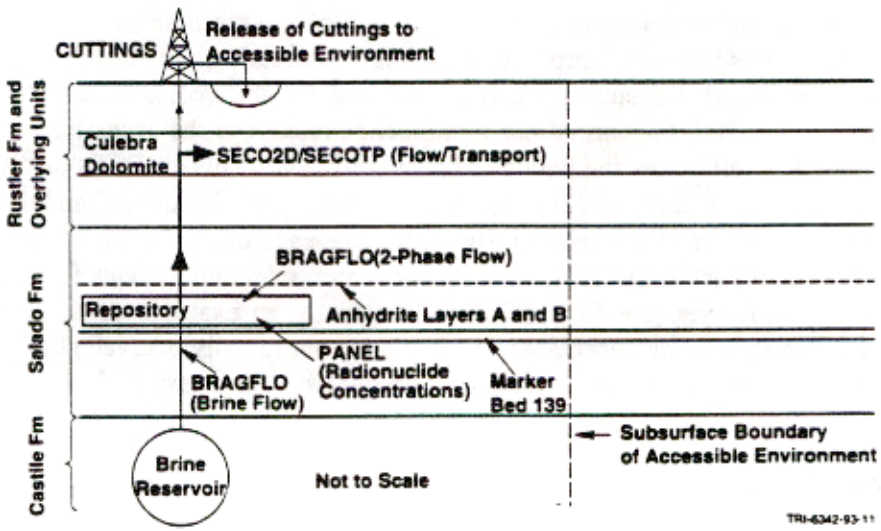


Figure 3. Models used in 1992 WIPP PA.

Proceedings) and in more detail in Vol. 2 of Ref. 14. Detailed calculations were performed for a subset of the scenarios indicated in Eq. (9) and then used to algebraically construct the releases associated with the remaining scenarios needed to develop CCDFs of the form shown in Fig. 2 (Ref. 9, Vol. 2, Ch. 3; Ref. 20).

DISCUSSION

The need to separate stochastic and subjective uncertainty controls the overall organization of the WIPP PA. Without this separation, it is difficult to assess the meaning of probabilistic statements coming out of the assessment (i.e., do these statements represent different possibilities that have a real potential of occurring, a degree of belief with respect to different alternatives, or some combination of the preceding). The probabilities pS_i appearing in Eq. (1) represent stochastic uncertainty. As indicated Eqs. (2), (3) and (4), subjective uncertainty enters the PA due to analyst uncertainty with respect to how to evaluate the risk representation in Eq. (1). What is referred to as uncertainty and sensitivity analyses is typically an attempt to assess the impact of subjective uncertainty. Uncertainty and sensitivity analysis play an important role in a PA by both indicating how much confidence should be placed in the results and where efforts can be invested most productively to improve this confidence.

With respect to stochastic and subjective uncertainty, there are actually two probability spaces: A probability space $(S_{st}, \mathcal{A}_{st}, p_{st})$ for stochastic uncertainty and a probability space $(S_{su}, \mathcal{A}_{su}, p_{su})$ for subjective uncertainty. The WIPP PA uses a different experimental design to cover each space. The division of the sample space S_{st} associated with stochastic uncertainty into the scenarios S_i in Eq. (1) is a form of importance sampling. The scenarios S_i are the strata in this design and the scenario probabilities pS_i are the strata probabilities. Importance sampling is often used to assure the inclusion of potentially important, but low probability, events in an analysis. The sample space S_{su} associated with subjective uncertainty is covered with a design based on random or Latin hypercube sampling.[22] This design is used to assure the full coverage of the range of each variable and is often used when either there is not enough information to plan an analysis based on importance sampling or the presence of a large number of potential dependent variables makes the use of importance sampling impractical.

The primary focus of the EPA standard for the geologic disposal of radioactive waste[11] is a CCDF for normalized radionuclide release to the accessible environment that is required to fall below the bound indicated in Fig. 1. This CCDF is displaying the effect of stochastic uncertainty and is constructed from the probabilities pS_i and the vectors $\mathbf{cS}_i$ in Eq. (1). Further, as illustrated in Fig. 2, the presence of subjective uncertainty leads to a distribution of such CCDFs. Upon first encounter, many individuals feel that this standard is novel. However, the EPA standard is actually an example of the Farmer limit line approach to specifying acceptable risk[23] and is conceptually equivalent to the large release safety goal proposed by the U.S. Nuclear Regulatory Commission.[24, 25]

REFERENCES

1. U.S. DOE, DOE/EIS-0026, 1980.
2. U.S. DOE, DOE/EIS-0026-FS, 1990.
3. U.S. DOE, DOE/EM/48063-2, 1991.
4. S.G. Bertram-Howery, et al., SAND89-0178, 1989.

5. A.R. Lappin, et al., SAND89-0462, 1989.
6. M.G. Marietta, et al., SAND89-2027, 1989.
7. S.G. Bertram-Howery, et al., SAND90-2347, 1990.
8. WIPP Performance Assessment Division, SAND91-0893/1, 2, 3, 1991.
9. J.C. Helton, et al., SAND91-0893/4, 1992.
10. S. Kaplan and B.J. Garrick, *Risk Anal.* **1**, 11-27 (1981).
11. U.S. EPA, *Federal Register* **50**, 38066-38089 (1985).
12. J.C. Helton, et al., *Nucl. Sci. Eng.* **114**, 286-331 (1993).
13. J.C. Helton, et al., *Sci. Basis Nucl. Waste Management* **26**, 885-898 (1993).
14. WIPP Performance Assessment Division, SAND92-0700/1, 2, 3, 1992.
15. WIPP Performance Assessment Division, SAND92-0700/4, 1993.
16. J.C. Helton, *Nucl. Tech.* **101**, 18-39 (1993).
17. International Atomic Energy Agency, Safety Series Report No. 100, 1989.
18. J.C. Helton, et al., SAND90-7103, 1991.
19. R.M. Cranwell, et al., NUREG/CR-1667, SAND80-1429, 1990.
20. J.C. Helton and H.J. Iuzzolino, *Rel. Eng. Sys. Safety* **40**, 277-293 (1993).
21. J.C. Helton, *Rel. Eng. Sys. Safety* **40**, 259-275 (1993).
22. M.D. McKay, et. al., *Technometrics* **21**, 239-245 (1979).
23. F.R. Farmer, *Nucl. Safety* **8**, 539-548 (1967).
24. U.S. NRC, *Federal Register* **51**(162), 30028-30033 (1986).
25. J.C. Helton and R.J. Breeding, *Rel. Eng. Sys. Safety* **39**, 129-158 (1993).

USING DATA AND INFORMATION TO FORM DISTRIBUTIONS OF MODEL PARAMETERS IN STOCHASTIC SIMULATIONS OF PERFORMANCE OF THE WASTE ISOLATION PILOT PLANT (WIPP)

Martin S. Tierney[1]

[1] Sandia National Laboratories, Albuquerque, NM 87185

INTRODUCTION

Before disposing of transuranic radioactive waste at the Waste Isolation Pilot Plant (WIPP), the U.S. Department of Energy (DOE) must evaluate compliance with long-term regulations of the U.S. Environmental Protection Agency (EPA), specifically the *Environmental Standards for the Management and Disposal of Spent Nuclear Fuel, High-Level and Transuranic radioactive Wastes* (40 CFR 191), and the *Hazardous and Solid Waste Amendments to the Resource Conservation and Recovery Act* (RCRA). Sandia National Laboratories (SNL) is conducting iterative performance assessments (PAs) of the WIPP for the DOE to provide interim guidance and to comply with the requirements of the *Land Withdrawal Act* (PL-102-579), which reinstated the major part of 40 CFR 191 for the WIPP as first promulgated in 1985. These PAs take the form of stochastic simulations of possible long-term behavior of the WIPP system using computer-implemented mathematical models of that system (consequence models). Uncertainties in long-term system behavior are studied by propagating uncertanties in consequence-model parameters through a calculation using Monte Carlo methods. Models that assign probabilities to ranges of the consequence-model parameters are here called *probability models*.

This paper describes methods used to form distributions of uncertain model parameters that appear in the system of linked computer codes developed to perform the consequence calculations (Marietta et al., these *Proceedings*) within the overall methodology for stochastic simulation of the WIPP (Helton et al., these *Proceedings*).

THE WIPP PARAMETER SET

As suggested by the scheme of Granger Morgan et al.,[1] the types of quantities appearing as elements of the WIPP parameter set can be classified in seven categories:

1. *Model constants*, for example, precisely known constants such as Planck's constant = 6.6256×10^{-27} erg s, or $\pi = 3.14159$.

2. *Model-domain parameters*, for example, coordinates of nodes on spatial and temporal grids; locations and dimensions of engineered features of the system.

3. *Model-control parameters*, for example, any parameter set by the user to control timing and accuracy of computations: number of dynamic time steps, numbers giving convergence criteria, cutoff values for certain dependent variables.

4. *Material-property parameters*. Parameters specifying magnitudes of physical or chemical properties of materials that occupy cells of a spatial grid or parts of system features; this category may also include initial and boundary conditions on submodel dependent variables. Examples are shown in Table 1.

5. *Event-and-process parameters*. This category is the time-domain counterpart of material-property parameters; it includes the number of external events of a given kind that act upon the system during a given interval on the time grid (e.g., the number of exploratory boreholes that penetrate a waste disposal compartment between 2000 and 3000 yr after closure) and the intensities of external processes that affect the system during each interval of the time grid (e.g., mean precipitation and temperature as functions of time in a region under changed climatic conditions). See Table 2 for examples.

6. *Indices for alternative models*. There are several acceptable submodels of phenomenon relevant to WIPP performance that nevertheless may differ in their influence on results of a calculation with the total-system model; to test this influence, alternatives are numbered, runs are made incorporating each alternative in the total-system model, and results are compared.

Table 1. Some uncertain material-property parameters of consequence models used in 1991 WIPP PA exercises (adopted from Tables 6.0-1 and 6.0-2 of Ref. 5).

Material	Properties
Halite within Salado Formation	Undisturbed permeability and pore pressure.
Anhydrite layers within Salado Formation	Undisturbed permeability, porosity, pore pressure; threshold displacement pressure.
Castile Formation brine	Initial pressure; bulk reservoir storativity.
Culebra Dolomite Member of Rustler Formation	Longitudinal dispersivity; matrix and fracture porosity; fracture spacing; matrix and fracture partition coefficients for elements Am, Np, Pu, Th and U; transmissivity field (60 equally likely realizations).
Unmodified waste form	Gas generation rates for corrosion and microbial action under inundated and humid conditions; stoichiometric coefficients for corrosive and microbial action; solubilities for nuclide charge states Am^{3+}, Np^{4+}, Np^{5+}, Pu^{4+}, Pu^{5+}, Th^{4+}, U^{4+}; U^{6+}; Eh-pH conditions; volume fractions of metals/glass and combustibles; initial waste saturation.

Table 2. Some event-and-process and probability-model parameters used in 1991 WIPP PA exercises (adopted from Table 6.0-3 of Ref. 5).

Event-and-Process Parameters:
1. Intrusion borehole diameter
2. Intrusion borehole permeability
3. Recharge amplitude factor under climate change
4. Area of pressurized brine reservoir underlying WIPP site
Probability-Model parameter:
5. Rate constant in Poisson Drilling Model

7. *Probability-model parameters*, for example, means, variances and correlation coefficients in analytic probability distributions for values of material-property parameters; mean rates of occurrence of events of a given kind (appearing in probability distributions for event-and-process parameters); weights assigned to the indices of alternative forms of a submodel. See Table 2 for an example.

The current data base for WIPP model parameters[2] has entries for more than 200 parameters in categories 5, 6 and 7. Almost all of these parameters are uncertain (i.e., they cannot be assigned a single, precise value) because (a) measurements of quantities from which the parameter can be calculated are absent or too few in number to form a precise estimate of the parameter using classical methods of statistics; or (b) the parameter quantifies some aspect of a hypothetical event, process, or natural feature that is believed to influence the performance of the WIPP system (e.g., the number of inadvertently drilled boreholes that penetrate the WIPP repository in the 10,000-yr period following closure). Uncertainty in a parameter is quantified in the time-honored fashion by defining a probability distribution on the natural range of parameter values. Although all of the 200+ model parameters have been assigned probability distributions, sensitivity and uncertainty studies with WIPP models[3,4] have to date investigated effects of parametric uncertainty arising from the "sampling" of only about 70 distinct parameters.

FORMATION OF DISTRIBUTIONS

In the WIPP PA, formation of a cumulative distribution function (CDF) for an uncertain parameter may employ either empirical data or subjective judgments of experts, or a mix of the two kinds of information; in addition, considerable judgment on the part of PA analysts is required to ensure that parameter distributions are relevant to the spatial and temporal scales implicit in the numerical consequence models.

Techniques for constructing CDFs for uncertain model parameters fall roughly into three classes: (1) direct use of data to construct an *empirical* CDF; (2) finding the analytic distribution that best fits available data (e.g., through use of the Kolmogorov-Smirnov test or the chi-squared test), and (3) Bayesian techniques that combine available data and expert judgment to form prior and posterior CDFs.[6] Class 3 includes all subjective procedures that rely entirely upon expert judgment to assign a shape to the distribution. The amount of subjective judgment required by these techniques increases from class 1 to 3; the "best" technique to be used in a particular situation depends strongly upon the kinds and amounts of empirical data and subjective information that are available concerning the parameter.

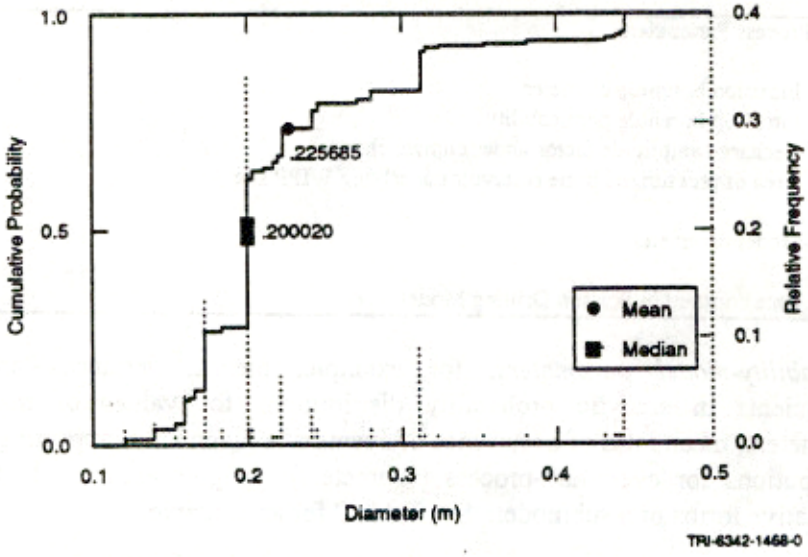


Figure 1. Distribution of historical drill bit diameters (Figure 4.2-7, Ref. 5)

Construction of empirical CDFs using available empirical data is appropriate if the parameter is intrinsically discrete (e.g., Figure 1) or when there are many data points for an intrinsically continuous quantity and that quantity can be related to the parameter by a deterministic, continuous function. The advantage of this technique lies in the fact that the empirical CDF is an unbiased estimator of the population's true CDF;[7] its disadvantages are that the empirical CDF may not capture probabilities of extreme values at the tails of the distribution, and—for continuous parameters and few data points—the empirical CDF may be too coarse to permit a representative, uniform set of sample values of the parameter to be drawn. The latter disadvantage may in part be offset by joining the vertices of the piecewise constant empirical CDF with straight lines (e.g., Figure 2), a procedure that is computationally simple and is justified by the Maximum Entropy Principle.[8]

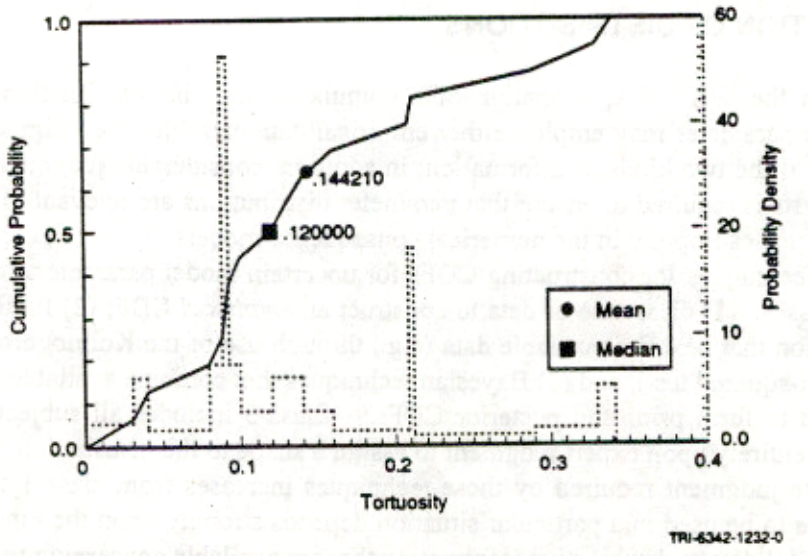


Figure 2. Distribution of tortuosity of Culebra matrix (Figure 2.6-15, Ref. 5)

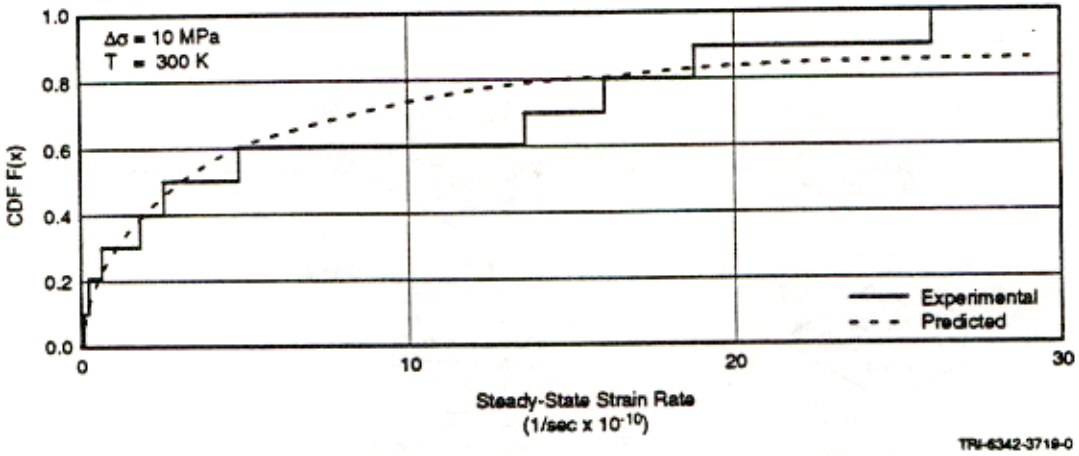


Figure 3. Typical comparison between predicted and experimental CDF for the parameter, ε_s, at T = 300 K and $\Delta\sigma$ = 10 MPa. (Example of use of Kolmogorov-Smirnov Test to fit a distribution taken from Ref. 9.)

The two standard techniques for testing whether a data set is consistent with a proposed analytic distribution (i.e., normal, lognormal, beta distributions, etc.) are the chi-squared test and the Kolmogorov-Smirnov test. The use of either technique is seldom mentioned in published performance assessments, perhaps because of the sparse data sets so characteristic of measured quantities in the earth sciences or because these tests require lengthy calculations with the data before a distribution is chosen. In connection with PA for the WIPP Project, Pfeifle et al.,[9] have used the Kolmogorov-Smirnov test to find analytic distributions that are consistent with their measurements of certain constants (e.g., Figure 3) appearing in a mathematical model of salt creep.

WIPP PA analysts have been compelled to adopt techniques from class 3 (Bayesian and subjective techniques) to construct distributions for most of the uncertain parameters appearing in their consequence models.[5] Because of the expense and time required to make and interpret measurements of earth-science quantities, the process of constructing CDFs for WIPP consequence model parameters has largely bypassed classical techniques of Bayesian estimation and has instead relied heavily on purely subjective judgments of scientific specialists. The elicitation of the judgment of specialists can be either an informal process involving only a few responsible investigators (Figure 4), or a formal process involving many experts and rigid controls.[10] Examples of distributions obtained by informal and formal elicitations are shown respectively in Figures 5 and 6.

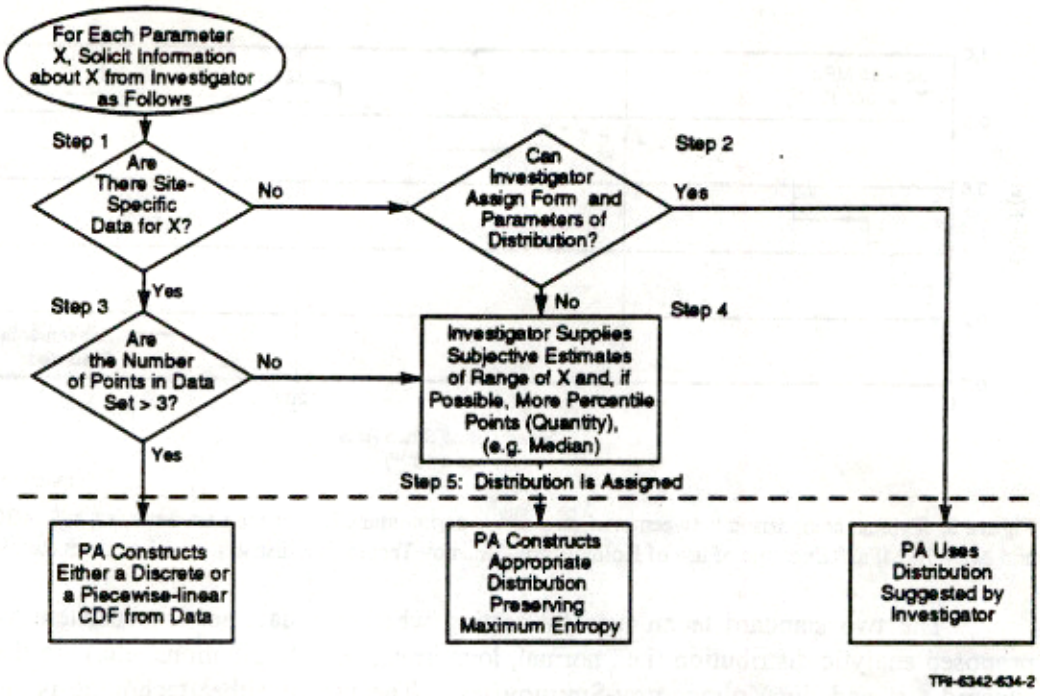


Figure 4. An informal five-step procedure used to construct cumulative distribution functions for the 1990 WIPP performance simulations. (Figure E-1, Ref. 8).

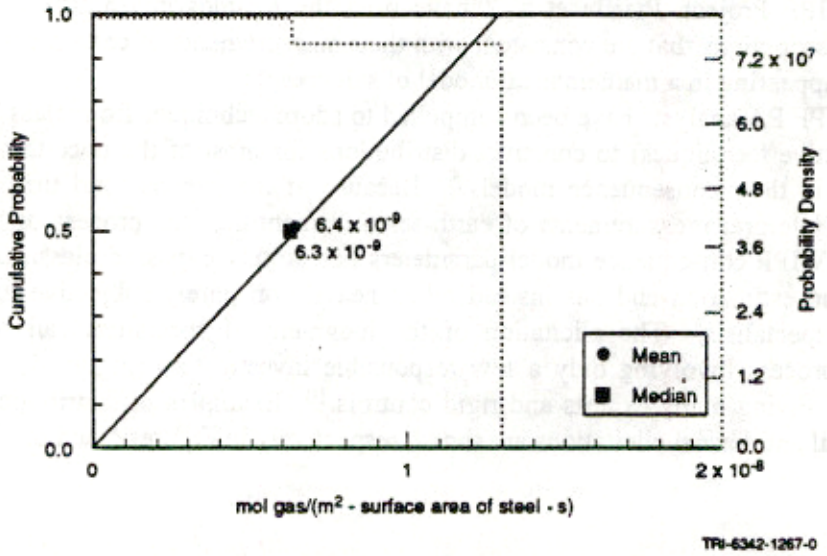


Figure 5. Constructed distribution for gas production rates from corrosion under inundated conditions. (Distribution obtained from informal elicitation.) (Figure 3.3-11, Ref. 5).

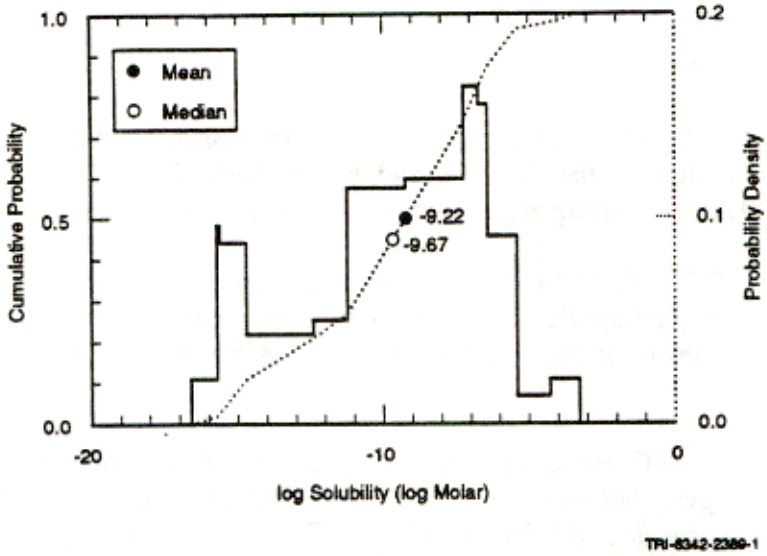


Figure 6. Constructed distribution for solubility of plutonium. (Distribution obtained from formal elicitation.) (Figure 3.3-3(e), Ref. 2).

REFERENCES

1. Granger Morgan, M., M. Henrion, and M. Small. 1990. *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*. Cambridge, UK: Cambridge University Press.

2. WIPP PA (Performance Assessment) Division. 1991. *Preliminary Comparison with 40 CFR Part 191, Subpart B for the Waste Isolation Pilot Plant, December 1991. Volume 3: Reference Data*. SAND91-0893/3. Albuquerque, NM: Sandia National Laboratories.

3. WIPP PA (Performance Assessment) Department. 1992. *Preliminary Performance Assessment for the Waste Isolation Pilot Plant, December 1992. Volume 3: Model Parameters*. SAND92-0700/3. Albuquerque, NM: Sandia National Laboratories.

4. Helton, J.C., J.W. Garner, R.D. McCurley, and D.K. Rudeen. 1991. *Sensitivity Analysis Techniques and Results for Performance Assessment at the Waste Isolation Pilot Plant*. Contractor Report SAND90-7103. Albuquerque, NM: Sandia National Laboratories.

5. WIPP PA (Performance Assessment) Department. 1992. *Long-Term Gas and Brine Migration at the Waste Isolation Pilot Plant: Preliminary Sensitivity Analyses for Post-Closure 40 CFR 268 (RCRA), May 1992*. SAND92-1933. Albuquerque, NM: Sandia National Laboratories.

6. Martz, H., and R. Waller. 1982. *Bayesian Reliability Analysis*. New York, NY: John Wiley and Sons, Inc.

7. Blom, G. 1989. *Probability and Statistics: Theory and Applications*. New York, NY: Springer-Verlag.

8. Tierney, M.S. 1990. *Constructing Probability Distributions of Uncertain Variables in the Models of the Performance of the Waste Isolation Pilot Plant (WIPP)*. SAND90-2510. Albuquerque, NM: Sandia National Laboratories.

9. Pfeifle, T.W., K.D. Mellegard, and D.E. Munson. 1992. *Determination of Probability Density Functions for Parameters in the Munson-Dawson Model for Creep Behavior of Salt*. SAND90-2366. Albuquerque, NM: Sandia National Laboratories.

10. Bonano, E.J., S.C. Hora, R.L. Keeney, and D. von Winterfeldt. 1990. *Elicitation and Use of Expert Judgment in Performance Assessment for High-Level Radioactive Waste Repositories*. SAND89-1821; NUREG/CR-5411. Albuquerque, NM: Sandia National Laboratories.

MODELING SYSTEM USED FOR THE PERFORMANCE ASSESSMENT FOR THE WASTE ISOLATION PILOT PLANT (WIPP)

M.G. Marietta*, J.C. Helton, **, and M.S. Tierney*

*Sandia National Laboratories, Albuquerque, NM 87185
**Arizona State University, Tempe, AZ 85287

INTRODUCTION

Before disposing of transuranic radioactive waste at the Waste Isolation Pilot Plant (WIPP), the United States Department of Energy (DOE) must evaluate compliance with long-term regulations of the United States Environmental Protection Agency (EPA), specifically the *Environmental Standards for the Management and Disposal of Spent Nuclear Fuel, High-Level and Transuranic Radioactive Wastes* (40 CFR 191) (EPA, 1985), and the *Hazardous and Solid Waste Amendments* to the *Resource Conservation and Recovery Act* (RCRA, 1976). Sandia National Laboratories (SNL) is conducting iterative performance assessments (PAs) of the WIPP for the DOE to provide interim guidance and to comply with the requirements of the *Land Withdrawal Act* (WIPP LWA, 1992), which reinstated the major part of 40 CFR 191 for the WIPP as first promulgated in 1985. An additional, non-regulatory objective, which has been requested by the DOE and the National Academy of Sciences WIPP Panel, is to evaluate the long-term safety of the WIPP.

This paper describes the PA system of linked computer codes that has been developed to perform consequence calculations within the probabilistic system assessment methodology for the WIPP. The methodology is described by Helton in these *Proceedings*. Data and cumulative distribution functions (CDFs) are described by Tierney in these *Proceedings*.

CONSEQUENCE MODELING SYSTEM FOR 1992

Consequence modeling for the WIPP performance assessment uses a linked system of computational models to describe the disposal system and a Monte Carlo technique that relies on multiple simulations using sampled values for selected input parameters to quantify uncertainty in the performance estimate. A full analysis includes selecting imprecisely known parameters to be sampled, constructing distributions for each of these parameters incorporating available data and subjective information (Tierney, 1994, in these *Proceedings*), generating a sample from these variables, and calculating consequences for each sample element. Consideration of alternative conceptual models, which may require

different input parameters and perhaps different computational models, at present is included by repeating the full analysis for each conceptual model to assess uncertainty among alternative models. Results for preliminary comparison with 40 CFR 191, Subpart B, are usually displayed in terms of complementary cumulative distribution functions (CCDFs), which are plots of exceedance probability versus consequence. The consequence measure for §191.13 is the EPA normalized sum. Construction of CCDFs is discussed by Helton, 1994, in these *Proceedings*.

Uncertainty and sensitivity analyses use a Latin hypercube sampling technique followed by stepwise rank regression analysis (Iman and Helton. 1985; Helton et al, 1991, 1992). In other sensitivity analyses for alternative conceptual models, specific parameter groups are assigned fixed values corresponding to extreme and median values, and all other parameters in the database are sampled probabilistically over the full range of possible values. A parameter or group of parameters is thus tested *ceteris paribus* (all other things being equal) within a Monte Carlo simulation (Helton et al., 1991). To compare with the 40 CFR 191 for each conceptual model, results are assembled into CCDF plots of probability versus 10,000-year normalized cumulative radionuclide release, as recommended in the guidance to 40 CFR 191. The technique isolates effects of variations in parameter groups (used to represent alternative conceptual models) on predicted performance. Priorities can then be suggested for future modeling and experimental research.

COMPUTATIONAL MODELS

Major computer programs (codes) used in the computational models for the 1992 preliminary performance assessment (Table 1 and Figure 1) are described in detail in Sandia WIPP Performance Assessment Department, 1992. They reflect improvements in the conceptual and numerical models used in three previous performance assessments (Marietta et al., 1989; Bertram-Howery et al., 1990; and WIPP PA Division, 1991), and permit the replacement of simplifying assumptions with more realistic models. Three of the most significant improvements in 1992 are discussed here.

The 1992 calculations mark the first time the effects of salt creep were explicitly included in performance assessments. Salt will deform over time by creep in response to a pressure gradient, and; if the repository remained at atmospheric pressure, lithostatic stresses would cause it to close almost completely within 100 years (Tyler et al., 1988; Munson et al., 1989a,b). Gas will be generated within the repository by degradation of the waste, however, and pressure within the repository will rise to elevated levels that will retard complete creep closure and may perhaps partially reverse the process. In 1991, no model was available to describe the coupled interaction of creep closure and gas pressurization, and the performance-assessment calculations used a simplifying assumption that porosity within the disposal region would remain constant through time. As discussed in detail in WIPP PA Department, 1992, the 1992 calculations use output from the geomechanical code SANCHO (Stone et al., 1985) to define the porosity of the waste as a function of pressure. Although this method does not represent a full coupling of creep closure and gas generation, the modeling improvement allows the performance assessment to evaluate the importance of changing void volume in the repository.

The method used to incorporate spatial variability in the transmissivity field in the Culebra was modified significantly from that used in 1991. The Performance Assessment Department now uses an automated inverse approach to calibrate a two-dimensional model to both steady-state and transient pressure data generating multiple realizations of the

Table 1. Summary of Computer Models Used in the 1992 WIPP Performance Assessment to Calculate Scenario Consequences

Model	Description
BRAGFLO	Describes the multiphase flow of gas and brine through a porous, heterogeneous reservoir. BRAGFLO solves simultaneously the coupled partial different equations that describe the mass conservation of gas and brine along with appropriate constraint equations, initial conditions, and boundary conditions. Additional information: WIPP PA Department, 1992.
CCDFPERM	Constructs probabilities and consequences for various computational scenarios associated with human intrusion by exploratory drilling. Also constructs CCDFs. Additional information: WIPP PA Department, 1992; Helton and Iuzzolino, 1993.
CUTTINGS	Calculates the quantity of radioactive material brought to the surface in cuttings and cavings generated by an exploratory borehole that penetrates a waste panel. Additional information: Berglund, 1992.
GENII-S	Estimates potential radiation doses to humans from radionuclides in the environment. Additional information: Leigh et al., 1993.
GRASP-INV	Generates transmissivity fields (estimates of transmissivity values) conditioned on measured transmissivity values and calibrated to steady-state and transient pressure data at well locations using an adjoint sensitivity and pilot-point technique. Additional information: LaVenue and RamaRao, 1992.
PANEL	Calculates rate of discharge and cumulative discharge of radionuclides from a repository panel through an intrusion borehole. Discharge is a function of fluid flow rate, elemental solubility, and radionuclide inventory. Additional information: WIPP PA Division, 1991, Section 5.3.
SECO_FLOW	Calculates single-phase Darcy flow for groundwater-flow problems in two dimensions. The formulation is based on a single partial differential equation for hydraulic head using fully implicit time differencing. Additional information: WIPP PA Department, 1992; Roache, 1992.
SECO_TRANSPORT	Simulates fluid flow and transport of radionuclides in fractured porous media. Additional information: WIPP PA Department, 1992; Roache, 1992.
SANCHO	Solves quasistatic large deformation, inelastic response of two-dimensional solids with finite-element techniques. Used in the 1992 performance assessment to determine porosity of the waste as a function of time and cumulative gas generation. Additional information: WIPP PA Department, 1992; Stone et al., 1985.

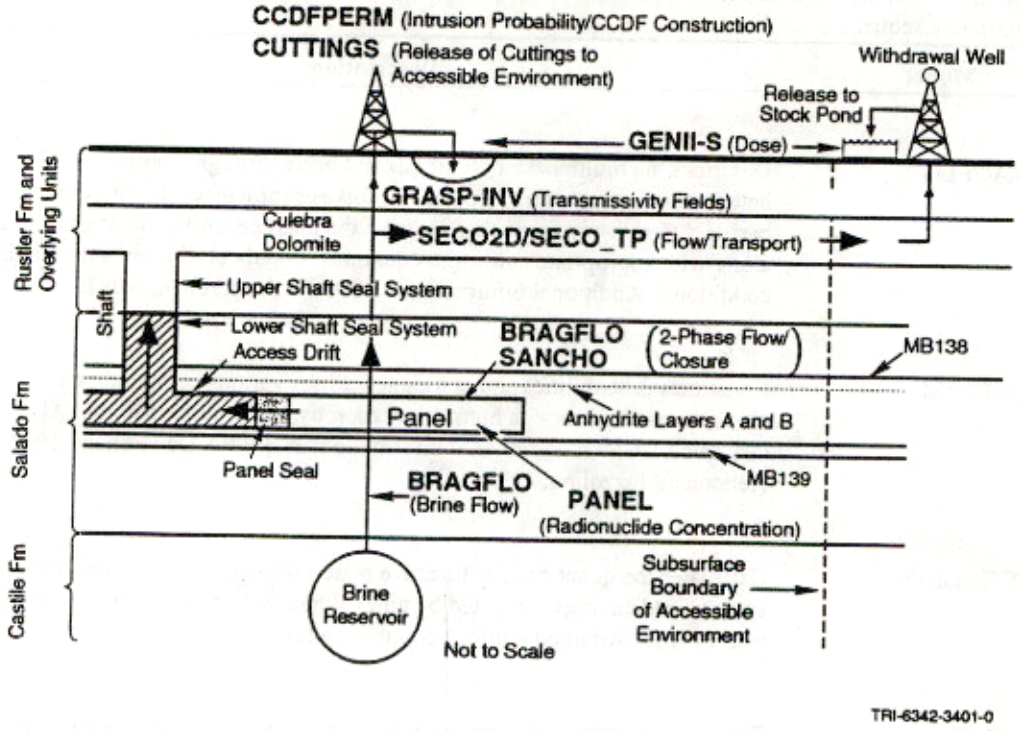


Figure 1. Major codes used in the 1992 performance assessment.

transmissivity field (LaVenue and RamaRao, 1992). Seventy equally probable, calibrated fields were sampled for use in the 1992 performance assessment.

Radionuclide transport in the Culebra, which had been simulated using STAFF2D (Huyakorn et al., 1991) in the 1991 performance assessment, is now simulated by the SECO_TP code. SECO_TP is a dual-porosity model in which advective transport is allowed only in fractures, and diffusion of solute occurs into the rock matrix surrounding the fracture. The fracture system for the 1992 simulation is idealized as planar and parallel, and each fracture wall may be coated with a layer of clay of both uniform thickness and porosity. The model is capable of simulating both physical retardation by diffusion and chemical retardation by sorption in both clay fracture-linings and dolomite matrix.

IMPROVEMENTS FOR NEXT PERFORMANCE ASSESSMENT ITERATION

Several significant improvements remain to be made in the performance-assessment modeling system, including the following. First, the model used in 1992 for groundwater flow in the Culebra does not include possible effects of subsidence related to potash mining or a representation of recharge that includes present or future vertical groundwater flow within the Rustler Formation (leakage). A three-dimensional version of SECO_FLOW/ SECO_TRANSPORT is being used to assess the importance of these subsidence effects as well as the importance of other past modeling assumptions. Second, the model used to represent the response of the repository and the surrounding strata to the generation of gas by waste degradation does not include effects of possible pressure-dependent fracturing of anhydrite layers within the Salado Formation. A submodel to capture the effects of possible anhydrite fracturing has been included in BRAGFLO. In addition, a new mechanistic, gas-generation model is presently being developed to evaluate the adequacy of the simple

stoichiometric formulation presently in BRAGFLO. Finally, the cuttings model has been modified to estimate the possible spalling of borehole-wall waste material into the intrusion hole when the drill bit penetrates a gas-pressurized repository. The releases resulting from such spallation will be included as direct releases to the surface.

REFERENCES

Berglund, J.W. 1992. Mechanisms Governing the Direct Removal of Wastes from the Waste Isolation Pilot Plant Repository Caused by Exploratory Drilling. SAND92-7295. Albuquerque, NM: Sandia National Laboratories.

Bertram-Howery, S.G., M.G. Marietta, R.P. Rechard, P.N. Swift, D.R. Anderson, B.L. Baker, J.E. Bean, Jr., W. Beyeler, K.F. Brinster, R.V. Guzowski, J.C. Helton, R.D. McCurley, D.K. Rudeen, J.D. Schreiber, and P. Vaughn. 1990. *Preliminary Comparison with 40 CFR Part 191, Subpart B for the Waste Isolation Pilot Plant, December 1990.* SAND90-2347. Albuquerque, NM: Sandia National Laboratories.

EPA (Environmental Protection Agency). 1985. "40 CFR Part 191: Environmental Standards for the Management and Disposal of Spent Nuclear Fuel, High-Level and Transuranic Radioactive Wastes; Final Rule," *Federal Register*. Vol. 50, no. 182, 38066-38089.

Helton, J.C., and H.J. Iuzzolino. 1993. "Construction of Complementary Cumulative Distribution Functions for Comparison with the EPA Release Limits for Radioactive Waste Disposal," *Reliability Engineering and System Safety*. Vol. 40, no. 3, 277-293.

Helton, J.C., J.W. Garner, R.D. McCurley, and D.K. Rudeen. 1991. *Sensitivity Analysis Techniques and Results for Performance Assessment at the Waste Isolation Pilot Plant.* Contractor Report SAND90-7103. Albuquerque, NM: Sandia National Laboratories.

Helton, J.C., J.W. Garner, R.P. Rechard, D.K. Rudeen, and P.N. Swift. 1992. *Preliminary Comparison with 40 CFR Part 191, Subpart B for the Waste Isolation Pilot Plant, December 1991. Volume 4: Uncertainty and Sensitivity Analysis Results.* SAND91-0893/4. Albuquerque, NM: Sandia National Laboratories.

HSWA. 1984. *Hazardous and Solid Waste Amendments of 1984.* Public Law 98-616.

Huyakorn, P.S., H.O. White, Jr., and S. Panday. 1991. *STAFF2D Version 3.1: A Two-Dimensional Finite Element Code for Simulating Fluid Flow and Transport of Radionuclides in Fractured Porous Media with Water Table Boundary Conditions.* Herndon, VA: HydroGeoLogic, Inc.

Iman, R.L., and J.C. Helton. 1985. *A Comparison of Uncertainty and Sensitivity Analysis Techniques for Computer Models.* SAND84-1461, NUREG/CR-3904. Albuquerque, NM: Sandia National Laboratories.

LaVenue, A.M., and B.S. RamaRao. 1992. *A Modeling Approach To Address Spatial Variability within the Culebra Dolomite Transmissivity Field.* SAND92-7306. Albuquerque, NM: Sandia National Laboratories.

Leigh, C.D., B.M. Thompson, J.E. Campbell, D.E. Longsine, R.A. Kennedy, and B.A. Napier. 1993. *User's Guide for GENII-S: A Code for Statistical and Deterministic Simulations of Radiation Doses to Humans from Radionuclides in the Environment.* SAND91-0561. Albuquerque, NM: Sandia National Laboratories.

Marietta, M.G., S.G. Bertram-Howery, D.R. Anderson, K.F. Brinster, R.V. Guzowski, H. Iuzzolino, and R.P. Rechard. 1989. *Performance Assessment Methodology Demonstration: Methodology Development for Evaluating Compliance with EPA 40 CFR 191, Subpart B, for the Waste Isolation Pilot Plant.* SAND89-2027. Albuquerque, NM: Sandia National Laboratories.

Munson, D.E., A.F. Fossum, and P.E. Senseny. 1989a. *Approach to First Principles Model Prediction of Measured WIPP In Situ Room Closure in Salt.* SAND88-2535. Albuquerque, NM: Sandia National Laboratories.

Munson, D.E., A.F. Fossum, and P.E. Senseny. 1989b. *Advances in Resolution of Discrepancies Between Predicted and Measured In Situ WIPP Room Closures.* SAND88-2948. Albuquerque, NM: Sandia National Laboratories.

RCRA. 1976. *Resource, Conservation, and Recovery Act of 1976.* Public Law 94-580, 90 Stat. 2795.

Roach, P.J. 1992. "Computational Fluid Dynamics Algorithms Developed for WIPP Site Simulations," *Proceedings of the 9th International Conference on Computational Methods in Water Resources, Denver, CO, June 1992.* p. 375-382.

Sandia WIPP Project. 1992. *Preliminary Performance Assessment for the Waste Isolation Pilot Plant, December 1992. Volume 3: Model Parameters.* SAND92-0700/3. Albuquerque, NM: Sandia National Laboratories.

Stone, C.M., R.D. Krieg, and Z.E. Beisinger. 1985. *SANCHO: A Finite Element Computer Program for the Quasistatic, Large Deformation, Inelastic Response of Two-Dimensional Solids.* SAND84-2618. Albuquerque, NM: Sandia National Laboratories.

Tyler, L.D., R.V. Matalucci, M.A. Molecke, D.E. Munson, E.J. Nowak, and J.C. Stormont. 1988. *Summary Report for the WIPP Technology Development Program for Isolation of Radioactive Waste.* SAND88-0844. Albuquerque, NM: Sandia National Laboratories.

WIPP LWA. 1992. *Waste Isolation Pilot Plant Land Withdrawal Act.* Public Law 102-579.

WIPP PA (Performance Assessment) Department. 1992. *Preliminary Performance Assessment for the Waste Isolation Pilot Plant, December 1992. Volume 2: Technical Basis.* SAND92-0700/2. Albuquerque, NM: Sandia National Laboratories.

WIPP PA (Performance Assessment) Department. 1993. *Preliminary Performance Assessment for the Waste Isolation Pilot Plant, December 1992. Volume 4: Uncertainty and Sensitivity Analyses for 40 CFR 191, Subpart B.* SAND92-0700/4. Albuquerque, NM: Sandia National Laboratories.

WIPP PA (Performance Assessment) Division. 1991. *Preliminary Comparison with 40 CFR Part 191, Subpart B for the Waste Isolation Pilot Plant, December 1991. Volumes 1-3.* SAND91-0893/1-3. Albuquerque, NM: Sandia National Laboratories.

REGULATORY AND INSTITUTIONAL CONSIDERATIONS IN PERFORMANCE ASSESSMENT FOR THE WASTE ISOLATION PILOT PLANT (WIPP)

D.R. Anderson, and M.G. Marietta

Sandia National Laboratories, Albuquerque, NM 87185

INTRODUCTION

Before disposing of transuranic radioactive waste at the Waste Isolation Pilot Plant (WIPP), the United States Department of Energy (DOE) must evaluate compliance with long-term regulations of the United States Environmental Protection Agency (EPA), specifically the *Environmental Standards for the Management and Disposal of Spent Nuclear Fuel, High-Level and Transuranic Radioactive Wastes* (40 CFR 191) (EPA, 1985), and the *Hazardous and Solid Waste Amendments* to the *Resource Conservation and Recovery Act* (RCRA, 1976). Sandia National Laboratories (SNL) is conducting iterative performance assessments (PAs) of the WIPP for the DOE to provide interim guidance and to comply with the requirements of the *Land Withdrawal Act* (WIPP LWA, 1992), which reinstated the major part of 40 CFR 191 for the WIPP as first promulgated in 1985. An additional, non-regulatory objective, which has been requested by the DOE and the National Academy of Sciences WIPP Panel, is to evaluate the long-term safety of the WIPP.

This paper (1) provides background information on the regulation, (2) describes the approach, adopted by the WIPP PA, for building a consistent and defensible technical and modeling basis for the certification application, (3) presents example system performance measure results for 40 CFR 191, 40 CFR 268.6, and safety based on the WIPP PA (Helton, 1994, these *Proceedings*), data and information available (Tierney, 1994, these *Proceedings*), and models used (Marietta et al., 1994, these *Proceedings*), (4) identifies important issues to be resolved by the regulatory and applicant during the iterative (biennial) PA review process required by the *Land Withdrawal Act*, and (5) discusses institutional issues concerned with communication of a complex PA to various review groups, the regulator, and the public.

REGULATORY CRITERIA FOR THE WIPP

The EPA regulations applicable to the long-term performance of the WIPP include Subpart B of 40 CFR 191, promulgated in 1985 but remanded to the EPA in 1987 for reconsideration, and the regulations implementing the *Resource, Conservation, and Recovery Act* (RCRA, 1976). The Council on Environmental Quality promulgated the regulations

for implementing the *National Environmental Policy Act* (NEPA) (NEPA, 1970, as amended; EPA, 1978); however, the EPA has the responsibility for reviewing and publicly commenting on potential environmental impacts of major federal actions. Additional requirements are specified in the *WIPP Land Withdrawal Act* (WIPP LWA, 1992).

Radioactive-Waste Disposal Standards (40 CFR 191)

The radioactive-waste disposal standards, *40 CFR Part 191-Environmental Standards for the Management and Disposal of Spent Nuclear Fuel, High-Level and Transuranic Radioactive Waste* (EPA, 1985), are divided into two subparts. Subpart A applies to a disposal facility prior to decommissioning and limits annual radiation doses from waste management and storage operations to members of the public in the general environment. Subpart B applies after decommissioning and sets probabilistic limits on cumulative releases of radionuclides to the accessible environment for 10,000 years. Subpart B also sets probabilistic limits on both radiation doses to members of the public in the accessible environment for 1000 years of undisturbed performance and radioactive contamination of certain sources of groundwater within or near the controlled area for 1000 years after disposal. The DOE must provide a reasonable expectation that the WIPP will comply with the quantitative requirements of Subpart B of 40 CFR 191. Appendix A of 40 CFR 191 specifies how to determine release limits; Appendix B of 40 CFR 191 provides nonmandatory guidance for implementing Subpart B.

Resource, Conservation, and Recovery Act (RCRA)

The *Resource, Conservation, and Recovery Act* (RCRA) (RCRA, 1976) was enacted to provide management of hazardous wastes. The long-term regulations promulgated for implementing the RCRA, specifically 40 CFR 268 (EPA, 1986) for the WIPP, prohibit land disposal of specified hazardous wastes, including volatile organic compounds and heavy metals, unless the owner or operator of the facility petitions for a variance and successfully demonstrates "to a reasonable degree of certainty, that there will be no migration of hazardous constituents from the disposal unit or injection zone for as long as the wastes remain hazardous" or the waste is treated in accordance with applicable treatment standards (40 CFR 268.6(a), EPA, 1986). Guidance provided by the EPA on the interpretation of this wording indicates constituents below health-based or environmentally based levels at the disposal-unit boundary (EPA, 1992).

National Environmental Policy Act (NEPA)

The *National Environmental Policy Act* (NEPA) (NEPA, 1970, as amended) is enforced by regulations that are not specific regulatory guidelines, but contain a mandate for evaluating the environmental consequences of all significant aspects of a project (EPA, 1978). The DOE has prepared several environmental impact statements (EISs) that have addressed the predicted experimental, operational, and long-term behavior of the repository (US DOE, 1979, 1980, 1990a). The potential health risks posed by estimated groundwater releases of the TRU radionuclides and by the direct removal of radionuclides to the surface as a result of drilling have been assessed in the NEPA documentation for the WIPP.

The regulations that implement the NEPA do not specifically require calculating doses of radionuclides to members of the public. However, the WIPP Panel of the National

Academy of Sciences, a panel that reviews the scientific basis for the WIPP, has requested safety assessments that present dose calculations for 10,000 years or peak arrival times of radionuclides, whichever occurs first. In accordance with the WIPP Panel's request, preliminary probabilistic safety assessments in which doses have been calculated for hypothetical exposure pathways are part of the analyses that evaluate long-term performance of the WIPP.

UNDISTURBED PERFORMANCE

Analyses of undisturbed performance are of interest for both the Individual Protection Requirements (§191.15) of 40 CFR 191 and 40 CFR 268.6. Brine migration is of interest for 40 CFR 191 because of the potential for radionuclide transport in the liquid phase. Both gas and brine migration are of interest for 40 CFR 268.6 because of the potential for transport of regulated hazardous constituents in both gas and brine phases. However, preliminary results are intended to provide interim guidance to the WIPP Project as it develops a compliance strategy for 40 CFR 268.6, and should not be used as the basis for regulatory decisions. The modeling system and data base remain incomplete, and one potentially important process, the pressure-dependent fracturing of anhydrite interbeds above and below the waste-emplacement region, was included in the 1992 PA. Furthermore, transport of radionuclides and heavy metals in brine and volatile organic compounds in gas was not modeled. Performance measures described to date apply only to the migration of the fluid phases and do not provide information about potential concentrations of contaminants within the fluids. If additional analyses of gas and brine migration continue to show a potential for gas migration beyond regulatory boundaries, evaluations of hazardous constituent concentrations using expanded databases and more detailed computational models would be performed.

REQUIREMENTS OF 40 CFR 268.6

The *Land Disposal Restrictions* (EPA, 1986) regulate disposal of specified hazardous wastes. For the WIPP, hazardous constituents mixed with the radioactive transuranic waste can include solids such as lead and other heavy metals, and semivolatile and volatile organic compounds (VOCs) as residual liquids sorbed on waste materials or as gases associated with the waste in waste containers. A detailed inventory of the 40 CFR 268 contaminants anticipated for the WIPP is not available at this time, but a preliminary list of anticipated hazardous constituents were documented in the *Waste Isolation Pilot Plant No-Migration Variance Petition* (US DOE, 1990b). The Environmental Protection Agency (EPA) subsequently issued the *Conditional No-Migration Determination for the Department of Energy Waste Isolation Pilot Plant (WIPP),* which mandated waste characterization requirements for the WIPP Test Phase and recommended waste characterization data needs in support of any long-term performance assessment.

In general, 40 CFR 268 prohibits the disposal of hazardous wastes unless the owner or operator of the facility petitions for a variance and successfully demonstrates "to a reasonable degree of certainty, that there will be no migration of hazardous constituents from the disposal unit or injection zone for as long as the wastes remain hazardous" or the waste is treated in accordance with applicable standards (40 CFR 268.6 (a), EPA, 1986). General guidance provided by the EPA on the interpretation of this wording indicates that "no migration" will be defined to be concentrations of hazardous constituents below health-

based or environmentally based levels at the disposal-unit boundary (EPA, 1992). Following guidance from the EPA (EPA, 1990, p. 13073), the SNL WIPP PA Department has assumed for the purposes of these analyses that the length of the regulatory period is 10,000 yr.

The 40 CFR 268 Disposal Unit

The "disposal unit" for the WIPP as applied to 40 CFR 268.6 (RCRA, 1976) is defined to include the entire volume of the Salado Formation from top to bottom within the 41 km^2 (16 mi^2) WIPP land-withdrawal area (DOE, 1990c). The SNL WIPP PA Department assumes for the purpose of PA modeling that the disposal-unit boundaries will remain unchanged for long-term performance. The RCRA disposal unit contains a smaller volume than that contained within the boundary of the accessible environment used in preliminary comparisons with 40 CFR 191, Subpart B. As is the case for radionuclides regulated under 40 CFR 191, migration of hazardous constituents is allowed into the Salado Formation within the land-withdrawal area. Unlike the requirements of 40 CFR 191, however, migration of hazardous constituents into the Rustler Formation and other overlying strata within the land-withdrawal area could constitute a potential violation if they exceed concentration limits.

Human Intrusion and 40 CFR 268.6

The extent to which estimates of the consequences of human intrusion will be required for long-term compliance evaluations has not been determined. The EPA has determined that human intrusion need not be considered for the Test Phase, and describes it as a long-term issue to "be addressed at the time a petition is considered for permanent disposal" (EPA, 1990, p. 47720). Consideration of inadvertent human intrusion is required for compliance with 40 CFR 191, Subpart B, and analyses of the consequences of intrusion during exploratory drilling for hydrocarbons are performed.

PA METHODOLOGY

Analyses have been performed using the Monte Carlo methodology (Helton, 1994, these *Proceedings*) and modeling system (Marietta et al., 1994, these *Proceedings*) described in detail in WIPP PA Department, 1992. In keeping with the requirement in 40 CFR 191.13 for probabilistic estimates of performance and a consideration of uncertainty in the results, this methodology relies on multiple realizations using deterministic models of physical processes and a Latin hypercube sampling (LHS) strategy to incorporate uncertainty for input parameters. Values for selected parameters are described by a range and distribution based on available data (Tierney, 1994, these *Proceedings*), and each simulation uses a separate input vector of sampled values drawn from the assigned distributions. The methodology is well suited for conducting uncertainty and sensitivity analyses that provide quantitative and qualitative insights about the potential variability in model results caused by uncertainty in specific input data (Helton et al., 1991, 1992; Helton, 1993). Sensitivity analysis techniques and methods for displaying their results have been summarized by Helton et al. (1991). Scatterplots and stepwise linear regression analyses are used in this volume to evaluate model sensitivity to uncertainty in sampled parameters.

DISCUSSION OF THE 1992 PRELIMINARY COMPARISON WITH THE CONTAINMENT REQUIREMENTS

Results presented in WIPP PA Department, 1992 are consistent with the conclusion made in previous preliminary comparisons that performance estimates for the WIPP lie below the limits set by the Containment Requirements (Bertram-Howery et al., 1990; WIPP PA Division, 1991). As illustrated in Figure 1, consideration of alternative models for the probability of human intrusion and radionuclide transport in the Culebra provides insight into the relative impacts on performance of specific components of the natural barrier system and institutional controls at the WIPP.

The uppermost CCDF in Figure 1, labeled "Total, Single Porosity + Cuttings, λ_0" and calculated using the single-porosity and constant λ models, represents an estimate of the performance of the disposal system with very little contribution from the natural barrier provided by retardation in the Culebra and no contribution from the potential institutional barrier that could be provided by passive markers, as required by the Assurance Requirements. For the modeling system and data base used in 1992, the mean CCDF for this case lies below the EPA limits.

The segments of a CCDF shown with a dotted line and labeled "Total, Discharge from Borehole + Cuttings, λ_0" display performance with no contribution whatsoever from retardation in the Culebra. This CCDF is unlike the others in that releases are not calculated at the accessible environment, and therefore is not suitable for comparisons, preliminary or otherwise, with the Containment Requirements. The curve displays releases directly into the Culebra (with cuttings also included) from boreholes occurring at 1000 years, and therefore provides an estimate of total releases if subsurface transport to the accessible environment were instantaneous and complete. The curve shows repository performance estimated with contributions from only the natural barrier provided by the Salado Formation and the engineered barrier system. Instantaneous and complete transport in the Culebra is physically unrealistic, and this curve is displayed only for the purpose of comparison with the curve described in the previous paragraph, which was calculated using the single-porosity and constant λ models. The two cures are identical for most of their lengths. The differences between the curves are caused by radioactive decay during transport, and rapid transport in the single-porosity transport model in effect allows all sufficiently long-lived radionuclides that enter the Culebra to be released to the accessible environment within the 9000 years following intrusion.

The CCDF in Figure 1 labeled "Total, Dual Porosity + Cuttings, K_d=0, λ_0," represents an estimate of the performance of the disposal system if physical retardation by diffusion into the pore volume of the Culebra is included as a part of the natural barrier system. The area between the first and second CCDFs is a measure of the potential regulatory impact of including physical retardation. Similarly, the next CCDF in Figure 1, calculated using the dual-porosity, $K_d \neq 0$, and constant λ models, represents an estimate of the performance of the disposal system if both physical and chemical retardation in the Culebra are included in the natural barrier system. The location of this third curve is determined entirely by cuttings releases.

The final CCDF in Figure 1, calculated using the dual-porosity, $K_d \neq 0$, and time-dependent λ models, shows the effect of including expert judgment on the efficacy of passive markers in reducing the probability of human intrusion. This final CCDF, also determined entirely by cuttings releases, was calculated using what the WIPP Performance Assessment Department believes at this time to be the most realistic conceptual model for the disposal system, based on models and data available in 1992. As indicated previously, results are

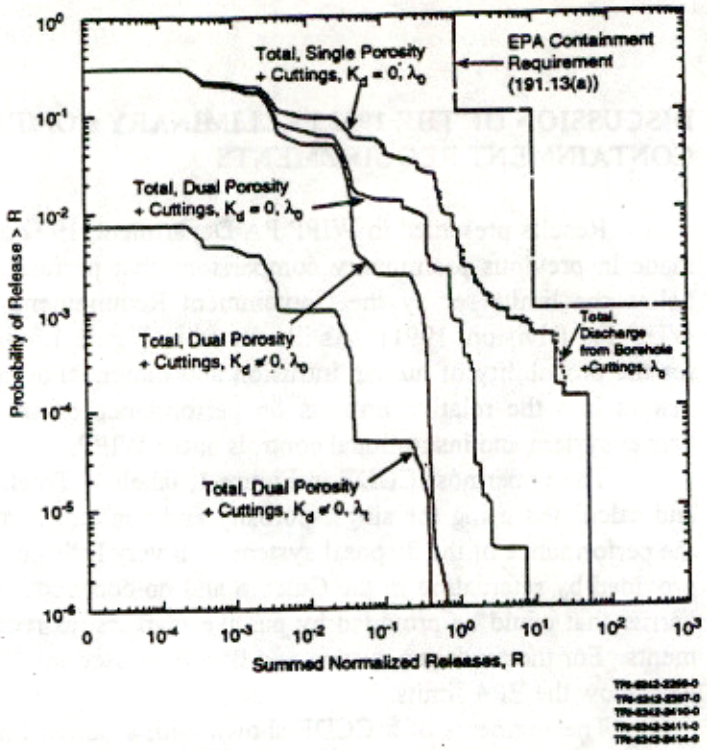


Figure 1. Comparison of mean CCDFs for total (cuttings plus subsurface) releases from intrusions occurring at 1000 year showing the impact of including specific components of the natural and institutional barrier systems. Both curves shown for $K_d=0$ are dominated completely by cuttings releases. Summed normalized releases are displayed using an inverse hyperbolic sine scale, which differs from a logarithmic scale only in the interval between 0 and 10^{-4}.

preliminary, and none of the curves shown in Figure 1 are believed sufficiently defensible for use in a final compliance evaluation.

GAS FLOW BEHAVIOR

Gas may flow in the anhydrite layers beyond the disposal-unit boundaries in some realizations. Significant volumes of gas (i.e., greater than one m^3) flow past the southern disposal-unit boundary in Marker Bed (MB) 139, anhydrite a + b, and in MB138, respectively. The maximum gas flow past a boundary occurs in MB138, with 1.7×10^6 m^3 of gas (at reference conditions). All gas is assumed to have the physical properties of hydrogen. Because the viscosity of hydrogen is lower than that of other gases likely to be present or produced in the waste (CO_2, CH_4, N_2), this assumption should result in greater and more extensive gas flows than if other gases were used. The cumulative gas flows up through the shaft seal are small compared with the flows out the anhydrite layers, where the maxima are more than an order of magnitude higher.

SAFETY ASSESSMENT

Comparisons of mean doses (50-year committed effective dose equivalents [CEDEs]) due to different hypothetical pathways resulted in a critical pathway comprised of an E1E2-type intrusion (Helton, 1994, these *Proceedings*), subsurface transport through the Culebra to a stock well, and then a stockpond-to-cow-to-human exposure

pathway for a typical local rancher. The maximum value for the 50-year CEDE for the critical pathway is 0.01 mrem.

A comparison of the risk of health effects can be made with International Commission on Radiological Protection (ICRP) recommendations by assuming a probability of 5×10^{-4} health effects per rem and a scenario probability of 10^{-2} (Bertram-Howery et al., 1990). Doses are summed over all radionuclides and all exposure pathways for releases from a stockpond. Risk is estimated to be less than 10^{-9}. Risk, in terms of health effects to a typical individual of the critical group for hypothetical WIPP pathways, is orders of magnitude less than the ICRP-recommended risk limit and other nations' target risk criteria for deep-geologic nuclear waste repositories.

REFERENCES

Bertram-Howery, S.G., M.G. Marietta, R.P. Rechard, P.N. Swift, D.R. Anderson, B.L. Baker, J.E. Bean, Jr., W. Beyeler, K.F. Brinster, R.V. Guzowski, J.C. Helton, R.D. McCurley, D.K. Rudeen, J.D. Schreiber, and P. Vaughn. 1990. *Preliminary Comparison with 40 CFR Part 191, Subpart B for the Waste Isolation Pilot Plant, December 1990.* SAND90-2347. Albuquerque, NM: Sandia National Laboratories.

EPA (Environmental Protection Agency). 1978. "40 CFR Parts 1500-1508: Regulations for Implementing the Procedural Provisions of the National Environmental Policy Act," as amended and published in the most recent *Code of Federal Regulations*. Washington DC: Office of the Federal Register, National Archives and Records Administration.

EPA (Environmental Protection Agency). 1985. "40 CFR Part 191: Environmental Standards for the Management and Disposal of Spent Nuclear Fuel, High-Level and Transuranic Radioactive Waates; Final Rule," *Federal Register*. Vol. 50, no. 182, 38066-38089.

EPA (Environmental Protection Agency). 1986. "40 CFR Part 268: Land Disposal Restrictions," as amended and published in the most recent *Code of Federal Regulations*. Washington DC: Office of the Federal Register, National Archives and Records Administration.

EPA (Environmental Protection Agency). 1990. "Conditional No-Migration Determination for the Department of Energy Waste Isolation Pilot Plant (WIPP)," *Federal Register*. Vol. 55, no. 133, 28397-28398.

EPA (Environmental Protection Agency). 1992. *"No Migration" Variances to the Hazardous Waste Land Disposal Prohibitions: A Guidance Manual for Petitioners, Draft, July 1991.* EPA/S30/R-92/03. Washington, DC: US Environmental Protection Agency, Office of Solid Waste.

Helton, J.C. 1993. "Risk, Uncertainty in Risk, and the EPA Release Limits for Radioactive Waste Disposal," *Nuclear Technology*. SAND91-1255J. Vol. 101, no. 1, 18-39.

Helton, J.C., J.W. Garner, R.D. McCurley, and D.K. Rudeen. 1991. *Sensitivity Analysis Techniqus and Results for Performance Assessment at the Waste Isolation Pilot Plant.* SAND90-7103. Albuquerque, NM: Sandia National Laboratories.

Helton, J.C., J.W. Garner, R.P. Rechard, D.K. Rudeen, and P.N. Swift. 1992. *Preliminary Comparison with 40 CFR 191, Subpart B for the Waste Isolation Pilot Plant, December 1991-Volume 4: Uncertainty and Sensitivity Analysis Results.* SAND91-0893/4. Albuquerque, NM: Sandia National Laboratories.

NEPA. 1970. *National Environmental Policy Act.* Public Law 91-190.

RCRA. 1976. *Resource, Conservation, and Recovery Act of 1976.* Public Law 94-580, 90 Stat. 2795.

US DOE (Department of Energy). 1979. *Draft Environmental Impact Statement, Management of Commercially Generated Radioactive Waste,* DOE/EIS-0046-D. Washington, DC: US Department of Energy.

US DOE (Department of Energy). 1980. *Final Environmental Impact Statement: Waste Isolation Pilot Plant.* DOE/EIS-0026. Washington, DC: US Department of Energy. Vols. 1-2.

US DOE (Department of Energy). 1990a. *Final Supplement Environmental Impact Statement, Waste Isolation Pilot Plant.* DOE/EIS-0026-FS. Washington, DC: US Department of Energy, Office of Environmental Restoration and Waste Management.

US DOE (Department of Energy). 1990b. *WIPP No Migration Variance Petition.* DOE/WIPP 89-003, Revision 1. Carlsbad, NM: Westinghouse Electric Corporation, Waste Isolation Division.

US DOE (Department of Energy). 1990c. *Draft Plan for the Waste Isolation Pilot Plant Test Phase: Performance Assessment and Operations Demonstration.* DOE/WIPP 89-011. Carlsbad, NM: US Department of Energy, Waste Isolation Pilot Plant.

WIPP LWA. 1992. *Waste Isolation Pilot Plant Land Withdrawal Act.* Public Law 102-579.

WIPP PA (Performance Assessment) Department. 1992. *Preliminary Performance Assessment for the Waste Isolation Pilot Plant, December 1992.* SAND92-0700. Albuquerque, NM: Sandia National Laboratories. Vols. 1-5.

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)

THE DYNAMIC FLOWGRAPH METHODOLOGY: A METHODOLOGY FOR ASSESSING EMBEDDED SYSTEM SOFTWARE SAFETY

Chris Garrett, Michael Yau, Sergio Guarro and George Apostolakis

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

INTRODUCTION

Embedded systems are systems in which the functions of mechanical and physical devices are controlled and managed by dedicated digital processors and computers. These latter devices, in turn, execute software routines (often of considerable complexity) to implement specific control functions and strategies. Embedded systems have gained a pervasive presence in all types of applications, from the defense and aerospace to the medical, manufacturing, and energy fields. The advantage of using embedded systems is that very sophisticated and complex logic can be executed by relatively inexpensive microprocessors loaded with the appropriate software instructions. The originally implemented logic can also be modified at any point in the life of the system it is designed to control by uploading new software instructions. Due to this flexibility, embedded systems are being used increasingly in a number of safety critical applications.

While the cost-effectiveness and flexibility of embedded systems are almost universally recognized and accepted, it is also increasingly recognized that the task of providing high assurance of the dependability and safety of embedded system software is becoming quite difficult to accomplish, due precisely to its very complex and flexible nature. Software, unlike hardware, is unique in that its only failure modes are the result of design flaws as opposed to any kind of physical mechanisms such as aging[1-3]. As a result, traditional safety assessment techniques, which have tended to focus upon physical component failures rather than system design faults, have been unable to close the widening gap between the extraordinarily powerful capabilities of modern software systems and the levels of reliability which we are capable of exacting from them.

The Dynamic Flowgraph Methodology (DFM) is a methodology for analyzing and testing embedded system software dependability[4]. It has two fundamental goals: 1) to identify how certain postulated events may occur in a system; and 2) to identify an appropriate testing strategy based on an analysis of system functional behavior. System models which express the logic of the system in terms of causal relationships between physical variables and temporal characteristics of the execution of software modules are analyzed to determine how a certain state (desirable or undesirable) can be reached. This

is done by developing timed fault trees which take the form of logical combinations of static trees relating the system parameters at different points in time. The resulting information concerning the hardware and software states that can lead to certain events of interest can then be used to identify those software execution paths and associated hardware and environmental conditions which are potentially capable of leading to serious failures in the implemented system. The verification effort can then be focused specifically on these safety critical features of the system to ensure that such failures cannot be realized. This paper illustrates DFM by applying it to the problem of modeling and analyzing the Titan II Space Launch Vehicle (SLV) Digital Flight Control System (DFCS).

BASIC FEATURES OF DFM

The application of DFM is a two-step process, as follows:

Step 1: Build a model of the embedded system being analyzed.

Step 2: Analyze the model to produce fault (or success) trees which relate the events, in both the physical system and the software, which can combine to cause system failures, including the time sequences in which they occur, and identify system failure (success) modes in the software and associated hardware as prime implicants of the timed fault (success) trees.

The first step consists of building a model that expresses the logical and dynamic behavior of the system in terms of its physical and software variables. The second step uses the model developed in the first step to build timed fault (or success) trees that identify logical combinations of hardware and software conditions that cause certain specific system states of interest, and the time sequences in which these conditions come about. These system states can be desirable or undesirable, depending on the objective of the analysis. This is accomplished by backtracking through the DFM model of the embedded system in a systematic, specified manner. The information contained in the fault trees concerning the hardware and software conditions that can lead to system states of interest can be used to uncover undesirable or unanticipated software/hardware interactions, thereby allowing improvement of the system design by eliminating unsafe software execution paths, and to guide functional testing to focus on a particular domain of inputs and system conditions.

DFM models take the form of directed graphs, with relations of causality and conditional switching actions represented by arcs that connect network nodes and special operators. The nodes represent important process variables and parameters, while the operators represent the different types of possible causal or sequential interactions among them. DFM's usefulness as a tool for the analysis of embedded systems derives from its direct and intuitive applicability to the modeling of causality driven processes. DFM models provide, with certain limitations, a complete representation of the way a system of interconnected and interacting components and parameters is supposed to work and how this working order can be compromised by failures and/or abnormal conditions and interactions.

The application of DFM to a simple hardware system is illustrated in Fig. 1, where a valve is used to control a downstream flowrate. In Fig. 1(a), a piping and instrumentation diagram (P&ID) is drawn to describe the functional layout of the system, its components, and other elements of basic engineering data regarding the process. Other important attributes, most notably the ones linked to operational logic and control modes as well as the analyst's own understanding of the system, while not directly contained nor implicitly expressed in the P&ID, are nevertheless represented in the DFM model of the system (Fig. 1(b)). The DFM model is built with physical parameters UP, F, FM, and VX as continuous variable nodes, where

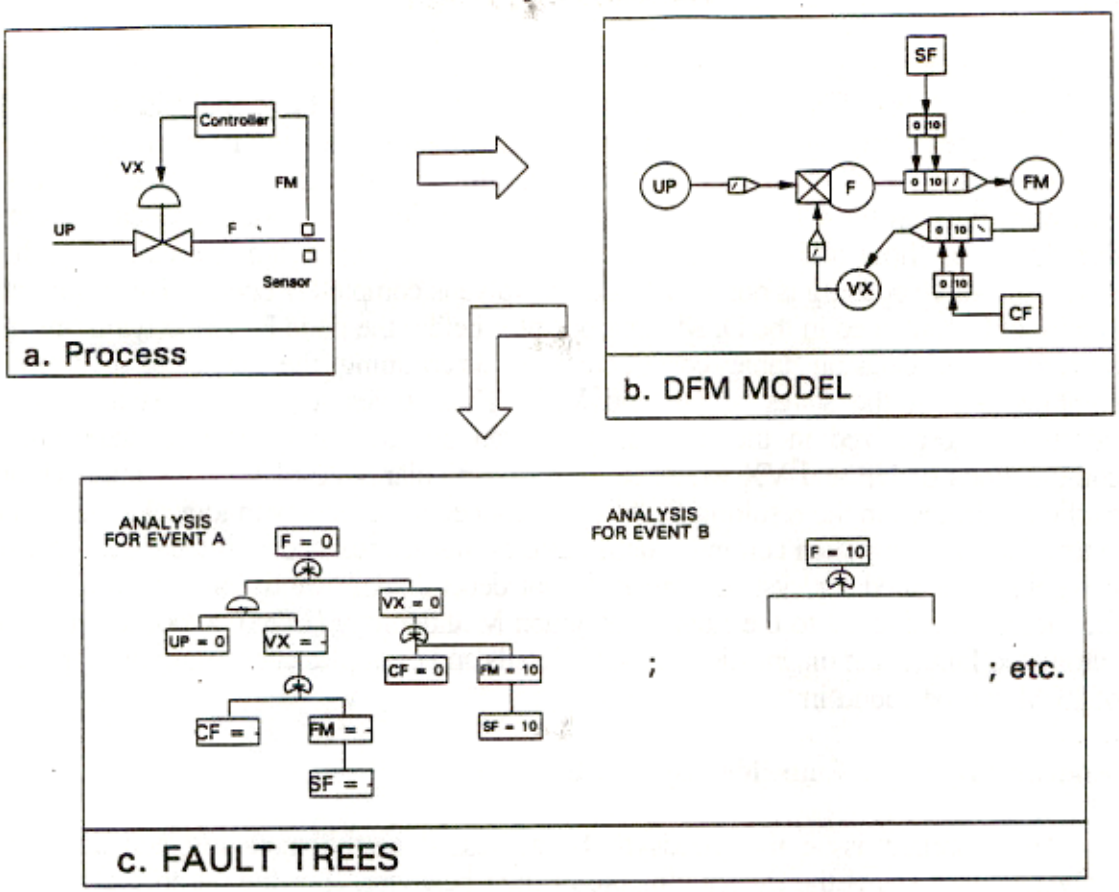


Figure 1. Illustration of DFM Modeling and Fault Analysis

UP = Upstream pressure,
F = Flow rate,
FM = Flow rate measure,
VX = Valve position at the present time,
and SF and CF as discrete variable nodes, where:
SF = Sensor state,
CF = Control Function.

The relationships between parameters are represented by gains in transfer boxes, which may be different for different conditions. Edges connect nodes through transfer boxes. An example of how relationships are represented in the DFM model is the direct proportionality relationship between nodes UP and F. This is represented by a "/" in the transfer box between the nodes. The two nodes are connected through the transfer box using directed edges (Fig. 1(b)). According to the different degraded states of the flowrate sensor, SF, (the sensor may fail high, fail low, etc.) the relationship between the nodes F and FM may change. This is clearly shown in the model (Fig. 1(b)).

It should be noted that the results of a DFM analysis are obtained in the form of fault trees, which show how the investigated system/process states may occur. DFM thus shares, in the form of the results it provides, many of the features of fault tree analysis. The difference, however, is that it provides a documented model of the system's behavior and interactions, which fault tree analysis does not provide nor document directly. The most important feature of this methodology is that it is possible to produce, from a single DFM system model, a comprehensive set of fault trees that may be of interest for a given system. This is a most useful feature since, once a DFM model has been developed, it is not necessary to perform separate model constructions for each system state of interest (as is

the case in fault tree analysis). Because DFM modeling focuses on parameters, rather than components, it also offers greater modeling flexibility than fault tree analysis, although this flexibility goes along with proportionately more complex modeling rules and syntax.

In Fig. 1(c), the fault tree for the top event, "flow rate is high," is derived. By working backward through the DFM model starting from the flow rate node F, we can determine that the state, "flow rate F is high," is caused by either "upstream pressure UP is high" AND "the valve opening is nominal," OR "the valve is completely open." This information is implicitly contained in the DFM input operator before the node F. Underlying this input operator is a decision table constructed by determining the states of F from the combinations of the states of UP and VX. Thus, given a particular state of F, the information organized in the decision table can be used in reverse to determine the combinations of UP and VX which cause this particular state of F. This information is explicitly denoted in the resulting fault tree by connecting events with logical AND and OR gates. Backtracking then continues until basic events are reached. To the extent to which it would be applied for systems which do not depend significantly on software, DFM is functionally equivalent to the Logic Flowgraph Methodology (LFM), a tool for computer-automated failure and diagnostic analysis. Details and examples concerning the application of LFM can be found in[5-6].

Modeling Dynamic Embedded System Behavior

An important issue that needs to be addressed in the modeling and analysis of embedded systems is the dynamic nature of their behavior. For the purpose of modeling such behavior and representing its effects in the system fault trees, the execution of software is modeled as a series of discrete state transitions within the DFM model. The usefulness of this approach is that it provides the ability to represent changes in the system logic at discrete points in time. This allows the development of fault trees which reflect static relationships between the variables at different points in time.

Embedded system software is generally real-time control software which receives real-time data from the physical part of the system and performs appropriate control actions on the basis of this data. The first step in modeling this type of software is to identify those portions of it which explicitly involve time dependencies such as interrupts and synchronization routines. The control flow among the above defined software "components" is then represented by a state transition network in which the execution of each particular software component is represented by a transition between states. Associated with each transition is a time which represents the execution time of the software routine to which it corresponds. The modeling of the data flow between the software components is completely analogous to the modeling of causality flow. Associated with each transition in the state transition network is a DFM transfer box which, instead of describing a one-to-one causal relationship between physical variables, describes, in general, several many-to-one mappings between the corresponding software component's inputs and outputs and any relevant global variables.

The state transition network is then incorporated into the DFM model of the hardware system. The principal step in the integration of the software and hardware portions of the model is the identification of all data that is exchanged between the software and the physical world, i.e., the identification of all of the software "images" of hardware parameters and physical variables. Corresponding parameters are then connected through a transfer box and an edge which indicates the direction of information flow. In almost all cases, an interface point is constituted either by a sensor that measures a physical parameter to be input to the software or an actuator which translates a software command into a physical movement. Thus, one has to include in the hardware portion of the model nodes representing both the measured physical parameter and the associated measurement, or the

software command and the actuator movement, respectively. The sensors and actuators themselves will be modeled as transfer functions normally representing direct proportionality but also containing conditional faulted mappings which represent different degraded states. The software portion of the model will begin with the measured value nodes which represent the images of physical parameters which are used as input to the software and end with the software commands which are output to the actuators. It is also important to note that, in addition to having a direct causal effect on the physical system via sensor measurements and actuator commands, software actions will, in general, also have an indirect effect on the physical system by conditionally changing the gains between physical variable nodes. This will occur whenever software controls the functions of physical devices such as pumps, valves, etc., and is modeled by edges connecting the relevant software variable nodes with the transfer boxes in question.

Fault trees are developed by an automated backtracking procedure which takes into account the timing effects introduced by the state transition network, resulting in trees which are time dependent. After a top event has been identified and translated in terms of the state(s) of one or more nodes of the system, backtracking proceeds until a transfer box is reached which is associated with a time transition (software module). Development of that branch of the tree is then suspended and the remaining branches are developed until they reach either a basic event or another time transition. The result is a fault tree for the system at time t_n. Then, from the state transition network, the transition is found which maps the system state from time t_n to time t_{n-1}, i.e., the last transition to have occurred. From that transition's transfer box, the input values associated with that transition at time t_{n-1} are found, and backtracking continues as before until, again, all branches end with either basic events or the outputs of other time transitions. This is the fault tree for time t_{n-1}. This process continues backward through successive transitions in the state transition network. The result is a series of linked, static fault trees which represent the state of the system at different times and which are linked through the inputs and outputs of time transitions (software module executions). The nature of the particular system dynamics being studied will provide heuristic rules for determining how far back in time one should go before halting the procedure.

MODELING THE TITAN II SLV DFCS WITH DFM

The DFM model of the Titan II SLV DFCS[7-8] is shown in Figure 2. In a DFM model, circles are nodes representing hardware or software parameters, boxes are DFM operators describing the relationships between the nodes, the solid arrows are causality edges indicating functional relationships, and dotted arrows are conditioning edges representing conditional relationships. The principal step in integrating the software and hardware portions of the model is the identification of all data that is exchanged between the software and the physical world. In the Titan II system, the software reads in the gimbal angle measurements α, β, γ, and γ_R, the accelerometer counts a_{um}, a_{vm}, and a_{wm}, and the pitch rate PR and yaw rate YR. The outputs are the thrust chamber deflection angles θ_P, θ_R, and θ_Y.

In Figure 2, transfer boxes A and F model the inertial measurement unit (IMU), which compares the initial and current orientations of the body axis, B_i and B_f, to generate the gimbal angle measurements α, β, γ, and γ_R, and also measures the accelerations a_{um}, a_{vm}, and a_{wm}. Transfer box D represents the gyros which measure the pitch rate PR and yaw rate YR. These sensor inputs are used by the flight control software to calculate the thruster deflections θ_P, θ_R, and θ_Y. Finally, transfer box C represents the rocket itself in which the body axes and the current acceleration depends on θ_P, θ_R, θ_Y, the thrust F, the rocket mass M, the moment of inertia I, and the center of mass CM. After linking up the

parameters by the transfer boxes and transition boxes, the next step is to construct decision tables to represent the relationships between the parameters and backtrack through the model to build fault trees. Decision tables representing the transfer boxes and transition boxes have been constructed and work is currently in progress to develop fault trees to investigate the dependability of the navigation and control functions during Stage I flight.

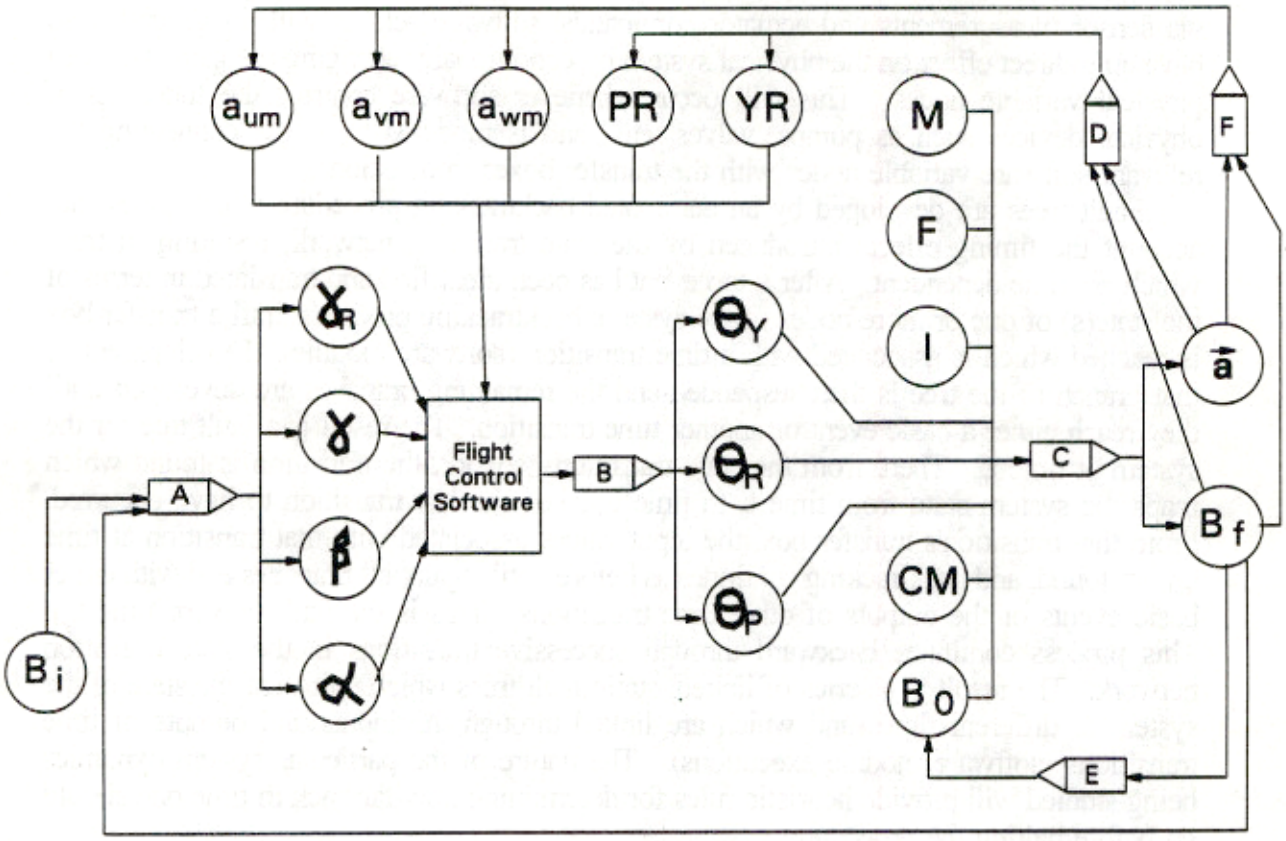


Figure 2. DFM Model of the Titan II Flight Control System

REFERENCES

1. J.A. McDermid, Issues in developing Software for Safety Critical Systems, *Reliability Engineering and System Safety*, Vol. 32, (1991).
2. S.B. Guarro, J.S. Wu, et al., Findings of a Workshop on Embedded System Software Reliability and Safety, UCLA-ENG 90-25, June 1990.
3. N.G. Leveson, P.R. Harvey, Analyzing Software Safety, *IEEE Transactions on Software Engineering* SE-9:569, (1983).
4. C.J. Garrett, S. B. Guarro, G. E. Apostolakis, Development of a Methodology for Assessing the Safety of Embedded Systems, 2nd Annual AIAA/USRA/AHS/ASEE/ISPA Aerospace Design Conference, Irvine CA, February 16-19, 1993.
5. S.B. Guarro, D. Okrent, The Logic Flowgraph: A New Approach to Process Failure Modeling and Diagnosis for Disturbance Analysis Applications, *Nuclear Technology* 67:348, (1984).
6. S.B. Guarro, J.S. Wu, et al., Embedded System Reliability and Safety Analysis in the UCLA ESSAE Project, Proc. of the Intnl. Conf. on Probabilistic Safety Assessment and Management (PSAM), Beverly Hills, CA, Feb. 4-7, 1991.
7. Martin Marietta Astronautics, "Guidance, Control, and Ground Equations for Flight Plan XX Volume I: Guidance Equations XX-U001-I-05," February 18, 1991.
8. Martin Marietta Astronautics, "Guidance, Control, and Ground Equations for Flight Plan XX Volume II: Flight Control Equations XX-T001-II-08," June 24, 1988.

DETERMINING THE PRIME IMPLICANTS FOR MULTI-STATE EMBEDDED SYSTEMS

E. J. Shields, G. E. Apostolakis, S. B. Guarro

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

INTRODUCTION

Binary logic, where the two values describe the event space, e.g. operating-failed, safe-unsafe, might not be sufficient for an adequate representation of the performance of a system, and its components. Situations occur where engineered systems are characterized by degrees of complexity, such that the failure or degeneration of some components does not completely prevent systems from accomplishing their missions. Or the performance of engineered systems and their parts might be suitably expressed by means of several values (i.e. multi-state) that allow for a more accurate representation of the system's physical variables (e.g. pressure, temperature, voltage, etc.) Nuclear and chemical plants, aircraft, and spacecraft, are examples of systems in these classes. It is precisely these types of system that inspired the Dynamic Flowgraph Methodology (DFM) currently under development at UCLA to analyze embedded software systems.[1]

Embedded systems are systems in which the functions of mechanical and physical devices are controlled and managed by dedicated digital processors and computers. These latter devices, in turn, execute software routines to implement specific control functions and strategies. The advantage of using embedded systems is in the almost unlimited flexibility provided by the software implementation of system control functions and by the computational power and speed of modern microprocessors.

One important issue that needs to be addressed in the modeling and analysis of embedded systems is the dynamic nature of their behavior. The DFM approach consists of a modeling and analysis environment in which LFM[2] structures are used to model the relationships between the various software and hardware variables of a system, while the execution of software is modeled as a series of discrete points in time. This allows the development of "timed" fault trees which reflect static relationships between variables at different points in time. This ability will enable an analyst to produce fault trees for an embedded system that would describe and illustrate how any kind of unsafe conditions or events may occur in the system as a whole, due to software faults, hardware faults or

combinations of the two. Systems which contain other than simple fault modes connected by AND-OR gates, i.e. EOR gates, multiple states, etc., are non-coherent and their unique failure modes cannot be determined by methods used on binary fault trees. Given the logic function representing a system's failure modes, Φ, where ϕ and φ are fundamental formulas (literals and conjunction of literals, containing no variable twice) of Φ, ϕ will be said to subsume φ if and only if all the literals whereof φ is a conjunction are among the literals whereof ϕ is a conjunction. We call ϕ a prime implicant of a formula Φ if ϕ implies Φ and subsumes no shorter formula which implies Φ.[3] It will be the focus of this paper to describe a method for determining the all prime implicants of multi-state "timed" fault trees.

TIMED FAULT TREES

One approach currently under evaluation is to represent the "timed" fault trees in the form of decision tables. A timed fault tree takes on the form of a combination of timed-stamped pieces of conventional static fault trees which describe system parameter states at different time steps. It is a series of snap shots of the system evolution, with each snapshot presented as a piece of a static fault tree with all significant time transitions explicitly identified within the logic structure of the tree, so the existence of certain logic relations among system states across time boundaries are identified. In conventional fault trees, only the probabilities of occurrence of events may exhibit time dependence. In timed fault trees, the logical structure of the tree may be time dependent. The most commonly derived results from fault trees are the minimal cut-sets for the top event. Each minimal cut-set is a complete set of the minimum necessary and sufficient combinations of hardware and software state(s) that can potentially cause the top event. However, because DFM uses a multi-state representation of variables, special methods are required to derive the system's prime implicants.

After the fault trees have been constructed, the sets of primary events which lead to the top event can be obtained. These sets of primary events are converted to tabular form by constructing "timed" decision tables. Each component of the system is modeled by a decision table. The decision table describes how each combination of input events specifies the output events, i.e. the state of the output. After some modification for use with multi-state variables, these decision tables can then be simplified via basic Boolean operations that are used for simplifying truth tables. These rules used in conjunction with the application of Quine's consensus theory can be used to reduce a decision table to its prime implicants, which will be used to calculate the systems top event probabilities. [4]

ILLUSTRATIVE EXAMPLE

The above concepts are best illustrated through a simple example. Consider a system having the DFM model shown in Figure 1 below. This model along with the decision tables that describe input-output relationships of the variables are needed for the analysis of a system failure or top event.

Variables A and F are outputs of transfer boxes where the relationship between the input and the output nodes is defined by a decision table and assumed to exist in the same time frame. The variables D and E are the outputs of transition boxes. The difference between transition and transfer boxes is that in transition boxes a time lag occurs between the time when inputs become true and the time when the output states are reached. In this example the time delay is 10 time units for both transition boxes 1 and 2. The balance of

the variables, B, C, G, and H, are basic events or process variable nodes that represent physical and software condition in the system, i.e. temperature, pressure, valve position, etc.

The goal is to develop a decision table that contains only the prime implicants for the given top event. A prime implicant table is developed by an automated backtracking procedure which takes into account the timing effects introduced by the transition boxes,

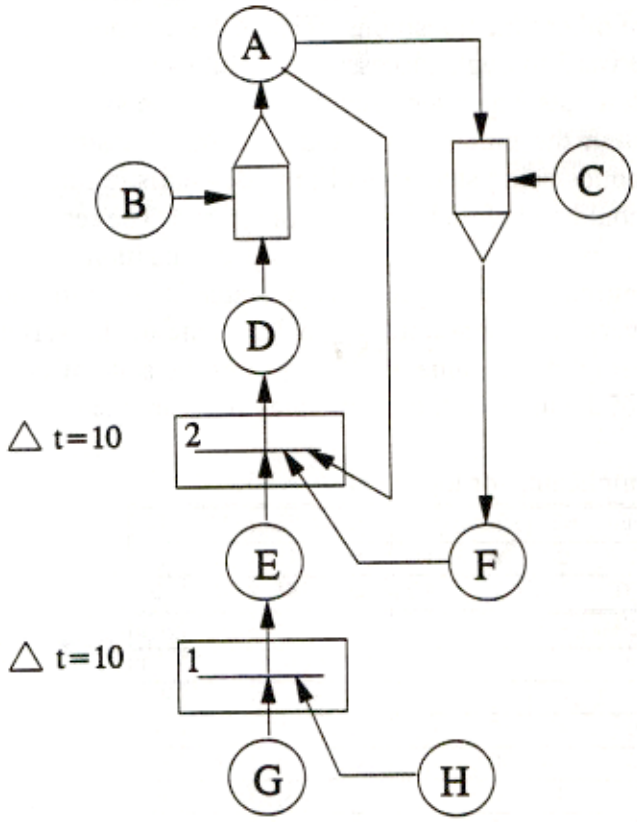


Figure 1. DFM Model.

resulting in decision tables which are time dependent. For this example the top event will be A = +1. A possible decision table definition for the variable A is given in Table 1. The output of the other transfer and transition variables would be defined in a similar manner.

Table 1. Decision table for transfer variable A.

BE B	T2 D	TF A
-1	-1	-1
0	-1	-1
+1	-1	-1
-1	0	-1
0	0	0
+1	0	+1
-1	+1	+1
0	+1	+1
+1	+1	+1

After a top event has been identified and translated in terms of the state(s) of one or more nodes of the system, backtracking proceeds until a transition box is reached. Development of the decision table is then suspended and the remaining inputs are developed until they reach either a basic event or another transition box. The result is a decision table for the system at time t_n. Then, from the DFM model, the transition is found which maps the system state from time t_n to time t_{n-1}, i.e., the last transition to have occurred. From that transition, the input values associated with that transition at time t_{n-1} are found, and backtracking continues as before until, again, all inputs are either basic events or the outputs of other time transitions. This is the decision table for time t_{n-1}. This process continues backward through successive transitions in the DFM model. The result is a decision table with inputs which represent the state of the system at different times and which are linked through the inputs and outputs of time transitions. The nature of the particular system dynamics being studied will provide heuristic rules for determining how far back in time one should go before halting the procedure. The resulting table will contain only values of process variables and any undeveloped transition variables along with the time at which they occurred. An example of such a table is given in Table 2. The top row describes the type of variable, the second row is the name of the variable, the third is the time the input is occurring, e.g. a value of -10 indicates the state of the input 10 time units before the occurrence of the top event, the remaining rows are the states of the given inputs.

Table 2. Prime implicants for top event A = +1.

BE	BE	BE	BE	BE	BE	BE	BE	BE	T2	TE
B	**B**	**B**	**C**	**C**	**G**	**G**	**H**	**H**	**D**	**A**
0	-10	-30	-10	-30	-20	-40	-20	-40	-30	0
+1	-	-	0	-	0	-	0	-	-	+1
-	-	-	-	-	+1	-	-	-	-	+1
-	-	-	-	-	-	-	+1	-	-	+1
-	-	-	0	-	0	-	0	-1	-	+1
-	-	-	0	-	0	-	0	-	-	+1
-	-	-	0	-1	0	-	0	-	-	+1
-	-	+1	0	-	0	-	0	-	-	+1
-	-	-	0	-	0	-	0	-	+1	+1
-	-1	-	0	-	0	-	0	-	-	+1
-	-	-	+1	-	0	-1	0	-1	-	+1
-	-	-	+1	-	0	0	0	-1	-	+1
-	-	-	+1	-	0	-1	0	0	-	+1
-	-	-	+1	-1	0	0	0	0	-	+1
-	-	+1	+1	+1	0	0	0	0	0	+1
-	-	-	+1	+1	0	0	0	0	+1	+1
-	-1	0	+1	0	0	0	0	0	0	+1
-	0	0	+1	0	0	0	0	0	0	+1
-	+1	-	0	-	0	-	0	-	-	+1
-	-	-	0	-	0	+1	0	-	-	+1
-	-	-	0	-	0	-	0	+1	-	+1
-	-	-	0	-	0	-	0	-	-1	+1
-	-	-1	0	-	0	-	0	-	-	+1
-	-	-	0	+1	0	-	0	-	-	+1

Consistency checking must also be employed to ensure that each event in the decision table is consistent with the events that appear before it. Events which violate logical and physical constraints imposed by the system must be removed from the table. Consistency checking for events occurring at the same time are well established, e.g. a variable cannot take two different values at the same time. However, because the decision

tables developed in this methodology contain information about the system at different points in time, it is necessary to perform consistency checks against the dynamic relationships between the variables. For example, in Table 2 if the input H represented the state of a valve, i.e. -1 - failed low, 0 - normal, and +1 - failed high, if we assumed the system cannot correct itself, rows 7, 14, and 23 would be removed because the indicate the change from a failed state to a normal state, e.g. -1 to 0 or +1 to 0. The decision table is then further simplified with the remaining rows representing the system's prime implicants.

The computer code to achieve the results outlined above is currently under development at UCLA. This code is a modified version of the PITE (Prime Implicants of Top Event) software.[5]

REFERENCES

1. C.J. Garrett, S.B. Guarro, G.E. Apostolakis, The Dynamic Flowgraph Methodology: A Methodology for Assessing the Dependabililty of Embedded software Systems, UCLA-ENG 42-93, June 1993.
2. C.T. Muthukumar, S.B. Guarro, G.E. Apostolakis, Logic Flowgragh Methodology: A Tool for Modeling Embedded Systems, IEEE/AIAA Digital Avionics Systems Conference, Los Angeles, CA Oct. 14-17, 1991
3. W. V. Quine, The Problem of Simplifying Truth Functions, Amer. Math. Monthly, 62:627(1955)
4. E. J. Henley, H. Kumamoto, "Probabilistic Risk Assessment: Reliability Engineering, Design, and Analysis", IEEE Press, New York (1992).
5. I. E. Ogunbiyi, Application of Decision Tables to Risk Analysis Studies, University of Houston, Sept. 1979.

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)

AN APPLICATION OF ISPA: SENSITIVITY ANALYSIS OF A COMPLEX ENGINEERING PROBLEM

Patrick R. McClure, Steven D. Clement, and Scott G. Ashbaugh

Science Applications International Corporation
Integrated Systems Performance Assessment Division
Albuquerque, NM 87106

ABSTRACT

Integrated System Performance Assessment (ISPA), a knowledge-based analysis technique, is used to perform a sensitivity analysis for a simple system. ISPA uses an event tree structure that allows the analyst to express his knowledge about the system probabilistically and provides a method for the treatment of inter-dependencies between system components.

INTRODUCTION

An analytical model may be used in design optimization or performance assessment of an engineered system. A system typically consists of several components, whose collective performance determines the overall system performance. System components can be defined as being one of two types:

- Independent components, whose performance are not affected by other system components or outside influences, and
- Dependent components, whose performance are tied directly to the performance of other system components or are influenced by factors external to the system.

The modeling of each system component may be complicated by its performance range, if large, or by uncertainties in the way in which external factors influence its performance. Component performance may be defined through empirical data or theoretical algorithms, or, if knowledge is incomplete, may be probabilistically characterized based on those component attributes that are known, while varying unknown attributes in a statistical fashion.

To analyze the affect of changing controllable component attributes and the range of system performance response to uncertain parameters, the engineer classically performs a

sensitivity analysis. The sensitivity analysis is historically performed using one of several generic methods. The most common methods are as follows:

- A mono-variate technique, in which parameters affecting system component performance are varied one at a time, and the effect on the system is measured; and
- A multi-variate technique, in which parameters affecting system component performance are varied simultaneously, and the effect on overall system performance caused by the variations in a single component is evaluated using a statistical method.

These sensitivity analysis techniques have disadvantages, which make them insufficient for a complete performance analysis of an engineered system. The mono-variate technique, while easy to use, will not provide insight into the interdependencies that may exist among system components. The multi-variate technique may provide some insight into component interdependicies, but does not provide a direct method for dealing with dependent components. In addition, results of the multi-variate technique may be difficult to interpret, and the method is sometimes difficult to use with complex systems.

This paper describes an innovative, knowledge-based analysis technique that facilitates performance assessment of complex engineered systems. This technique, known as Integrated System Performance Assessment, (ISPA)[1], applies a probabilistic modeling framework to the overall performance.

INTEGRATED SYSTEM PERFORMANCE ASSESSMENT

ISPA modeling begins by characterizing the system performance in terms of performance criteria. The analyst then develops causal relationship between these performance criteria and the system component attributes through both inductive and deductive reasoning. Specifically, the analyst indicates, using an event tree structure, the combinations of component performance required to attain a certain system performance goal. The structure of the tree indicates the causal relationships that the analyst believes exist. Because the event tree modeling framework is probabilistic, the analyst can indicate, within the context of the model, his or her confidence that a particular causal relationship is accurate. Multiple relationships with varying levels of confidence can be indicated if the analyst identifies more than one potential cause-effect relationship between any system component and any other component or one of the performance criteria. Because the level of confidence is specified, an uncertainty analysis can also be performed.

ISPA assists the analyst by identifying the relative importance of various system components to overall system performance. Because the ISPA approach takes performance information from individual system components, aggregates the data, and evaluates overall system performance, the model provides the analyst with the ability to conduct trade-off studies and "what-if" analyses by simulating numerous variations in system component attributes.

ISPA allows the integration of stand-alone computer models within a knowledge-based framework. This facilitates the use of computer modeling to predict component or overall system response for any one set of specified component attributes, while using the knowledge-based approach to analyze system performance over a wide range of component attributes. This approach allows the analyst to deduce the optimum set of component attributes to satisfy the established performance criteria, while also allowing the analyst to vary boundary conditions in case the system environment is uncertain.

DEMONSTRATION OF THE TECHNIQUE

The ISPA approach to performing sensitivity analysis is demonstrated by determining the relative importance of components in a simple system. The system to be analyzed is a thin walled aluminum cylinder capped at the bottom by concrete and submerged in water.

The object of the assessment is to determine if molten metal poured into the cylinder melts through the thin wall (melting temperature is 933 K) or cools inside the cylinder. The performance criteria for this system is the coolability or non-coolability of the molten metal, where a coolable system is defined as one in which the cylinder wall does not melt.

The analytical model selected to represent the system uses a transient two-dimensional finite-difference heat conduction model. The model contains correlations for natural convection, nucleate, transition and film boiling on the radial boundary of the cylinder. Melting and freezing of the materials is calculated at each node in the system. The pour rate of molten metal is used to calculate the height of material within the cylinder at each time step.

The analytical model is coded into FORTRAN for use with the event tree software used in the ISPA methodology. The nodalization selected to represent the cylinder is shown in Figure 1. Temperatures throughout the system are tracked for 40 seconds.

The initial and boundary conditions of the system are uncertain and the sensitivity of the system to these conditions is to be assessed. The independent components are as follows:

- The degree of sub-cooling of the water outside the cylinder: This value ranges from 0 to 50 degrees Celsius (Saturation is 373 K).
- The temperature of the relocating metal: The metal temperature ranges from 1500 to 2000 K. The melting temperature of the metal is assumed to be 1500 K.

The dependent component for this system is the pour rate of the metal into the cylinder, which is a function of the temperature of the relocating metal. This functional relationship is as follows:

- A high temperature (defined as 2000 K) produces a maximum pour of 0.2 kg/s.
- A medium temperature (defined as 1700 K) has an equal probability of producing a 0.1 kg/s or 0.2 kg/s pour rate.
- A low temperature (defined as 1500 K) has an equal probability of producing a 0.05 kg/s or 0.1 kg/s pour rate.

This simple distribution is selected only to demonstrate the technique. The ISPA methodology is suitable for analyzing significantly more complex problems in which a "family" of distributions for dependent components may exist.

ANALYSIS OF RESULTS

The system components and their dependencies are defined in an event tree format, shown schematically in Figure 2. Each branch of the tree defines a different set of initial and boundary conditions. While defining these conditions, the logic model considers their interdependicies and the level of confidence (as described by the analyst) that each is indeed correct. The tree serves as the driver that calls the system model for each combination of initial and boundary conditions. For this example, coolability of the metal in the cylinder is the performance criteria.

The results of the analysis are shown graphically in Figure 2. Looking at the various paths and outcomes shown in Figure 2, the analyst can observe the combinations of events

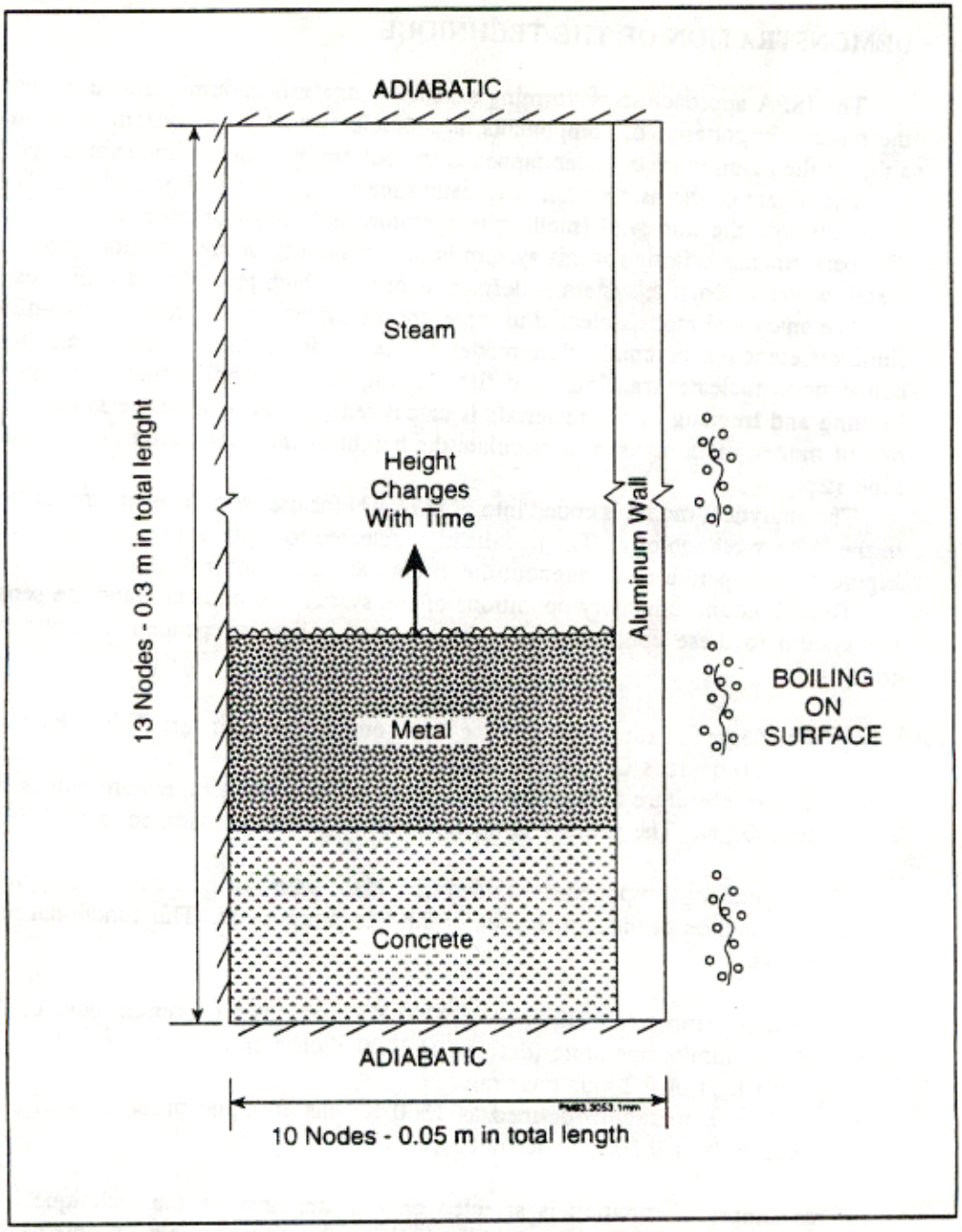


Figure 1. Schematic of Demonstration System (Aluminum Cylinder in Water).

that meet the performance criteria. Figure 2 indicates that a metal temperature of 1500 K, in combination with all values of sub-cooling and pour rate, meets the performance criteria.

In addition, the distribution of coolable and non-coolable results are shown in Table I for each component. The results show that sub-cooling of the water does not favor either state, coolability or non-coolability. By contrast, the temperature of the metal clearly indicates that a low temperature of 1500 K is coolable, while the higher temperatures of 1700 and 2000 K are non-coolable for all but one low probability case. The pour rate, a function of metal temperature, is coolable only for pour rates of 0.1 and 0.05 kg/s. The low pour rates are only possible for a metal temperature of 1500 K. Therefore, the results indicate that the most important component in determining coolability for this system is the metal temperature.

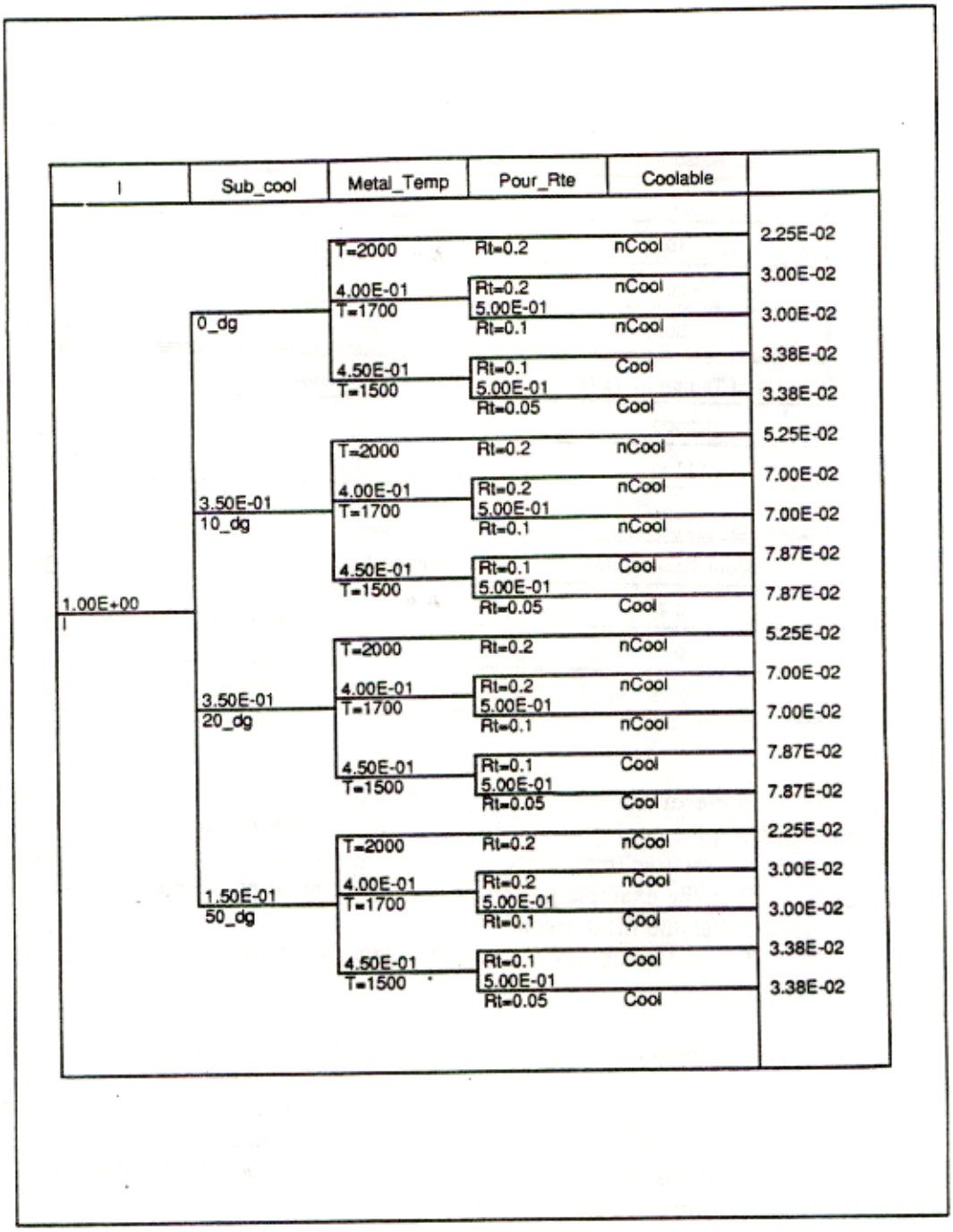


Figure 2. Main Event Tree.

SUMMARY AND CONCLUSIONS

IPSA is a knowledge-based analysis technique that facilitates performance assessment of complex engineering systems. These systems can be comprised of independent or dependent components, whose collective performance determines the overall performance of the system. The technique applies a probabilistic modeling framework to the overall performance assessment of a system. The technique can be used in the design optimization or sensitivity analysis of a system.

Table 1. Tabulation of Results.

Degree Sub-cooling	Fraction Coolable	Fraction Non-Coolable
0	0.068	0.083
10	0.157	0.192
20	0.157	0.192
50	0.098	0.053
Metal Temperature (K)	**Fraction Coolable**	**Fraction Non-Coolable**
2000	0.000	0.150
1700	0.030	0.370
1500	0.450	0.000
Pour Rate (kg/s)	**Fraction Coolable**	**Fraction Non-Coolable**
0.2	0.000	0.350
0.1	0.255	0.170
0.05	0.225	0.000

An example of the ISPA technique was performed for the sensitivity analysis of a simple system, the coolability of molten metal in an aluminum cylinder. Using the ISPA technique, the relative importance of the parameters in affecting system performance was identified. For the example presented, the temperature of the metal entering the cylinder was identified as the most crucial parameter.

The IPSA technique has several advantages over traditional methods of performing sensitivity studies:

- The technique provides an integrated and systematic method of performing the analysis.
- The modeling framework is probabilistic, allowing the analyst to express his confidence that a particular causal relationship is accurate.
- ISPA allows for dependent and independent components to be analyzed eliminating the potential for inconsistencies.
- Statistical methods such as Monte Carlo and Latin-Hypercube sampling in conjunction with regression analysis can still be used in the ISPA technique.

REFERENCES

1. C.N. Amos and S.D. Clement, "Integrated System Performance Assessment", Proceedings of PSAM II, San Diego, CA, March 20-24, 1994.

PRACTICAL PROBLEMS IN AGGREGATING EXPERT OPINIONS

Jane M. Booker, Richard R. Picard, Mary A. Meyer

Statistics Group
Los Alamos National Laboratory
Los Alamos, NM 87545

INTRODUCTION

Expert opinion is data given by a qualified person in response to a technical question. Thus it is an important part of many risk, reliability and safety studies. In these analyses, expert opinion provides information where other data are either sparse or non-existent. Improvements in forecasting result from the advantageous addition of expert opinion to observed data in many areas, such as meteorology and econometrics. More generally, analyses of large, complex systems often involve experts on various components of the system supplying input to a decision process; applications include such wide-ranging areas as nuclear reactor safety, management science, and seismology. Recent developments in aggregation place increased reliance on computers and modeling, including knowledge acquisition and the development of automated expert systems, such as for medical diagnoses.

For large or complex applications, no single expert may be knowledgeable enough about the entire application. In other applications, decision makers may find it comforting that a consensus or aggregation of opinions is usually better than a single opinion. Many risk and reliability studies require a single estimate for modeling, analysis, reporting, and decision making purposes. Aggregation methods also provide measures of dispersion accompanying that single estimate. For applications with large uncertainties, the strategy of combining as diverse a set of experts as possible helps characterize that uncertainty.

Decision makers are frequently faced with the task of selecting the experts and combining their opinions. However, the aggregation is often the responsibility of an analyst. Whether the decision maker or the analyst does the aggregation, the input for it, such as providing weights for experts or estimating other parameters, is imperfect owing to a lack of omniscience. This is only one of many difficulties associated with aggregation.

Aggregation methods for expert opinions have existed for over thirty years; yet many of the difficulties with their use remain unresolved. Major problem areas are summarized in the sections that follow: sensitivities of results to assumptions (in the data and the methods), weights for experts, correlation of experts, and handling uncertainties. The purpose of this paper is to discuss the sources of these problems and describe their effects on aggregation.

FORMALIZING THE AGGREGATION

Numerous models have been put forth to describe elicited expert opinions (Meyer and Booker, 1991). Consider, for illustration, a simple problem treated by Lindley and Singpurwalla (1986). Interest lies in a single unknown parameter, θ, denoting the log failure rate of a system component under some hypothesized operating conditions. A set

of k experts is consulted by a decision maker to provide information regarding θ. The i^{th} expert offers the opinion that θ is normally distributed with mean m_i and standard deviation s_i. It is now up to the decision maker to evaluate these opinions and obtain a single aggregated opinion regarding the component.

The decision maker may believe that the experts' stated opinions should be adjusted to reflect the effects of the factors affecting their stated opinions. Opinions are affected by factors such as the experts' personal biases, resulting from any conflict of interest, political concerns, or frame of mind. In addition, opinions are also affected by the manner in which the opinion is elicited such as question phrasing and response mode. Suppose the decision maker believes that the experts' estimates are distorted by the shift parameter, α_i , and a scale parameter, β_i such that:

$$m_i = \alpha_i + \beta_i \theta . \tag{1}$$

Note that $\alpha_i = 0$ and $\beta_i = 1$ correspond to the special case of accepting opinions at face value. Further suppose the decision maker feels that the i^{th} expert's stated standard deviation, s_i, differs from its actual counterpart u_i by the factor γ_i , i.e.,

$$u_i = \gamma_i s_i . \tag{2}$$

Specification of $\gamma_i > 1$, for example, allows the decision maker to inflate the i^{th} expert's stated uncertainty to compensate for the tendency of experts to exaggerate the extent of their knowledge (Capen, 1975).

Correlation among experts is almost always observed in real applications. Decision makers who surround themselves with "yes men" have severe problems in this regard. Correlation between the experts can stem from social pressures to conform (Janis, 1972) or from similarities in the experts' problem-solving processes (Booker and Meyer, 1988). Denote ρ_{ij} as the correlation between m_i and m_j given $\mathbf{s} = (s_1, s_2, ..., s_k)^T$ and θ.

At this point, the joint distribution of stated opinions $\mathbf{m} = (m_1, m_2 , ..., m_k)^T$ and $\mathbf{s}$ depends on underlying parameters $\{ \alpha_i , \beta_i , \gamma_i , \rho_{ij} \}$. Once the distribution of $(\mathbf{m},\mathbf{s})$ given θ is specified and combined with the decision maker's prior for θ, it is straightforward to obtain the decision maker's posterior for θ given the "data" $(\mathbf{m},\mathbf{s})$, not unlike a multivariate Bayesian calibration.

One strength of the Lindley-Singpurwalla (LS) approach is that it allows for explicit incorporation of parameters that are crucial to the decision maker's interpretation of the experts' input. Lacking any incorporation, the decision maker would have no direct way to compensate for factors that distort stated opinions. At the same time, however, specification of the parameter values $\{ \alpha_i , \beta_i , \gamma_i , \rho_{ij} \}$ in practice is acknowledged to be "an enormous task" (Lindley and Singpurwalla, 1986).

The original LS aggregation incorporated the following assumptions relevant to certain applications: 1) the decision maker's prior for θ is constant, 2) the distribution of $\mathbf{s}$ given θ does not depend on θ, and 3) the distribution of $\mathbf{m}$ given $(\mathbf{s},\theta)$ is multivariate normal with mean $\alpha + \beta \theta$ and covariance matrix Σ with elements $\rho_{ij}\gamma_i s_i \gamma_j s_j$. Under these conditions, the decision maker's posterior for θ is normal with mean

$$\mu = \beta^T \Sigma^{-1} (\mathbf{m} - \alpha) / \beta^T \Sigma^{-1} \beta \tag{3}$$

and standard deviation

$$\sigma = [\beta^T \Sigma^{-1} \beta]^{-1/2} \tag{4}$$

where $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k)^T$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_k)^T$.

There are many possible deviations from these assumptions: the decision maker's prior may not be flat, the experts may not provide normally distributed opinions, the modeling of $(\mathbf{m},\mathbf{s})$ in terms of underlying parameters may be more complex than described, and so on. In addition, the decision maker's estimates of the parameter values $\{ \alpha_i , \beta_i , \gamma_i , \rho_{ij} \}$, even when based on a modest amount of data, can still result in poor coverages of θ

from intervals derived from Equations (3) and (4). For example, over the distribution of (m,s) the portion of 95% intervals ($\mu \pm 1.96\sigma$) containing θ will be much less than 95%.

The sections below discuss these and other problems relating the aggregation of expert opinions.

PROBLEMS WITH METHOD ASSUMPTIONS AND THE DATA

In the usual case of gathering data for statistical analysis, basic rules are necessary to obtain a proper data for use in most methods. Sample points are assumed independently drawn from a population in such a manner (usually at random) so as to properly represent that population. Such a sample is described as a set of independently identically distributed (iid) values. The opinions from a set of experts may be neither independent nor identically distributed. The independence issue is further discussed in the correlation section. Many times there are very few experts available for sampling and the decision maker who selects them may deliberately choose experts for reasons (biases) of his own. This can make the sample a poor representation of the population. To obtain a reasonable sample and avoid any misrepresentation of the population, the decision maker should use a standard sampling method, such as simple random sampling or stratified random sampling, to select experts from the population.

Assuming the experts themselves represent the population of opinions possible, their estimates are affected by many factors such as how the elicitation was performed, the experts' and the elicitor's personal biases, and the experts' problem solving processes (especially for complex problems). Careful controls can reduce some of the elicitation effects influencing expert opinions, but their effectiveness has only been marginally studied (Meyer and Booker, 1991). For instance, if the experts were given a loosely formulated question, they might interpret it in differing ways, using varying assumptions or boundary conditions. Thus, they might be answering essentially different questions. Pilot testing of the questions for clarity and completeness is one way to reduce this problem; probing the experts for information on their assumptions, boundary conditions, definitions of terms, and problem-solving methods provides a second check.

Another sampling problem in using expert opinion is shared with other data gathering in reliability and risk analysis applications. In many applications, data is often extremely sparse, difficult to procure, or very costly to obtain. Methods designed for applications with large samples may suffer in performance when the sample is a small number of experts, not to mention only one expert. While small sample size methods, such as bootstrapping, are available in the statistical literature for some applications, their applicability for expert opinion applications would be very difficult to determine because it is difficult to find cases where large samples are possible. One mitigating tactic is to plan on gathering the opinions of the largest number of experts possible given the time and monetary constraints.

Aggregation methods (e.g., LS) may place further restrictions on the data such as requiring that it be normally distributed (Genest and Zidek, 1986). Robustness studies of certain statistical methods (such as regression) have often indicated that departures from normality, if not too severe, have little impact on the results. Perhaps this holds true for aggregation methods as well; however, no verification is currently available. In most cases, the data can be tested (e.g., tested for normality) to determine if the assumptions required are violated.

Many aggregation methods either assume that the experts are well calibrated or allow for calibrating them (such as in the LS method, through the estimates of the parameters $\{\alpha_i, \beta_i, \gamma_i\}$). In general, calibration focuses on the problem of how well the experts know their subject matter. Studies have indicated that experts cannot be well calibrated except in high-feedback situations such as blue-chip stocks and weather forecasting (Hogarth, 1975), but are lacking in determining the effects of using uncalibrated experts when calibrated experts are required. Until such results are available, decision makers should remain aware that in calibrating experts, they influence the aggregation through their adjustments. The decision maker's attempts to calibrate experts through the estimation of parameters can cause difficulties as described in the next section.

PROBLEMS WITH ESTIMATING PARAMETERS

Most aggregation methods rely on combining expert opinions through some type of weighting scheme. Thus, they require parameter estimation, usually in the form of estimating the weights for the experts. Some even suggest that the decision maker weight his own information in combination with that of his experts, as is done in the LS approach through incorporation of the decision maker's prior.

The LS method requires the decision maker to estimate parameters $\{\alpha_i, \beta_i, \gamma_i, \rho_{ij}\}$ for each expert — mean shift, mean scaling, standard deviation scaling parameters and inter-expert correlations. Apart from the mean shift term in Equation (3), the parameter estimates combine in much the same manner as a simplified weighting aggregation with the form:

$$\mu = \Sigma w_i m_i / \Sigma w_i \quad . \tag{5}$$

There are many ways to estimate weights (Meyer and Booker 1991). However, these require input from the decision maker. How well the decision maker knows the experts seriously affects the aggregation. Usually, additional performance data on the experts is necessary for proper estimation of weights or parameters (as in the LS method). Such data may not be available for many applications, requiring that the decision maker be the sole provider of estimates for weights or other parameters. Even when such data is available, the use of imperfect parameter values produces misleading posterior distributions. Specifically, the coverage of the underlying parameter θ by interval estimates is extremely poor.

As a result of the difficulties in estimating weights, some have suggested (Genest and Zidek, 1986) the use of equal weights. This solution changes the decision maker's influence to that of selecting the experts and, of course, weighting them equally. However, it also prevents adjustments for bias and underestimation of uncertainty which may vary from one expert to another. While comparison studies are lacking to provide guidance on the use of weights, the decision maker should perform his own sensitivity study, changing the weights to capture his uncertainties about them within a chosen aggregation method. For general weighting methods as in Equation (5), the $\{w_i\}$ must be highly variable in order to impact the aggregation. In the case where certain experts receive extremely large weights and others receive small ones, the decision maker might question the original selection process of the experts.

PROBLEMS WITH CORRELATION

For several decades, the problem of pooling potentially correlated expert opinions has been examined. The first methods for aggregating opinions assumed uncorrelated and independent expert opinions. As aggregation methods evolved, dependencies among experts were characterized by inter-expert correlations. Experts were thought to be correlated because "Experts often have some common training and experience, they see the same data, and they may use similar aids (e.g. statistical procedures such as regression analysis)." (Winkler, 1981), and because high correlations were observed among experts' estimates in some studies such as weather forecasting (Hogarth, 1975) and football betting lines (Stern, 1991; Winkler, 1981).

The sources of such correlation among experts were based on the speculation that some common conditions existed which mutually affected the experts in their estimation processes. More recently, sources of correlation have been identified from the problem solving processes of the experts rather than from their common backgrounds or experiences (Booker and Meyer, 1988). These problem solving processes include the different steps used by experts to arrive at an answer, including assumptions, boundary conditions, equations, and physical relationships.

Many elaborate weighting schemes were proposed in response to the hypothesized correlation among experts. These methods usually require the estimation of a correlation structure among the experts. The LS method, like many others, requires the decision maker to estimate correlation coefficients for all pairs of experts.

Examining the performance of the LS standard deviation, (4), under the simplified condition of all expert pairs having the same correlation coefficient, leads to a phenomenon that is also found in other methods. As the correlation coefficient increases, the resulting standard deviation increases, provided all other quantities are held constant. However, as the correlation coefficient continues to increase beyond some optimum point, the standard deviation begins to decrease. This result is algebraically verified by examining the derivatives of Equation (4) with respect to the common ρ. Even using different correlation coefficients in the LS method, the resulting standard deviation is very sensitive to the values in the correlation matrix (Picard and Booker, 1993).

The fundamental problems in using correlated experts are twofold. First, if the estimated correlation greatly differs from the true underlying correlation, then the final aggregation estimate and its variance will not be accurate. Second, the decision maker's collection of k experts probably does not provide him with k independent opinions or even k uncorrelated opinions. To understand the effects on the number of independent experts when experts share a common correlation, the concept of an equivalent number of experts, $n(\rho)$, has been proposed. If the correlation structure among the experts is the same, ρ, and the variance is the same, then Clemen and Winkler (1985) use an equivalent number of experts defined as

$$n(\rho) = k \; / \; [1+(k-1)\rho] \; . \tag{6}$$

For example, if there are 5 experts with a common correlation of 0.9, then the decision maker really only has the equivalent of 1 independent opinion. This relationship is presented to illustrate the effect of using correlated experts in the idealized case of common ρ and common variance. Spending large amounts of time and money on many experts whose opinions are all highly correlated is not cost effective.

Finding an aggregation method that can handle correlation among experts under realistic conditions and still be robust to effects induced by imperfect decision maker input is a difficult task. However, studies on effects of estimating correlations (Picard and Booker, 1993) and on the sources of correlations (Booker and Meyer, 1991) offer results for understanding the problems associated with correlation among experts and pave the way for additional work.

PROBLEMS WITH UNCERTAINTY

The PRA community has made progress in requiring and using uncertainty estimates from experts. Likewise, many aggregation methods have some mechanism for uncertainty characterization. These characterizations are commonly in the form of standard deviations, error bars, maximum to minimum ranges, intervals of values, or percentiles. However, there are some problem areas associated with characterizations of uncertainty.

First, neither the expert providing the information, nor the decision maker using it may have an adequate (or accurate) interpretation of the meaning of the uncertainty measure being used. Experts and decision makers are often unfamiliar with concepts such as percentiles or standard deviations. In addition, they may not be familiar with probability distributions, which often are the basis of quantifying uncertainty. An even worse case occurs if ill-defined terms are attached to values without admitting a lack of knowledge or simply due to custom. For example, the engineering literature commonly uses the term "error bars," but what is meant by this can greatly differ and is rarely defined. Thus, one expert's error bars may be a 90% coverage interval, another's may be a maximum to minimum interval of values.

Second, as mentioned above, there is the well documented problem that any of these measures given by experts generally underestimates the actual uncertainty. This remains a problem even when experts are familiar with the uncertainty estimates and are made aware of the underestimation bias through training and careful monitoring. For example, an interval defined by the expert using the 95^{th} and 5^{th} percentile values may in fact correspond to the 65^{th} and 35^{th} values in an underlying distribution.

The LS method is designed to use standard deviations provided by the experts of their estimates of the parameter θ. These standard deviations are adjusted by the decision maker to account for the underestimation of uncertainty using the $\{\chi\}$. However, the decision

maker's ability to properly make this adjustment remains in question. The results of a sensitivity study (Picard and Booker, 1993) indicate that even when the decision maker has sufficient data from the experts' past performance, uncertainties in estimates of $\{\gamma_i\}$ propagate to uncertainties in aggregated opinions which are not captured by Equation (4).

There are few studies which address these issues. The effects on aggregation of using one uncertainty measure versus another are not known. The success of using counter biasing techniques to provide better estimates of uncertainty has been limited (Meyer and Booker, 1991). Yet, characterizing and analyzing uncertainty remains very important in applications relying on expert opinion.

CONCLUSIONS

This paper has summarized many of the difficulties involved in aggregating expert opinions from multiple experts. Additional, more complicated problems exist. For example, in most expert elicitations, estimates from multiple experts are required for multiple events or components. So, many aggregation problems are multivariate in nature.

There are no widely accepted methods for quantitatively comparing diverse aggregation methods. One reason for this difficulty is because different methods assume different input information from the decision maker.

In addition, the robustness of each method to violations of assumptions and conditions requires much more study. While research into human cognition and knowledge acquisition areas continues, it rarely relates to the methodological issues of combining experts' information. Picard and Booker (1993) show how the LS method is very sensitive to imperfect decision maker input even when all the assumptions and conditions of the method are appropriate, and other aggregation procedures share this property.

Identifying the problem areas that are increasingly coming to the attention of analysts and decision makers is a good beginning. Even though more examination of the issues raised here is needed, studies continue to provide insight into the use of aggregation methods.

REFERENCES

Booker, J. M. and Meyer, M. A., 1988, "Sources and effects of interexpert correlation: an empirical study," *IEEE Transactions on Systems, Man and Cybernetics* 18:135-42.

Capen, E. C., 1975, "The difficulty of assessing uncertainty," Society of Petroleum Engineers and the American Institute of Mining, Metallurgy, and Engineers 50th Annual Fall Conference and Exhibit, Dallas, Texas (September 28-October 1).

Clemen, R. T. and Winkler, R. L., 1985, "Limits for the precision and value of information from dependent sources," *Operations Research* 33:427-42.

Genest, C. and Zidek, J. V. , 1986, "Combining probability distributions: a critique and an annotated bibliography," *Statistical Science* 1:114-35.

Hogarth, R. M., 1975, "Cognitive processes and the assessment of subjective probability distributions," *Journal of the American Statistical Association* 70:271-91.

Janis, I. C., 1972, "Victims of Group Think: A Psychological Study of Foreign Policy Decisions and Fiascos," Houghton Mifflin, Boston

Lindley, D. V. and Singpurwalla, N. D. , 1986, Reliability (and fault tree) analysis using expert opinions, *Journal of the American Statistical Association* 81:87-90.

Meyer, M. A. and Booker, J. M., 1991, "Eliciting and Analyzing Expert Judgment: A Practical Guide," Academic Press, London.

Picard, R. R. and Booker, J. M., 1993, "Aggregating expert opinion in the presence of decision maker uncertainty," Los Alamos National Laboratory report, LA-UR 93-2757.

Stern, H., 1991, "On the probability of winning a football game," *American Statistician* 45:197-83.

Winkler, R. L., 1981, "Combining probability distributions from dependent information sources," *Management Science* 27:479-88.

THE ANALYSIS OF COMPETING FAILURE MODES

Roger M. Cooke

Department of Mathematics and Informatics
Delft University of Technology
Delft, The Netherlands

INTRODUCTION

Modern reliability data bases distinguish several competing failure modes for components, usually categorized as "critical", "degraded" and "incipient". When degraded or incipient failures are observed the component is taken off line and repaired to as good as new; hence each failure mode *right – censors* the others. Current techniques for analysing censored component life data model the failure modes as independent competing risks: the time history of a component socket is modeled as observations of the minimum of independent life variables, one variable for each failure mode. In the reliability context these techniques are quite inappropriate and can lead to seriously underestimating the critical failure rate. This paper presents techniques for analysing competing failure mode data. We assume throughout that two failure modes are distinguished, namely (critical) failure and censors. This work is supported by the European Space Agency and is performed in cooperation with the Swedish Nuclear Directorate and the Riso National Laboratory.

NOTATION AND DEFINITIONS

Throughout, X is an exponential variable corresponding to critical failure, with failure rate λ; Z is an arbitrary life variable corresponding to censoring via incipient failure. We observe independent and identically distributed copies of $Y = \{X \wedge Z, 1_{\{X<Z\}}\}$; that is we observe the smaller of X and Z, and observe which it is. $x_1,\ldots x_m$; $z_1,\ldots z_n$ are observed times to critical resp. incipient failure, from $N = m+n$ independent observations of Y. $\mathcal{L}_X$ denotes the Laplace transform of X, and "~" denotes asymptotic equivalence as $N \to \infty$. The *subsurvival functions* for X and Z are respectively $S^*_X(t) = P(X>t \text{ and } X<Z)$, $S^*_Z(t) = P(Z>t \text{ and } Z<X)$ (Peterson 1977). Subsurvival functions completely characterize competing failure mode data in the sense that any function of the data can be expressed as a function of the subsurvival functions. The *conditional subsurvival functions* for X and Z are respectively $S^*_{X|X<Z}(t) = P(X>t \mid X<Z)$, and $S^*_{Z|Z<X}(t) = P(Z>t \mid Z<X)$. When X and Z have continuous increasing distribution functions, then S^*_X and S^*_Z are positive and strictly decreasing, and $S^*_X(0)+ S^*_Z(0) = 1$. The *conditional probability of incipient failure* is $\Phi(t) = P(Z<X \mid X \wedge Z>t)$. $X \perp Z$ says that X and Z are independent. When $X \perp Z$, then S^*_X and S^*_Z uniquely determine the distributions for X and Z (Peterson 1977, Tsiatis 1975). When $X \perp Z$ and X and Z are exponential variables, with failure rates λ and μ, then $S^*_{X|X<Z} = S^*_{Z|Z<X}$ and $\Phi(t) \equiv \mu/(\lambda+\mu) = P(Z<X)$ (Cooke, 1993); the maximum likelihood estimate of λ is $m/(\Sigma x_i + \Sigma z_i)$.

RANDOM SIGNS CENSORING

Perhaps the simplest model for dependent right censoring is *random sign censoring* (called *age – dependent* censoring in Cooke 1993). Consider a component subject to right censoring, where X denotes the time at which a component would expire if not censored. Suppose that the event that the component's life be censored is independent of the age X at which the component would expire, but *given* that the component is censored, the time at which it is censored may depend on X. This situation is captured in the following

Definition: Let X and Z be life variables with $Z = X - \xi$, where ξ is a random variable, $\xi \leq X$, $P(\xi = 0) = 0$, whose sign is independent of X. The variable $Y = (\min\{X,Z\}, 1_{\{X<Z\}})$ is called a *random sign censoring of* X *by* Z.

Theorem 1 (Cooke 1993) Let (S_1^*, S_2^*) be a pair of continuous strictly monotonic subsurvival functions; then the following are equivalent:

(1) There exist random variables ξ and X, $X \perp \mathrm{sgn}(\xi)$ such that $S_1^*(t) = P(X>t \cap \xi<0)$; $S_2^*(t) = P(X-\xi > t \cap \xi>0)$;

(2) For all $t > 0$; $S^*_1(t)/S^*_1(0) > S^*_2(t)/S^*_2(0)$.

Condition (1) of theorem 1 says that the subsurvival functions S^*_1 and S^*_2 are consistent with a random signs censoring model. For random signs censoring under the conditions of Theorem 1 the conditional probability of censoring is maximal at the origin: $\Phi(t) = 1/(1+S^*_X(t)/S^*_Z(t)) < \Phi(0)$. Every set of censored observations is consistent with a right censoring model, but not every set of censored observations is consistent with a random signs censoring model. Assuming continuity and strict monotonicity, *Theorem* 1 says that a random signs censoring model exists if and only if for all t>0 the conditional subsurvival function for failure dominates that of maintenance. Under random sign censoring the population of observed failures are statistically equivalent to the original population, hence: $\lambda \sim m/\Sigma x_i$. Recalling the estimate under independent right censoring, $\lambda \sim m/(\Sigma x_i + \Sigma z_i)$, and noting that typically $\Sigma z_i >> \Sigma x_i$ for reliable systems, it is evident that the independence asusmption can lead to gross underestimates of the critical failure rate in the case of random signs censoring.

RANDOM CLIPPING

Perhaps the simplest model of interaction between an exponential life process X a warning process Z is gotten by assuming that X is always censored by a random amount X–Z. More specifically, we assume that X is exponential and for some positive random variable W independent of X, we observe X–W. W may be thought of as a warning which a component emits prior to expiring at time X. Of course W may be greater than X, which we interpret as censoring at birth. Let us suppose that censors at birth are simply not recorded. Suppose in other words, that components emitting warnings at birth are simply repaired until the warning disappears, and that the false start is not recorded as an incipient failure at time 0. Indeed, this is what usually happens. We call the variable X–W *given* X–W>0 a random clipping (RC) of X. The following result entails that in this case $\lambda \sim n/\Sigma z_i$ (on this model m=0). Recall, X is exponential with parameter λ throughout.

Theorem 2 Let W>0 be a random variable independent of X, and U = X–W. Then conditional on U>0, U has the same distribution as X.

Proof: For $u \in (-\infty, \infty)$ and $v = \max\{0,-u\}$ we have $dF_U(u) = \int_{u>v} \lambda e^{-\lambda(u+w)} dF_W(w)$. If $u \geq 0$, then $v = 0$ and $f_U(u) \propto \lambda e^{-\lambda u}$. ■

BOUNDED RANDOM WARNING - RANDOM INSPECTION

The variable X is subject to random inspections. We assume that the component emits a warning at time X–W, before expiring at time X. If an inspection occurs in the interval (X–W, X), then the component is pulled off for preventive maintenance, and we say that X is censored by Z = 'time of first inspection in (X–W, X)'. If no inspection occurs in (X–W, X) then the component is observed to fail at time X, and we stipulate that Z = ∞. If W > X then the component is censored at birth. We consider a random inspection policy described by a Poisson distribution with intensity γ. For any I, the probability of no inspections in (t, t+I) is $e^{-\gamma I}$ and the probability of at least one inspection in this interval is $1-e^{-\gamma I}$ We assume that the life variable X is independent of the inspection process. We consider the warning variable W independent of X. The possibility of censoring at birth complicates the computations considerably, and this is of dubious value since censors at birth are seldom recorded as such. In cases where W is typically much smaller than X, the phenomena near the component's birth are not important. We therefore seek a model which avoids these complications near birth, yet which captures the overall behavior of independent warning times W with W<<X. We assume therefore that W is bounded by some number d, and that no warning is emitted by the component if it expires before d. More specifically, we assume W<d, W and X independent given X≥d, and W=0 if X<d. The variable Y = $(\min\{X,Z\}, 1_{\{X<Z\}})$ is called BRWRI(d,γ). For X≥d, the probability of censoring is independent of X, as in random signs censoring; for X<d, however the probability of censoring is zero. The analysis of S^*_Z is rather complicated and explicitly involves the distribution of W. However, we can extract useful information from S^*_X. $P(X<Z) = S^*_X(0) = P(X<Z \cap X\le d) + P(X<Z \cap X>d) = 1 - e^{-\lambda d} + e^{-\lambda d}\mathcal{L}_W(\gamma)$. The subsurvival function for X is given by:

$$S^*_X(t) = \begin{cases} \iint_t^\infty \lambda e^{-\lambda u} e^{-\gamma w}\, du dF_W(w) = e^{-\lambda t}\mathcal{L}_W(\gamma): & t > d; \\ e^{-\lambda t} - e^{-\lambda d} + e^{-\lambda d}\mathcal{L}_W(\gamma): & t \le d. \end{cases}$$

The conditional expectation $E(X|X<Z) \sim m/\Sigma x_i$ is just the integral of the conditional subsurvival function: $E(X|X<Z) = (1/S^*_X(0))\int S^*_X(t)dt = [(1-e^{-\lambda d}+e^{-\lambda d}\mathcal{L}_W(\gamma))/\lambda - de^{-\lambda d}(1-\mathcal{L}_W(\lambda)]/S^*_X(0) = (1/\lambda) - P(Z \le X)/P(X<Z)$.

Theorem 3 Let $Y = (\min\{X,Z\}, 1_{\{X<Z\}})$ be BRWRI(d,γ); then

$$\lambda \sim \left[\frac{\Sigma x_i}{m} + \frac{dP(Z \le X)}{P(X < Z)}\right]^{-1}.$$

The statistic estimating the failure rate is less than that in the case of of random signs censoring, but the difference goes to zero as d goes to zero.

RANDOM WARNING - CONSTANT INSPECTION

We suppose that X is inspected at regular intervals I. If a warning is seen at the i–th inspection, then X is censored at time Z = Ii. We suppose that there is some positive random variable W independent of X, such that X's warning is emitted at time X–W. In otherwords, X is censored by Z, with Z=iI if I(i–1) < X–W ≤ Ii < X; and X is observed to fail at time X if no inspection occurs in the interval [X–W, X]. In this case we stipulate that Z=∞. If W exceeds I with positive probability, then it becomes impossible to estimate the failure rate of X from censored data. We therefore consider only the case that P(W≤I) = 1. Censors at birth are now possible, but censoring more than one inspection interval of the component's life is excluded. The subsurvival function S^*_Z is not continuous and has an atom at zero.

It is convenient to measure time in units of I, so that I = 1. The variable Y = $(\min\{X,Z\}, 1_{\{X<Z\}})$ is RWCI(W). Recall for $0 < p < 1$:

$$\Sigma_{j>i}\, p^j = p^{i+1}/(1-p);\quad \Sigma_{i\geq 0}\,\Sigma_{j>i}\, p^j = p/(1-p)^2.$$

Theorem 4. Let Y = $(\min\{X,Z\}, 1_{\{X<Z\}})$ be RWCI(W); then (i) $P(Z\leq X) = (1-\mathcal{L}_W(\lambda))/(1-e^{-\lambda}) \sim n/N$; (ii) $\lambda \sim \ln(1+n/\Sigma z_i)$; (iii) $\Phi(i) = e^{-\lambda i}P(Z \leq X)/\mathcal{L}_W(\lambda)$; (iv) $S^*_Z(i)=S^*_X(i+1)$.

Proof: (i): Counting censors at birth, we have: $n/N \sim P(Z\leq X) = \Sigma_{i\geq 0}\, e^{-\lambda i}\int e^{-\lambda(i+W)}\, dF_W = (1-\mathcal{L}_W(\lambda))/(1-e^{-\lambda})$.

(ii): $S^*_Z(i) = P(Z > i \text{ and } Z < X)$

$$= \Sigma_{j>i}e^{-\lambda j} - \int e^{-\lambda(j+W)}dF_W = e^{-\lambda(i+1)}(1-\mathcal{L}_W(\lambda))/(1-e^{-\lambda}).$$

$$\Sigma z_i/N \sim \Sigma_{i\geq 0}S^*_Z(i) = (1-\mathcal{L}_W(\lambda))e^{-\lambda}/(1-e^{-\lambda})^2$$

$$= P(Z\leq X)e^{-\lambda}/(1-e^{-\lambda}).$$

Hence, $\Sigma z_i/n \sim e^{-\lambda}/(1-e^{-\lambda})$ from which (ii) follows. Using

$$S^*_X(i) = P(X > i \cap X < Z) = \Sigma_{j\geq i}\int e^{-\lambda(j+w)}\, dF_w - e^{-\lambda(j+1)} =$$

$$= (\mathcal{L}_W(\lambda) - e^{-\lambda})e^{-\lambda i}/(1-e^{-\lambda});$$

$$S^*_Z(i) + S^*_X(i) = \mathcal{L}_W(\lambda)e^{-\lambda i};$$

(iii) and (iv) are calculations. ■

The failure rate of X can be estimated independently of the distribution of W, in fact we can estimate $\mathcal{L}_w(\lambda)$ also, as (iii) shows. Note that this model is not consistent with random signs censoring as the probability of censoring is not independent of a component's age. Suppose that $W < d < 1$ with probability one, then the probability of X being censored when $j + d < X < (j+1)$ is zero.

A constant is statistically independent of every random variable. As a special case of *Theorem* 4, we may therefore consider the case that W is a constant, say d with $d < 1$. In such a model, a component issues a warning at time $X - d$ before expiring at time X. Such a model is termed CWCI(d). The Laplace transform of a constant d is simply $e^{-\lambda d}$. We have: $P(Z\leq X) = (1-e^{-\lambda})/(1-e^{-\lambda})$; $\Phi(i) = (1-e^{-\lambda d})/(e^{-\lambda d}(e^{\lambda} - 1))$.

PROPORTIONAL WARNING - CONSTANT/RANDOM INSPECTION

This model is similar to the previous model except that the warning is emitted at time X/δ if the component expires at X; with $\delta>1$ constant. Under constant inspection the process is called PWCI(δ). Exact solutions for this model are difficult. Howver if $i \leq 1/(\delta-1)$ then $\delta i \leq i+1$, and if δ is close to one, then most contributions will come from inspection periods i such that $\delta i \leq i+1$. Let "≈" denote "equal up to effects for $i > 1/(\delta-1)$". As before, we set I = 1. Note that there is no censoring at birth. We have:

Theorem 5 Let Y = $(\min\{X,Z\}, 1_{\{X<Z\}})$ be PWCI, then:

$$\text{(i) } \lambda \approx -\ln\left[1 - \frac{2nN}{\Sigma z_j + nN + n^2}\right];$$

(ii) $\delta \approx -(1/\lambda)\ln\left(1 - \dfrac{2nN}{\Sigma z_j + nN - n^2}\right)$

(iii) $\Phi(i) = e^{i\lambda(\delta-1)}/(e^{\lambda}-1) - 1/(e^{\lambda\delta}-1)$.

Proof: (i): The component is censored in the i–th observation period if and only if $i \le X < i\delta$, thus

$$n/N \sim P(Z \le X) = \left(\sum_{i \le 1/(\delta-1)} e^{-\lambda i} - e^{-\lambda\delta i}\right) + e^{-\lambda/(\delta-1)} \approx$$

$$\Sigma_{i\ge 0}\, e^{-\lambda i} - e^{-\lambda\delta i} =$$

$$\frac{1}{1-e^{-\lambda}} - \frac{1}{1-e^{-\lambda\delta}} = Q_1 - Q_2.$$

$$\Sigma z_j/N \sim \Sigma_{i\ge 0} S^*_Z(i) \approx \Sigma_{i\ge 0}\, \Sigma_{j>i}\, e^{-\lambda j} - e^{-\lambda\delta j} = e^{-\lambda}Q_1^2 - e^{-\lambda\delta}Q_2^2.$$

Note that the inner summation runs over $j > i$, as $S^*_Z(i) = P(Z > i \cap Z < X)$. Adding the "$j = i$" term to the summation results in:

$$n/N + \Sigma z_j/N \sim P(Z < X) + \Sigma_{i\ge 0} S^*_Z(i) \approx \Sigma_{i\ge 0}\, \Sigma_{j\ge i}\, e^{-\lambda j} - e^{-\lambda\delta j}$$

$$= Q_1^2 - Q_2^2 = (Q_1 - Q_2)(Q_1 + Q_2).$$

Hence dividing by the first equation and solving for Q_1:

$$Q_1 + Q_2 \sim 1 + \Sigma z_i/n;$$

$$2Q_1 = n/N + 1 + \Sigma z_i/n;$$

$$\lambda \approx -\ln\left(1 - \frac{2nN}{\Sigma z_j + nN + n^2}\right).$$

(ii): The expression for δ results from solving for Q_2:

$$2Q_2 \sim 1 + \Sigma z_i - n/N;$$

$$\delta \approx -(1/\lambda)\ln\left(1 - \frac{2nN}{\Sigma z_j + nN - n^2}\right).$$

(iii): $S^*_Z(i) = \Sigma_{j>i}\, e^{-\lambda i} - e^{-\lambda\delta i}$; $S^*_X(i) = \Sigma_{j\ge i}\, e^{-\lambda\delta i} - e^{-\lambda(i+1)}$;

$$S^*_Z(i) + S^*_X(i) = e^{-\lambda\delta i};$$

$$\Phi(i) = S^*_Z(i)/(S^*_Z(i) + S^*_X(i)) = e^{i\lambda(\delta-1)}/(e^{\lambda}-1) - 1/(e^{\lambda\delta}-1). \blacksquare$$

Another estimate of λ can be obtained using the subsurvival function for X, if we make a certain simplification. If X is observed to fail, this can only occur between δi and $(i+1)$ for some inspection time i. Suppose the failure time is recorded as $i+1$; suppose in other words, that failures could only be discovered at the next inspection. We should then have:

$$\Sigma x_i/N \sim \Sigma_{i\ge 0}\Sigma_{j\ge 0}\, e^{-\lambda\delta i} - e^{-\lambda(i+1)} = Q_2{}^2 - e^{-\lambda}Q_1{}^2;$$

$$\Sigma x_i/N + \Sigma z_i/N \approx (1-e^{-\lambda\delta})Q_2^2 = Q_2;$$

$$Q_1 = n/N + (\Sigma x_i + \Sigma z_i)/N;$$

$$\lambda \approx -\ln\left(1 - \frac{N}{n + \Sigma x_i + \Sigma z_i}\right).$$

This latter estimate involves upwards rounding off the failure times, but on the other hand it uses all of the observations, and is therefore less sensitive for sampling fluctuations.

The behavior of the PWCI model can be intuitively understood as follows; for larger values of X, the time during which the warning is on, $X(\delta-1)$ gets longer and it becomes more probable that the component will be censored. The observed failures times tend to be drawn from the lower end of the distribution; whereas observed maintenances tend to censor the older components. This suggests intuitively that $S^*_Z(t)/S^*_Z(0) > S^*_X(t)/S^*_X(0)$. For PWCI variables the function $\Phi(i)$ is increasing. Indeed, since $\delta>1$, statement (iii) shows that this is the case. We must note, however, that no failures would be observed for times X such that $X - X/\delta > 1$, since the warning period is then so large that inspection cannot miss it. In otherwords, we should see no failures beyond $x = \delta/(\delta-1)$. Substituting $j = 0$ in *Theorem* 5 (iii), we find to the first order: $\Phi(0) \simeq (\delta-1)/(\lambda\delta) \simeq P(Z \leq X)$. Note also that the variable X/δ follows a Weibull distribution if X is exponentially distributed. The errors which enter with "$\approx$" in the estimation of λ are on the order of $e^{-\lambda/(\delta-1)}/(\delta-1)$.

Suppose that inspection follows a Poisson distribution with intensity γ. If an inspection occurs while the warning is issued, the component is preventively maintained at time Z = "first inspection beyond X/δ"; if no inspection occurs in the interval $[x/\delta, X]$ then $Z = \infty$ and the component fails at X. The variable $Y = (\min\{X,Z\}, 1_{\{X<Z\}})$ is called PWRI(γ). The analysis of S^*_Z is rather complicated, but simple results can be obtained only from S^*_X.

Theorem 6 Let $Y = (\min\{X,Z\}, 1_{\{X<Z\}})$, be PWRI($\gamma$) then $\lambda \sim m^2/(N\Sigma x_i)$.

Proof: Put $\alpha = (\delta-1)/\delta$. Then $P(X < Z) = P\{\text{no inspection in } (X/\delta, X)\} = \int \lambda e^{-(\lambda+\gamma\alpha)t} dt = \lambda/(\lambda+\alpha) \sim m/N$. Also:

$$\Sigma x_i/N \sim \int S^*_X(t)dt = \int\int_{u>t} \lambda e^{-(\lambda+\gamma\alpha)u} du\, dt = \lambda/(\lambda+\alpha)^2;$$

$$\lambda \sim m^2/(N\Sigma x_i). \blacksquare$$

Expressions can be obtained for $S^*_z(t)$ and $\phi(t)$, but no simple pattern emerges. It is interesting to compare the two proportional warning models PWCI and PWRI for some representative values. We measure time in units of the inspection interval I, and choose $\gamma = 1$ so that the expected number of inspections per unit time is one. Putting $\alpha = (\delta-1)/\delta$, we have to the first order: $P_{PWCI}(X < Z) = (\lambda-\alpha)/\lambda$; $P_{PWRI}(X < Z) = \lambda/(\lambda+\alpha)$.

REFERENCES

Tsiatis, A. (1975) "A nonidentifiability aspect of the problem of competing risks" **Proceedings of the National Academy of Sciences USA**, 72, no 1 pp 20–22.

Peterson A.V. (1977) "Expressing the Kaplan–Meier estimator as a function of empirical subsurvival functions" JASA Dec. vol 72 no 360 pp 854–858

Cooke, R.M. (1993) "The total time on test statistic and age–dependent censoring" **Stat. and Prob. Let.** vol 18 no 5.

AN APPLICATION OF EXPERT OPINIONS APPROACH IN COMBINING MEASUREMENT RESULTS

Meir Haim, Mordechai Jaeger and Dov Tzidony

RAFAEL Reliability Center
P.O. Box 2250 (22)
Haifa 31021, Israel.

INTRODUCTION

The Expert Opinions approach is widely recognized in risk and reliability studies. According to this approach, several experts are asked for their opinions about a numerical value of an unknown parameter. The approach suggests a method for weighting these different opinions[1,2]. The paper describes an application of a decision making model, adapted for measurement problems. This model is based on the Expert Opinions approach, together with a loss function. Such a function should reflect the "penalty" involved in making a wrong decision, and therefore enables the analyst to make an "optimal" decision under a given criterion. The model applicability for controlling the yield of a desired product is demonstrated for an industrial chemical process.

A design parameter of the chemical process, namely the optimal addition time of a catalyst, is estimated by various measurement methods. Each method is based on a different physical phenomenon and has its own possible bias and uncertainty affecting its characteristic ***accuracy***. The term accuracy refers to the degree of agreement between the measured value by a given method and the "true" value[3].

The model is used to determine the catalyst addition time in order to minimize the loss due to reduced yield. Thus, by integrating technological and probabilistic considerations, the model becomes an effective decision making tool for efficient production management.

In the following chapters a probabilistic model is formulated and its applicability is demonstrated through an example.

MODEL FORMULATION

In this model θ is the "true", but unknown, optimal catalyst addition time. The decision maker's state of knowledge about θ is given by a p.d.f. $\pi(\theta)$. Several

spectroscopic methods such as Nuclear Magnetic Resonance (NMR), Infra Red (IR) and Ultra Violet (UV) can be used to estimate θ. The value θ_i is the estimate based on the i'th method (in our case i=1,2,3). The uncertainty of the decision maker concerning the accuracy of the i'th method is represented by a p.d.f. of the estimated θ_i ***given*** the "true" value θ, denoted as $f(\theta_i|\theta)$.

It is important to realize that each method is treated as an "expert". Pure technological considerations, concerning each method, are interpreted by a p.d.f. which weights the evidence procured by each "expert". This is portrayed by $f(\theta_i|\theta)$. The measurements resulted in by each method (i.e., θ_1, θ_2, θ_3), serve as new evidence for updating our current state-of-knowledge about θ, represented by $\pi(\theta)$.

The updating process is performed coherently via Bayes theorem:

$$\pi^*(\theta) = \frac{\pi(\theta)\cdot f(\theta_1|\theta)\cdot f(\theta_2|\theta)\cdot f(\theta_3|\theta)}{\int_{\theta'}\pi(\theta')\cdot f(\theta_1|\theta')\cdot f(\theta_2|\theta')\cdot f(\theta_3|\theta')\,d\theta'} \qquad (1)$$

$\pi^*(\theta)$ is the updated state-of-knowledge about θ, based on:

- an ***a priori*** state-of-knowledge distribution $\pi(\theta)$.
- evidence θ_1, θ_2, θ_3 (i.e., measurement results).
- accuracy of each method, interpreted by $f(\theta_i/\theta)$.

The objective is to calculate the best estimate for θ, associated with optimizing a loss function. An erroneous assessment of θ leads to a reduction in the production yield. The analysis is tackled as a decision making problem concerning the catalyst optimal addition time θ.

We define a loss function $L(\theta_o,\theta)$ which reflects the penalty associated with the "gap" between the assessed value θ_o and the "true" value θ.

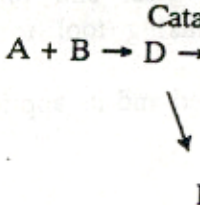
The commonly used approach involves selecting the value θ_o which minimizes the expected loss (i.e., Bayes decision rule):

$$\underset{\theta_o}{Min}\int_{\theta}\pi^*(\theta)L(\theta_o,\theta)\,d\theta \qquad (2)$$

APPLICATION

A General Reaction

Suppose a reaction of the type:



The desired product is E. In order to obtain a high yield, the catalyst should be added to the reaction vessel when the concentration of the intermediate D reaches a certain level C_{IM} at time θ (the order of magnitude is about one hour). The concentration level

level C_{IM} at time θ (the order of magnitude is about one hour). The concentration level (from which the actual catalyst addition time is derived) can be measured by various physical methods, e.g., NMR, IR, UV. Each of these methods is based on a different physical effect with its unique level of uncertainty. Since the levels of uncertainty are different for each of the models, so are their respective accuracies.

Accuracy Evaluations

The parameter of interest θ is (derived from C_{IM}); therefore, the accuracy of each method is estimated by evaluating the probability of being above or below θ. Given that the order of magnitude of θ is about one hour, the deviations of each method are given in minutes. In this manner each method's accuracy is described by some distribution.

NMR. In this method there is an equal probability of being above or below θ. However, it is believed that there is a fairly high probability that the deviations will not exceed 15 minutes. Hence, a normal distribution with $\mu=\theta$ and $\sigma=7.5'$ is assumed.

$$f(\theta_1 \mid \theta) = \frac{1}{\sqrt{2\pi}\,\sigma} \exp\left[-\frac{1}{2}\left(\frac{\theta_1-\theta}{\sigma^2}\right)^2\right] \tag{3}$$

IR. In this example this method is not symmetric since there is a greater chance to underestimate the "true" θ. Suppose that it is plausible to be up to 30' below θ or up to 10' above θ. Therefore, a triangular distribution is assumed:

$$f(\theta_2 \mid \theta) = \begin{cases} 0.05\left[1-\left(\frac{\theta-\theta_2}{30}\right)\right] & , \quad \theta-30<\theta_2\le\theta \\ 0.05\left[1-\left(\frac{\theta_2-\theta}{10}\right)\right] & , \quad \theta<\theta_2\le\theta+10 \\ 0 & , \quad \textit{else} \end{cases} \tag{4}$$

UV. In this method the deviations are symmetrical but relatively large ±30'. Hence, the appropriate distribution is uniform.

$$f(\theta_3 \mid \theta) = \begin{cases} 1/60 & , \quad \theta-30<\theta_3\le\theta+30 \\ 0 & , \quad \textit{else} \end{cases} \tag{5}$$

State-of-Knowledge Distribution

A uniform wide range state-of-knowledge distribution was selected. It reflects a relatively high degree of uncertainty about θ.

$$\pi(\theta) = \begin{cases} 1/R & , \quad \theta<\theta\le R \\ 0 & , \quad \textit{else} \end{cases} \tag{6}$$

Loss Function

The "penalty" for a wrong decision in our case is approximately proportional to the difference between θ and θ_o, and therefore the loss function $L(\theta_o,\theta)$ is:

$$L(\theta_o,\theta) = K\,|\theta-\theta_o| \qquad (7)$$

where K is a given constant (K>0).

Results

The measurement results in each method are:

$$\theta_1 = 80 \text{ min} \quad , \quad \theta_2 = 50 \text{ min} \quad , \quad \theta_3 = 60 \text{ min}$$

The updating is performed numerically according to Equation (1) and Bayes decision rule (Equation (2)) results in:

$$\theta_o^* = 71 \text{ min}$$

A sensitivity analysis was performed to examine the effect of a wrong decision on the loss function. The results indicated that a bias of ±5 minutes from the optimal value θ^*_0 increases the loss function by approximately 50%.

CONCLUSIONS

The described approach was found to be an effective tool in a decision making process. It intelligently combines measurement results which were evaluated by different physical methods.

It may be applied to other applications for measurement of water resource contamination.

REFERENCES

1. A. Mosleh and G. Apostolakis, Models for the use of expert opinion, in ***Low Probability High Consequence Risk Analysis***, ed. R.A. Waller and V.T. Covello, Plenum Press, New York, 1984.
2. S. Kaplan, "Expert information" versus "expert opinion". Another approach to the problem of eliciting/combining/using expert knowledge in PRA, ***Reliability Engineering and System Safety***, 35, 61-72 (1992).
3. ***Standard Methods for the Examination of Water and Wastewater***, M.A.H. Franson (ed.), American Public Health Association, 15th Edition, Washington DC, 18-20 (1981).

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)

SOME THOUGHTS ON THE REQUIREMENTS FOR A SECOND GENERATION HUMAN RELIABILITY ASSESSMENT PROCESS

Anthony J. Spurgin

Consultant
4252, Hortensia St.,
San Diego, CA. USA.

INTRODUCTION

Current Human Reliability Assessment(HRA) techniques are being questioned by many people in terms of their usefulness in representing the reliability of organizations and persons. For example, Ed Dougherty, Jnr. has argued eloquently for the need for a second phase in the development of HRA methods (Dougherty, 1990). I agree with Ed's premise that HRA developments are needed. This is not to infer that all that was done before was wrong. But rather as our knowledge of the field expands, this should be reflected in improved methods and increased awareness of the source of human errors. These improvements should not only in quantification methods, but in the representation of humans and organizations in risk models to help improve the safety of high risk operations.

BACKGROUND

By many accounts, the influence of humans on the plant accidents is considered to be in the range of 60% to 90%. If this is correct then our emphasis should be more on people and less on equipment. This is not to say that systems have no influence on safety, but rather that the approach should be balanced. Human reliability has been under-played in the PRA business, primarily due to the slow rate of development of HRA methods. The perspective of some authorities is that we cannot do anything about predicting human reliability, therefore the safety of high risk systems be obtained by designing out humans. This attitude has not helped to improve human reliability methods.

CURRENT HRA METHODS

There have been a number of reviews of the human reliable methods, for example Haney et al, 1989. Three basic methods have been developed, THERP, Time Reliability Curves (TRC) and expert judgement methods.

Criticism has been levelled at THERP, saying that it is too mechanistic and neglects the influences of cognitive behavior. It is difficult to get consistent results and is not plant specific. These criticisms have been around for a long time but the method continues to be used

The time reliability curves of which there are a number, including Hannaman, Spurgin and Lukic, 1984. TRCs are to various degrees connected to operator response data from simulators. TRCs are closer to operator reliability than THERP, but TRCs are not normally of direct use in PRAs, except for time limited situations. However, simulator data can be used to support the HRA. It is of use to Operations and Training(Bareith et al, 1993).

Expert judgement methods lie at the heart of the majority of PRAs. The task is often accomplished by interviewing operators and instructors. This approach is very suspect, depending as it does on the assessment of supposed experts. Many of the HRA experts lean on the use of operators as domain experts. Simulator exercises have shown, that operators are not very aware of their shortcomings. Instructors are a better resource, but even they are not that good, since they are not aware of crew to crew variability in performance. One advantage of the expert judgement method is that it is close to plant conditions. From my interviews of instructors, they are able to point out differences between expected and actual operator reliability. This an advantage over the application of either THERP or TRCs for the HRA process.

The EPRI Operator Reliability Experiments study (Spurgin et al, 1990) produced generic TRCS that could be modified by a specific task median times, thus approximating to plant specific values. The approach only useful for HRAs, when the available times are within the range of the TRC.

Simulator data shows that operators' responses can range from very consistent to inconsistent depending on the influence of procedures, MMI and training.

REVIEW OF ACCIDENTS

Detailed examination of real accidents can indicate how persons and equipment interact. Often in building analytical models of situations, we make simplifications which may or may not be appropriate. By examining real accidents we can raise questions that call help us better understand the situations we are analysing. We can see if we making the correct set of assumptions about how persons interact with the equipment and each other.

Over the last few years, we have seen a large number of accidents involving nuclear and chemical plants, aerospace vehicles of various kinds, ferries, oil rigs and tankers, trains and trucks, gas pipelines and medical equipment. Examination of the accidents clearly shows the central role that management plays in safety. The reviews indicate the

strong interactions between operations, maintenance and management. No part of society seems to be free of accidents. Problems abound!

The US nuclear industry is relatively good, when it comes to absolute measures of numbers persons killed or injured. However, the impact of the need to survive may cause this record to change unless steps are taken to preserving safety while increasing cost effectiveness, i.e., reducing O&M costs.

Management sets the tone of an organization and for the most part the staff are compliant with the wishes of management. The influence of Management has to be included in the HRA if we wish to understand the influence of humans on plant safety. The separation of operations and maintenance as modelling in the PRA is not justified, unless there are strict rules enacted and supported by management action. For example, the Piper Alpha accident was in part caused by the interaction between operations and maintenance and condoned by management. Management was held accountable by the enquiry. In more and more cases, management is found to be partially accountable for accidents. This is true in the case of Bhopal, the Kings Cross underground fire, Chernobyl and various tanker spills.

LESSONS DRAWN FROM REVIEWS

The study of accidents shows that all aspects of the organization have an impact on the initiation and sequence of accidents. If we are to reduce the frequency and consequences of accidents we need to be able to predict the interactions between the various parts of an organization. Management is significant contributor to both safe or unsafe practices. Management decides on the budgets and what aspects should be emphasized, i.e. production or safety, etc. Also, even small changes in management policy can effect the morale of the staff leading to significant changes in plant safety.

RECOMMENDATIONS FOR DEVELOPMENTS IN HRA

The next generation of HRA techniques needs to focus on the holistic effects of all aspects of plant organization on safety. To ignore the influence of management on training, maintenance and the morale, is to misestimate the reliability of the various operations. This is particularly the case when an organization is undergoing large and rapid changes in working conditions. In stable working environments, it might be possible to assume that the various parts of an organization can be considered to be independent of each other. This is not the case for organizations in turmoil. Organizational influences introduce dependencies not accounted for in the previous HRA methods.

In addition to worrying about how to incorporate management influences into the HRA process, there is a need to improve the current person-focused HRA tools for quantification and representation. There seems to be an attitude that it is possible to predict human reliability without understanding working conditions, i.e. we can make

predictions without observing the work place activities. Errors are induced by the working situation this includes procedures, the man-machine interface, training, etc., as well as the morale of the staff. Morale can affect the person's attention to detail, hence induce a higher error rate.

Currently we are using decision tree formulations in a number of HRA studies to help model these various influences. The decision tree approach is based on an integration of simulator results and expert judgements. This approach offers the capability of combining data, and expert judgement in a scrutable way, so that one can examine the assumptions that the HRA analyst is making. The tree headings and their order reflect the importance of the various contributing factors. The structure of the trees reflects the influence of the combination of events which result in the end state probabilities. The simulator results provide information, which aids the analyst select the headings and their order. Data on operator responses also help to determine the probability distributions of the end states. This process enables the simulator results to be integrated into the HRA process. The simulator is a useful tool for helping the HRA analyst understand the operators, unfortunately it does not supply all the answers.

It appears that a number of HRA analysts have difficulties with simulator results since it does not exactly match actual situations. I can appreciate their concerns, but ask the question what else is available that is better? I suggest the rather than resisting the use of simulators, we should be interested in using these vehicles to improve our understanding of human reliability and how it is affected by various situational factors. The influence of these factors can be transferred to other situations, which are not simulated. The simulator should be used for HRA research to answer questions about the influence of a number of things on operators. Some research has been carried out on the impact of various ways of controlling accidents, based on the use of procedures, operator knowledge, etc., in terms of their effectiveness. This kind of work was very useful in establishing the relative effectiveness of the various approaches, but more needs to be done. Without some of the basic work being carried out the results of the HRA is less significant. There is a need to carryout more basic research on some of these issues.

In summary, most of the current methods do not satisfy the need for accurate plant specific HRA methods and there is a need to develop better methods. It is my opinion that the simulator is a useful tool to help fulfil that need. Also the steps that we have taken to integrate the simulator results into a decision tree structure is a move in the right direction, but more needs to be done especially for situations like maintenance and testing.

The role of management needs to be fully factored into the HRA work, especially for organizations in transition. The current work on this aspect is in the early stage of development. It is an important issue and needs to be seriously addressed. Problem managements can have a profound effect on the safety of operation of high risk plant and this is illustrated by the record. Management needs tools to inform them of the consequence of their decisions before the

organizations run into problems, much the same as their financial tools provide!

REFERENCES

Bareith, A. et al., 1993, **On the use of Data Collected during Operator Reliability Experiments at Paks NPP**, PSAM II, San Diego, CA.

Dougherty, E. M., 1990, **HRA - Where Should Thou Turn?** Reliability Engineering and System Safety, 29 (3), p. 283-299.

Hannaman, G.W., A.J.Spurgin and Y.D.Lukic, 1984, **Human Cognitive Reliability Model for PRA Analysis**, NUS Corporation. San Diego, Draft EPRI report, Electric Power Research Institute, Palo Alto.

Haney. L.N., et al., 1989, **Comparison and Application of Quantitative Human Reliability Analysis Methods for Risk Methods Integration and Evaluation Program (RMEIP)**, NUREG/CR-4835 (1989).

Spurgin, A.J. et al., 1990, **Operator Reliability Experiments Using Power Plant Simulators**, EPRI NP-6937, Electric Power Research Institute, Palo Alto, California.

THE NEED FOR, AND A PROPOSED STRUCTURE OF, A SECOND GENERATION HRA METHODOLOGY

Gareth W. Parry

NUS
910 Clopper Road
Gaithersburg, Maryland 20878

INTRODUCTION

The numerous Probabilistic Safety Assessments (PSAs) that have been performed for nuclear power plants have highlighted the importance of considering the impact of plant personnel on the potential for severe accidents. While some effort has been expended on developing approaches to represent this impact by incorporating human error basic events in the structure of the plant logic models-the event trees and fault trees-(see Wakefield et al, 1992), considerably more effort has been expended on developing methods to estimate human error probabilities (HEPs) for those events. From the point of view of impacting the risk from full power operation, it is generally assumed that the most important set of human interactions are those that represent the responses of the operating crew that follow an initiating event, and that are carried out using guidance from written procedures, which include emergency operating procedures, abnormal operating procedures, annunciator response procedures, etc. The human reliability analysis (HRA) approaches that have been used in PSAs have been criticized on several counts, and there is an emerging consensus that improved methods are required (See for example, Dougherty, 1990). This paper presents the author's views on why improved methods are needed, and gives some suggestions on what form a new HRA approach for use in conventional PSAs should take, and how this might be developed.

A CRITIQUE OF CURRENT PRA PRACTICE

Two of the major criticisms of HRA approaches used in PSAs are; (a) they do not generally address errors of commission, and (b) there is no universally accepted, theoretically sound method of quantifying human error probabilities.

Errors of Commission

Interactions that are associated with operating crew responses following an

initiating event are usually introduced into the plant model through a binary, success/non-success logic; failures are modeled as occurring from non-response, i.e., as errors of omission. Other failure modes, such as specific inappropriate acts resulting from human error, and which cause transitions into or between different accident scenarios, are rarely explicitly identified, and the impact of their consequences is therefore missing from the model. Because, ultimately, PSA scenarios can be interpreted in terms of the availability/unavailability or configuration of the plant equipment, it can be argued that most possible scenarios are already imbedded in the structure of the logic model. However, as implied above, their frequencies are not estimated correctly unless the probabilities of transition between scenarios due to inappropriate actions have been factored in. These inappropriate actions are the errors of commission of most interest to the PSA analyst.

Quantification of HEPs

Several different approaches have been proposed for the estimation of human error probabilities. Most approaches are based on the premise that the HEPs can be expressed as a function of influencing factors, sometimes called performance shaping factors. It is in the approach to determining what are the key influencing factors, and characterizing the impact of those influences, that the differences lie. Some approaches explicitly address several performance shaping factors (Williams 1988; and Embrey 1984), while others pick out a small number of key factors (Spurgin et al 1990; Dougherty and Fragola 1988). It is generally true, however, that there is relatively little in the way of a firm theoretical basis for any of these models, although there may be some empirical support for their applicability.

In their defense, however, the models do have one major feature in common. They all attempt to increase the HEPs from scenario to scenario, as the scenarios become more demanding. In this way, an attempt is made to capture the scenario dependence of the error probabilities in a relative way.

A major issue associated with quantification is how to address probabilistic dependence. In many PSA models, several human interaction basic events may occur in the same accident sequence cutset, or scenario description. These events may not be independent; the probability of the second, third, etc., may be a function of whether the first failure event occurs. This dependence generally implies some shared cause, or influence factors. Current models do not address causes explicitly and have difficulty in addressing this dependence quantitatively. A consequence of ignoring this dependence is the possibility of inadvertently suppressing the importance of human responses in certain scenarios. It is true, however, that PSA analysts are aware of the possibility of such dependencies, and attempt, on the basis of certain guidelines, to identify the scenarios where such dependency exists, and to ensure that they are not screened out of the analysis too early (Wakefield et al., 1993).

GENERAL STRUCTURE OF A METHOD FOR THE ANALYSIS OF ERRORS IN A SYSTEM CONTEXT

One possible solution to address both the issues of dependency and errors of commission is to develop a human reliability analysis method that is based upon an explicit consideration of causes of error. This paper presents a possible approach to developing such a method.

It is assumed that the ultimate goal is to develop a predictive theory of errors as they are manifested in terms of the impact on the system. The theory should be

predictive not in the sense of identifying when an error will be made, but in having the capability of recognizing the signature of particularly error prone situations or scenarios and of providing a means of assessing the relative likelihood of the different error expressions in these different scenarios. The interface with a PSA systems model is in the definition of these error expressions, i.e., how the errors are manifested in the context of the system. There are several categories that could be considered, for example; a. inadequate response, which can be divided into no response, slow response, or premature response, or b. alternate response, of which there may be many possibilities. In general, as discussed earlier, only no or slow response are normally modelled in current PSAs.

The definition of an error expression is completed by specifying which specific equipment is affected and how. An error expression can, therefore, be equated with a failure mode of a piece of equipment or of a function. As will be seen in the following, this "error" in the timeframe of the operator interactions with the system is not necessarily an isolated point event, but more generally, corresponds to failure of a process.

For each error expression, the theory should recognize that there are different error modes, corresponding to proximate causes of the error expression, e.g., chose incorrect procedure, failure to see alarm, etc. An error mode is a quasi-phenomenological description of a failure mechanism as it is manifested in the interfaces between the operators and the system and/or information base. The error modes give some explanation of how the failure (or error expression) occurred and what the associated error was, but not why the error was made. Typically errors may occur in the operator information interface, in the formulation of a response, or in its execution.

The next level of detail involves identifying for each mode, error mechanisms or error causes which explain why the error occurs. It is assumed that it is appropriate to characterize human error occurrence in a probabilistic way, and that, for PSA purposes, this explanation may be best characterized in terms of scenario specific factors we will call performing influencing factors (PIFs).

Errors, in a PSA context, are, as stated previously, failures of a process, and that process, in most cases, allows recovery from an initial error, partly because the inertia of the system does not lead immediately to failure of vital equipment, or to an irreversible plant state, and the operators can receive feedback from the plant, affording them the opportunity to recognize and recover from errors. Therefore, in modeling human interactions, and estimating the probabilities of error expressions, it is therefore important to incorporate recovery mechanisms. Since different error expressions result in different system responses, the feedback to the operators will also be different, and will impact the potential for recovery. The potential for recovery is also a function of the error cause. For example, errors of intention are generally felt to be less likely to be recovered than are simple slips.

The above considerations suggest that a cause-based HRA model should recognize that the different error causing mechanisms may be affected by different PIFs and that they have different recovery potential. One model having some of these characteristics has been reported in Parry et al., (1992). In a model based on this concept, an error expression is the logical sum of contributions from several error modes, which in turn can result from several error mechanisms modified by appropriate recovery mechanisms.

This can be expressed symbolically as:

$$P(E|S) = \sum_{j} \sum_{i} \sum_{k} P_{ji}(S) P_{nr}^{jik}(S) \qquad -(1)$$

where P(E|S) is the probability of error expression E in scenario S, $P_{ji}(S)$ is the probability of mechanism i resulting in mode j in scenario S, and $P_{nr}^{jik}(S)$ is the probability of non-recovery from mode j, mechanism i via recovery mechanism k in scenario S. A scenario is a snap-shot of the system in terms of the status of its component parts and the parameters that are used to trigger the human interaction, and also of the influence factors that are judged to impact human performance (the PIFs).

DEVELOPING AN HRA MODEL

The key issue in developing an HRA model that fits into the framework described above is how to identify what (measurable) PIFs should be used to characterize the scenarios, and how to represent their impact on the HEPs. It is clear that PIFs will not be equal in their impact, and are not independent; for example, stress may be determined by the combined impact of factors such as workload, rate of change of plant parameters, etc. Other PIFs can influence each other by reinforcement, or they can counteract each other; for example, training is a good defense against unclear procedures. It should also be remembered that a PSA scenario is really representative of a population of possible realizations of that scenario and therefore the PIFs are also representative of average characteristics of that population.

While it may be possible, by studying data, to gain some understanding, of how PIFs should be measured and how they influence the propensity for errors, development of models of error mechanisms can provide considerable insights. In characterizing potential causes of error we need to identify both the internal mechanism (internal to the operator), which explains why he committed the particular error mode, and external causes representing events external to the operator that have an influence on his behavior.

To proceed further it is necessary to adopt a cognitive model. The model most in favor with HRA analysts (see for example, Cacciabue and Hollnagel, 1993) is that of Reason (1990). Briefly described, this model has two principal components, a working memory where potential solutions are evaluated, and the knowledge base which stores potential solutions. To create a predictive model applicable to a specific scenario it is necessary to characterize the knowledge base as it relates to that scenario (the signature of the scenario), and to specify the retrieval rules, and the evaluation rules.

In the analysis of common cause failures the concepts of trigger events, and conditioning events (Paula and Parry, 1990) have provided an useful approach to understanding historical events. Conditioning events create the conditions that increase the susceptibility of the system to failure, but the actual transition to failure requires some trigger event to occur. In the case of human error, this will have the utility of separating PIFs into those whose effects are established prior to the event and influence the structure of the knowledge base, and those which are related with the characteristics of the event and which affect the retrieval and evaluation process.

To illustrate how this model can provide guidance on how to identify appropriate PIFs, consider first an inappropriate action resulting from misdiagnosis. Based on Reason's hypothesis that the dominant cognitive primitives for information retrieval are similarity matching and frequency gambling, it is reasonable to propose that scenarios that are candidates for misdiagnosis are those whose signatures are similar to those of other more commonly experienced or expected scenarios. This model implies that for an error to occur there should be a common subset of factors that define the signature of the actual scenario, and that scenario erroneously assumed by the operator to be what he is responding to. Therefore, one of the PIFs for this PSA

model might be some comparative measure between the signature of the actual scenario, and that of the incorrectly identified scenario. In this way the PIF measures would differ for different error expressions, i.e., different misdiagnoses. Another PIF might be related to the relative frequency of training on the "related" scenarios. These are examples of conditioning PIFs. The trigger PIFs could be those that create conditions under which the similarity might be enhanced. Candidate PIFs are those which lead to obscuring or distorting some necessary information, or which force hurried decision as a result of information overload for example. These PIFs in contrast may be absolute rather than comparative measures.

PIFs associated with the recovery process must also be addressed. Recovery can be effected in many ways, e.g., (a) by another crew member performing an independent assessment, (b) by an alarm which draws the operator's attention to the fact that the initial response has not resolved the problem, or indeed has created a new one, (c) by monitoring the plant, allowing the operator to realize the result of the action he took is not in accordance with his expectations, and reanalyze the situation. These all involve information gathering, decision-making, and action. However, they are different in detail for the different recovery mechanisms. For example, in mechanism (c), information is gathered in a directed way, whereas in (b) it is not. Perhaps of more serious concern is the fact that for both (b) and (c), there is a danger that the same sort of error made initially in the decision mode, is propagated through the recovery opportunity. This would occur, for example, if there was a strong mind set that the original decision was correct, and that therefore something else must be wrong.

In any case, it is reasonable to suggest that the potential for recovery is, in some way, a function of the difference between the signature of the incorrect state and that of the correct state, or, for execution errors, that of the state the operator thinks the plant is in. In this case, some PIF measures should reflect the quality of the feedback and might be measured as a function of the difference in the signatures of the correct and incorrect scenarios.

To summarize, what we are suggesting is that investigating mechanics of error causation can provide potentially useful suggestions on how to characterize scenarios so that those that can potentially lead to error may be clearly identified. In particular, because it appears necessary to consider comparative measures to represent some PIFs, it is suggested that it is not sufficient, when considering error potential, to consider the characteristics of a scenario in isolation, but that those of potential alternate scenarios must also be considered. An example application of these ideas to the analysis of errors of commission is presented in Parry et al., 1994.

CONCLUSION

This paper has presented some ideas on the form of, and an approach to developing an improved HRA method for use in PSAs. This approach is based on an attempt to understand error causation in a detailed way.

The cycle of committing errors and recovering from them is a highly dynamic process, and a dynamic PRA approach is a valuable tool to investigate the characteristics of the operator model. One such approach is described in a paper at this conference presented by Professor A. Mosleh from the University of Maryland.

ACKNOWLEDGEMENTS

This work has been supported in part by EPRI under project number RP-8013-04. The author is grateful to Dr. D.H. Worledge of EPRI, and Professor A. Mosleh, C. Smidts, K.S. Hsueh, and S.H. Shen, at the University of Maryland for many conversations which have helped to shape the ideas expressed here.

REFERENCES

Cacciabue, P.C., and Hollnagel, E., 1993, Human models in reliability and safety analysis of interactive systems, *in:*"Proceedings of PSA '93", American Nuclear Society.

Dougherty, E.M., 1990, Human reliability analysis - where shouldn't thou turn? *Reliability Engineering and System Safety,* 29: 283

Dougherty,E.M., Fragola,J.R., 1988 "Human Reliability Analysis: An Engineering Approach with Nuclear Power Plant Operations", John Wiley, New York.

Embrey, D.E., et al., 1984, "SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgement," NUREG/CR-3518, U.S. Nuclear Regulatory Commission, Washington, D.C.

Parry, G.W. et al. 1991, "An approach to the analysis of operating crew responses using simulator exercises for use in PSAs", *in:*" Proceedings of the OECD/BMW Workshop on Special Issues of Level 1 PSA", GRS-86.

Parry, G.W., Julius, J.J., Jorgensen, E.J., and Mosleh, M., 1994, A procedure for the analysis of errors of commission in a PSA, *in: "Proceedings of this Conference."*

Paula, H.M., and Parry, G.W., 1990, "A Cause Defense Approach to the Understanding and Analysis of Common Cause Failures", NUREG/CR-5460, U.S. Nuclear Regulatory Commission, Washington D.C.

Reason, J., 1990, "Human Error", Cambridge University Press, Cambridge, England.

Spurgin, A.J., et al., 1990, "Operator Reliability Experiments Using Power Plant Simulators", 3 Volumes. EPRI NP-6937.

Wakefield, D.J., Parry, G.W., Hannaman, G.W., Spurgin, A.J., and Moieni, P., 1992, "SHARP1-A Revised Systematic Human Action Reliability Procedure", EPRI TR-101711, (licensable document).

Williams, J.C., 1988, A data based method for assessing and reducing human error to improve operational performance, *in* "Proceedings of IEEE 4th Conference on Human Factors in Power Plants, Monterey, California, 6-9 June.