PROCEEDINGS OF

PSAM — II

Volume 1

(Sessions 1 - 36)

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

San Diego, California, U.S.A.

March 20-25, 1994

PROCEEDINGS OF

PSAM — II

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

San Diego, California, U.S.A.

March 20-25, 1994

Editors

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

Contributing Editors

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

FOREWORD

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

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

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

The Editors

SPONSORED BY THE

Society for Risk Analysis

European Safety and Reliability Association

COSPONSORED BY THE

American Nuclear Society

American Society of Mechanical Engineers

IEEE Reliability Society

SPONSORING ORGANIZATIONS

Aerospace Corporation

APG, Inc.

ASCA, Inc.

Electric Power Research Institute

Idaho National Engineering Laboratory

Kazarians & Associates

Los Alamos National Laboratory

PLG, Inc.

PRC, Inc.

SAIC

Sandia National Laboratories

Scientech, Inc.

Tenera

Unocal Corporation

University of California, Los Angeles

University of Maryland

US Department of Energy

GENERAL PROGRAM CHAIRMAN

Michael G. Stamatelatos, Scientech, Inc.

ASSOCIATE GENERAL CHAIRMAN

Doug Orvis, Accident Prevention Group

SENIOR ADVISORY BOARD

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

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

CONFERENCE LOCAL ORGANIZING COMMITTEE

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

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

ORGANIZING STAFF

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

TECHNICAL PROGRAM COMMITTEE

CHAIRMAN

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

ASSOCIATE CHAIR

J.S. Wu, ASCA, Inc.

MEMBERS

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

CONTENTS

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

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

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

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

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

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

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

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

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

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

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

004 Dependent Failures

Chair: M. Haim, Rafael

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

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

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

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

005 Advances in Human Reliability Analysis

Chair: G.W. Parry, NUS

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

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

Human Reliability Analysis for Seismic Events

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

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

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

Application of HRA in the Commonwealth Edison Individual Plant Examinations

L. Soth (Commonwealth Edison)

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

Chair: N. Ortiz, SNL

Methodology to Evaluate Uncertainty in Thermalhydraulic Code Calculations

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

010 Computer-based Systems and Plant Models

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

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

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

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

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

011 PSA for Dynamic Systems: Modeling Approaches

Chair: M. Marseguerra, Univ. of Milan

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

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

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

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

Chair: G.W. Hannaman, SAIC

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

016 Uncertainty in Performance Assessment

Chair: M.G. Marietta, SNL

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

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

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

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

018 Reliability, Models & PSA

Chair: K. Inoue, Kyoto Univ.

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

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

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

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

019 Risk Management for Continuous Releases of Airborne Toxics

Chair: W.E. Kastenberg, UCLA

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

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

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

020 Applications for Process Operational Safety

Chair: F. Dombek, NUS

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

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

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

021 Management of Risk in Chemical Processes

Chair: G.D. Kaiser, SAIC

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

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

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

022 Risk Management in DOE (I)

Chair: K. Murphy, USDOE

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

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

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

023 Environmental Consequence Analysis

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

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

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

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

024 Computerized Monitors and Operator Aids (I)

Chair: A.J. Spurgin, Consultant

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

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

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

025 PSA for Dynamic Systems: Analysis Techniques

Chair: N.O. Siu, INEL

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

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

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

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

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

Chair: O. Svenson, Stockholm U.

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

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

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

027 Hazard Analysis in the Process Industries

Chair: T. Aldemir, Ohio State U.

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

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

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

028 Risk Management in Operations

Chair: M. Stamatelatos, Scientech

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

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

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

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

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

Chair: D. Okrent, UCLA

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

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

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

030 Uncertainities in Chemical and Physical Phenomenology-ConsequenceAnalyses

Chair: M.L. Brown, AEA Technol.

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

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

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

031 Computerized Monitors and Operator Aids (II)

Chair: L. Norros, VTT Finland

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

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

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

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

032 Methodology

Chair: L.R. Abramson, LANL

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

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

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

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

033 Team Skills and Group Processes in Human Reliability

Chair: D. Orvis, Accident Prevention Group

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

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

034 Reliability/Availability/Maintainability Improvement

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

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

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

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

035 Regulation and Legal Issues

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

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

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

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

036 Risk Management in DOE (II)

Chair: T. Eng, USDOE

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

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

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

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

Chair: S. Kaplan

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

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

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

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

038 Risk Assessment - Space and Missile Systems

Chair: S. Guarro, The Aerospace Corporation

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

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

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

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

039 Expert Judgment

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

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

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

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

040 Benefits of Understanding Human Errors in Complex Systems

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

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

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

041 Methods for Improved Operations of Nuclear Units

Chair: K. Jamali, USDOE

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

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

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

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

042 Time Dependent Effects

Chair: D.L. Kelly, INEL

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

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

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

043 Risk Communication to Professionals

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

048 Risk Assessment of Industrial Facilities

Chair: N. Sankaran, UNOCAL

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

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

049 External Events

Chair: S.T. Khericha, INEL

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

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

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

050 Risk Management in DOE (III)

Chair: R.R. Fullwood, BNL

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

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

Chair: D.R. Anderson, SNL

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

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

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

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

052 Software Dependability (II)

Chair: R. Mulvihill, PRC

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

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

053 Expert Judgment in Assessment Studies

Chair: M.A. Cunningham, USNRC

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

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

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

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

054 HRA, the Second Generation (I)

Chair: P.C. Cacciabue, JRC

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

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

055 Instrumentation and Control Reliability

Chair: R. Roberts, Ultramar

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

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

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

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

056 Risk Communication

Chair: R.A. Bari, BNL

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

057 Resource Planning and Value-Impact Applications

Chair: K. Klein, USDOE

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

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

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

058 Examples of PRA in Design Decisions

Chair: B. Buchbinder, NASA

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

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

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

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

059 Use of PRA Models in Assessing Technologies and Device Applications

Chair: M. Zentner, Westinghouse Hanford

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

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

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

060 HRA, the Second Generation (II)

Chair: E. Hollnagel, Computer Resources Intl.

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

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

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

061 Transportation Risk (I)

Chair: T. Altenbach, LLNL

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

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

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

062 Environmental Risk Management--Waste

Chair: C. Peabody, USDOE

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

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

063 Methods for Uncertainty Analysis (II)

Chair: A. Camp, SNL

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

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

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

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

064 Risk Based Prioritization

Chair: G.E. Cummings, LLNL

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

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

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

065 Meaning and Interpretation of Probability

Chair: A. Mosleh, U. Maryland

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

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

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

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

066 Cognitive Modeling and Simulation in Human Reliability Analysis

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

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

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

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

067 Comparative Risk Assessment of Complex Technological Systems (I)

Chair: S. Haddad, New South Wales Govt.

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

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

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

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

068 Risk Assessment Failure Data Estimation

Chair: C. Fleming, PLG

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

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

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

069 Waste Risk Management

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

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

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

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

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

070 Reactor PSA Studies

Chair: M. Hitchler, Westinghouse Savannah Rvr.

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

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

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

071 Accident Precurssors

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

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

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

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

072 Aging Analysis: Methodology & Applications

Chair: D.H. Johnson, PLG

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

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

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

073 Human Reliability Applications and Models

Chair: S. Kondo, Tokyo Univ.

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

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

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

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

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

074 Comparative Risk Assessment of Complex Technological Systems (II)

Chair: S. Hirschberg, P. Scherrer Inst.

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

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

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

075 Fire Risk Analysis for Enineered Systems

Chair: R. Friedman, NASA Lewis

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

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

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

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

076 Risk-Based Regulation (I)

Chair: V. Joksimovich, Accident Prevention Group

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

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

078 Process Safety Management

Chair: R.L. Cummings, Interstate Assessment Technologies

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

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

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

Chair: F.R. Hubbard, FRH

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

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

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

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

080 Understanding Organization Factors Through Risk Models

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

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

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

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

081 DOE Safety Studies

Chair: R.E. Hall, BNL

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

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

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

082 Fires, Floods, and Spatial Interactions

Chair: R. Oehlberg, EPRI

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

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

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

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

083 Environmental Restoration Decision Support System

Chair: D. Rice, LLNL

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

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

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

084 Reliability Based Design in Structural Engineering

Chair: D. Frangopol, U. Colorado

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

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

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

085 Transportation Risk (II)

Chair: M. Kazarians, Kazarians & Assoc.

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

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

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

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

Chair: J.H. Bickel, INEL

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

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

087 Causal Factors in Human Reliability: Experiments and Databases

Chair: A.A. Dykes, PLG

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

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

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

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

088 Risk Based Methods for Reliability/Availability/Maintainability

Chair: S. Lydersen, Norwegian Inst. Technol.

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

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

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

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

089 Seismic Risk Analysis

Chair: D.A. Moore, Primatech

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

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

090 Risk Based Regulation (II)

Chair: G. Apostolakis, UCLA

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

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

091 Management Issues

Chair: D. Cunha, Northrop Corp.

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

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

092 Industrial and Transportation Risks

Chair: D. Henneke, TENERA

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

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

Identification and Evaluation of Maritime Exposures

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

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

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

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

Chair: D. Bley, PLG

On a Class of Dependent Failures

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

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

K. Porn (Studsvik Eco & Safe)

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

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

094 Applications of Human Reliability Analysis

Chair: D.I. Gertman, INEL

HRA for Explosive Ordinance Disposal

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

Nuclear Case Study for A SGTR Sequence

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

Insights into Pilot Situation Awareness Using Verbal Protocol Analysis

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

095 Risk Methods for Defense Applications

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

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

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

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

096 Risk Communication to the Public

Chair: M.E. Paté-Cornell, Stanford U

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

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

097 Broad Risk Perspectives Within the DOE Weapon Complex

Chair: H.P. Alesso, LLNL

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

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

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

098 Risk Management - International Space Applications

Chair: C. Preyssl, European Space Agency

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

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

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

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

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

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

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

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

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

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

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

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

101 Risk Assessment of Nuclear Waste Storage and Processing

Chair: D. Stack, LANL

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

102 Fire Risk

Chair: V. Ho, PLG

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

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

103 Risk-Based Regulation (III)

Chair: F. Rahn, EPRI

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

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

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

104 Industrial Risk Management - An EEC Perspective

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

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

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

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

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

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

105 Environmental Risk Management--Restoration

Chair: T.E. McKone, LLNL

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

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

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

106 Data Collection and Evaluation

Chair: D. Croucher, EG&G Rocky Flats

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

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

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

107 Organizational Factors and Nuclear Power Plant Safety

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

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

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

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

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

108 Interactive Fault Detection and Diagnosis--Approaches

Chair: A. Poucet, ITER EDA

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

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

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

020 Applications for Process Operational Safety

Chair: F. Dombek, NUS

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

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

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

SYSTEM-BASED APPROACH TO SAFETY EQUIPMENT CLASSIFICATION FOR A RADIOCHEMICAL FACILITY.

Mr. Sixto T. Almodovar and Ms. Cheryl L. Whalen

Jason Associates Corporation
12625 High Bluff Drive
San Diego, CA 92130

INTRODUCTION

The safety class of a piece of equipment (system, component, part, etc.) has a high impact on its cost and operation. Hence, there is always a strong motivation to classify a piece of equipment at the lowest possible Safety Class that will not jeopardize the overall safety of the facility.

The most common approach to safety equipment classification is a deterministic ***barrier*** methodology which relies primarily on engineering judgement and on passive barriers over an unspecified, but usually very long, mission time. A ***system-based*** approach is proposed in this paper which offers some advantages over the ***barrier*** approach. These advantages may be of even more significance as requirements for evaluating hazardous material safety impacts are addressed. Many of the Department of Energy (DOE) facilities located in Washington (Hanford), Colorado (Rocky Flats), and other states are radiochemical facilities which contain both radioactive and hazardous materials, as opposed to power plants where the significant hazards are usually limited to radioactive materials.

DETERMINISTIC APPROACH TO SAFETY EQUIPMENT CLASSIFICATION

In performing a safety classification using the barrier-based approach, the bases of the safety equipment classification process are ***barriers*** whose safety functions and/or environmental protection functions keep hazards away from the public, the workers and the environment.

Barriers can include items like tanks, filter banks, isolating valves, drains, check valves, other types of valves, continuous air monitors among others. An example of these barriers is shown in Figure 1. The functions of these barriers can be any or all of the following:

1. CONTAINMENT/CONFINEMENT of hazards,
2. PREVENTION/CONTROL of hazards, and
3. MONITORING of the hazardous releases, but not usually monitoring of the hazard barrier state, degradation, or conditions.

The safety equipment classification process using the ***barrier*** approach is:

1. Deterministic;
2. Unrelated to mission time;
3. Based on passive barriers, where no credit is taken for active systems used to mitigate the accident or recover from it (these mitigation systems are handled separately, as part of the barrier classification);
4. Based on engineering judgement; and
5. Independent of operator actions to correct or mitigate the accident.

There are wide variations in the safety equipment classification methods used from one facility to another because of differences in corporate safety culture, independent of the potential consequences of the equipment failure. Nuclear criticalities are often given the highest safety class available even though the consequences in terms losses may not be justify this classification and accidents involving hazardous materials have often been overlooked, even though the consequences may be more severe than those involving radioactive materials.

Once an initiating event has been identified, either as a natural phenomena initiating event, or as a "credible" accident scenario initiating event, the safety equipment classification process using the ***barrier*** approach then looks at the consequences of a postulated failure of the next, single barrier <u>without</u> considering:

1. The barrier's frequency of failure;
2. Operator action during the accident sequence (accident mitigation by the operator);
3. Operator action after the accident sequence (accident recovery by the operator); or
4. The actions of any engineered safety systems.

The barrier is then classified according to the <u>consequences</u> which might potentially result from its failure.

The classification process does consider a "legitimate pathway to the environment" through the various barriers depending on the barriers' presence, design, seismic qualifications, etc.

Some of the short-comings of this approach are:

1. "Credible" in this approach is based on subjective engineering judgement. There is no numerical guidance as to what is credible. Equipment failure frequency and event sequence frequency are not considered explicitly.

2. There is no good way to handle "slow" accident precursors. Equipment whose deterioration may lead to an accident is usually included in the classification process even though the equipment may take months or years to deteriorate.

SYSTEM-BASED APPROACH TO SAFETY EQUIPMENT CLASSIFICATION

In performing a safety classification using the ***system-based*** approach, it is acceptable to group (i.e., postulate the failure of) several barriers in sequence, in order to find an "effective", "credible" cause of release, or "effective", "credible" initiating event. "Credible" is a given numerical value, typically, a failure mode or type with a frequency of greater than 10^{-6} /year is deemed "credible". An illustrating example is:

> For a given earthquake, the annual frequency of a catastrophic leak from a steel tank holding a toxic hazard is given as 10^{-3}. The steel tank is inside a concrete tank whose annual frequency of a catastrophic leak is 10^{-2}. The steel tank and the concrete tank are not designed to withstand the postulated earthquake. However, both tanks are inside a steel containment building which has been design to withstand the earthquake.

If the management of the facility in this example:

1. Defines the function of its highest Safety Class (Safety Class 1) to protect the public from the consequences of a release of radioactive or environmental hazards;

2. Defines the function of its Safety Class 2 to protect the workers from the consequences of a release from the same radioactive and environmental hazards; and

3. Uses Non-Safety Class for all others,

then one approach to this sequence of events would be to classify the steel tank and the concrete tank as Safety Class 2 (or perhaps even Non-Safety Class), and then classify the steel containment building as Safety Class 1. This assumes that the consequences (due to amount, toxicity, etc.) of releasing the hazardous material fall in the Safety Class 1 category.

This is the preferred approach using the ***system-based*** methodology. This approach does offer flexibility. This approach can be used to contain costs for a project, while ensuring the safety of the project. Or if added safety is desired or required, a different definition for the Safety Class requirements can be used. Another way of looking at this example process would be to classify the steel tank, the concrete tank and the steel

containment building as Safety Class 1 systems and structures. This calls attention to the design and instrumentation of the two inner tanks and adds to the concept of defense in depth by multiple barriers. This classification approach assumes that during the earthquake, both the steel tank and the concrete tank will fail. To the steel containment building, this sequence of events "looks effectively" like a "credible", single initiating event. It does not "look" like a two event sequence.

Typically a facility could use the first ***system-based*** approach to classify the equipment as protecting workers, the public and environment, while maintaining lower costs. The second approach then gives a direct measure of the added costs for the higher level of confidence implicit in the approach.

As requirements for including accidents involving hazardous materials are implemented the time required and cost of using the ***barrier*** approach is rising dramatically. A hazardous material is defined to be any substance, whether it is a waste or not, which is capable of harming the public, the workers, and the environment because of its radioactive or chemical properties.

A hazardous material, therefore, is any of the following:

1. Any Comprehensive Environmental Responsibility, Compensation, and Liability Act (CERCLA) hazardous substance as identified in 40 CFR 302.4;

2. Any Environmental Protection Agency Emergency Planning and Community-Right-to-Know Act (EPCRA) extremely hazardous substance as identified in 40 CFR 355, Appendix A;

3. Any dangerous waste or hazardous substance defined and regulated by the state or local agency charged with protection of the environment for the specific location of the facility; or

4. Various oil and petroleum products.

The wide range of materials defined as hazardous and the number of defining agencies and regulations will added significantly to the difficulties and inadequacies encountered using the ***barrier*** approach for radiochemical facilities.

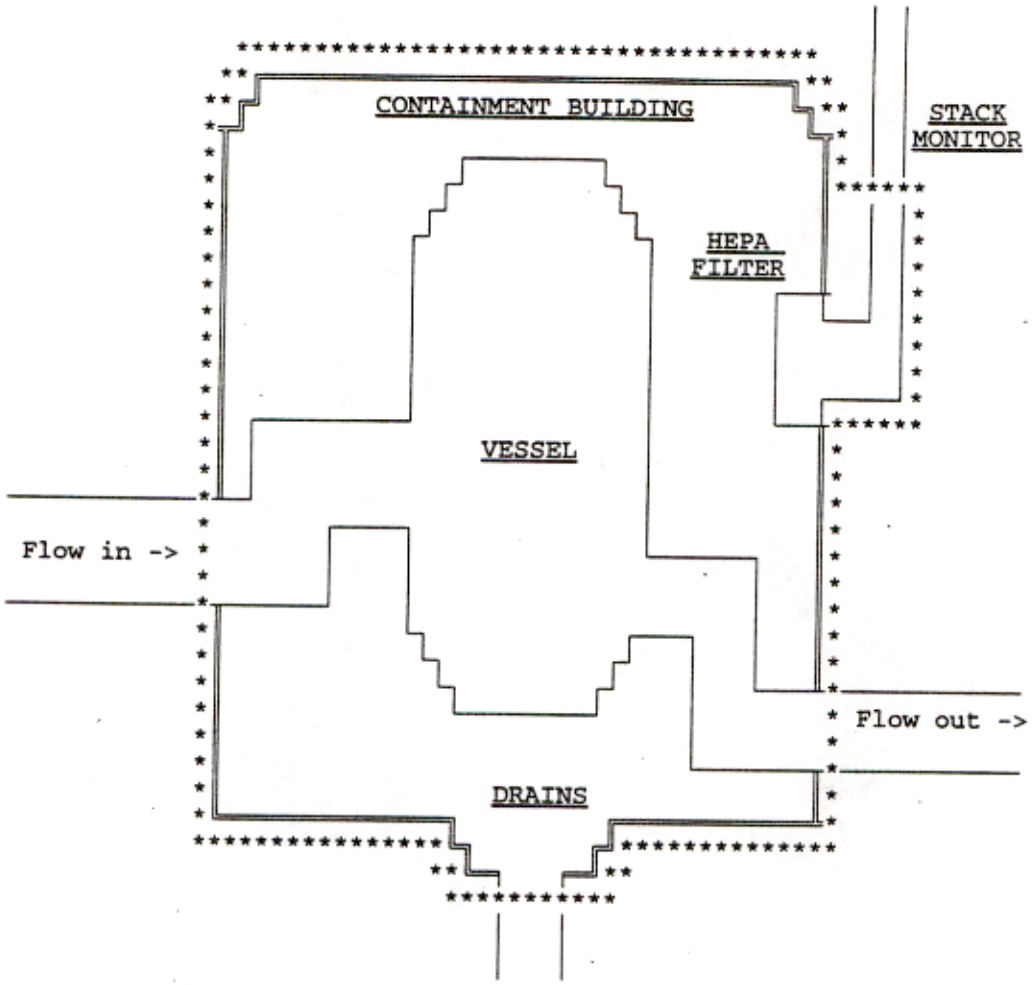


Figure 1. Safety Equipment Classification

All penetrations and systems which breach the barrier (depicted by *) are the same safety class as the (containment, confinement) barrier they breach.

A PROBABILISTIC RISK ANALYSIS OF AN LPE LABORATORY

Shimshon Arueti[1] and Michael Mor[2]

[1]RAFAEL Reliability Center
[2]SCD, An ELOP–RAFAEL Partnership
P.O. Box 2250
Haifa, Israel

INTRODUCTION

This paper addresses an application of Probabilistic Risk Assessment (PRA) methodology and PRA tools for a small scale analysis. It represents the combined effort of a safety analyst and a domain specialist (i.e., the laboratory's most experienced technician).

The objective of this assignment was to qualitatively and quantitatively, via PRA, analyze the main contributors to, and the probability of a safety related event in an LPE laboratory. Three major events were considered:

- LABEXP: A large Hydrogen explosion in the laboratory
- LOCALEXP: A local reactor or bubbler explosion
- LABFIRE: A large fire in the laboratory.

The analysis provides low–cost–high–consequence conclusions and recommendations, which, upon implementation, will reduce the laboratory technician's operation risk by almost two orders of magnitude.

THE LPE PROCESS

Liquid Phase Epitaxy (LPE) is a thin layer growth technology for the microelectronics industry which has been known for over twenty years. The technology is based upon the broad use of Hydrogen gas as a major carrier in the growth process. The Hydrogen is necessary mainly to ensure the purity of the process materials and to prevent them from oxidation.

Figure 1 below describes the process flow and the major laboratory components. The heart of the laboratory is a glass reactor in which the growth process takes place. The reactor environment is heated by a furnace. The hydrogen source is a high pressure tank located outside the laboratory. The used hydrogen exits the system through a bubbler and is burned before being released to the atmosphere.

The main source of concern in laboratory operation is a hydrogen leak, which becomes an explosive mixture when combined in high concentration with oxygen.

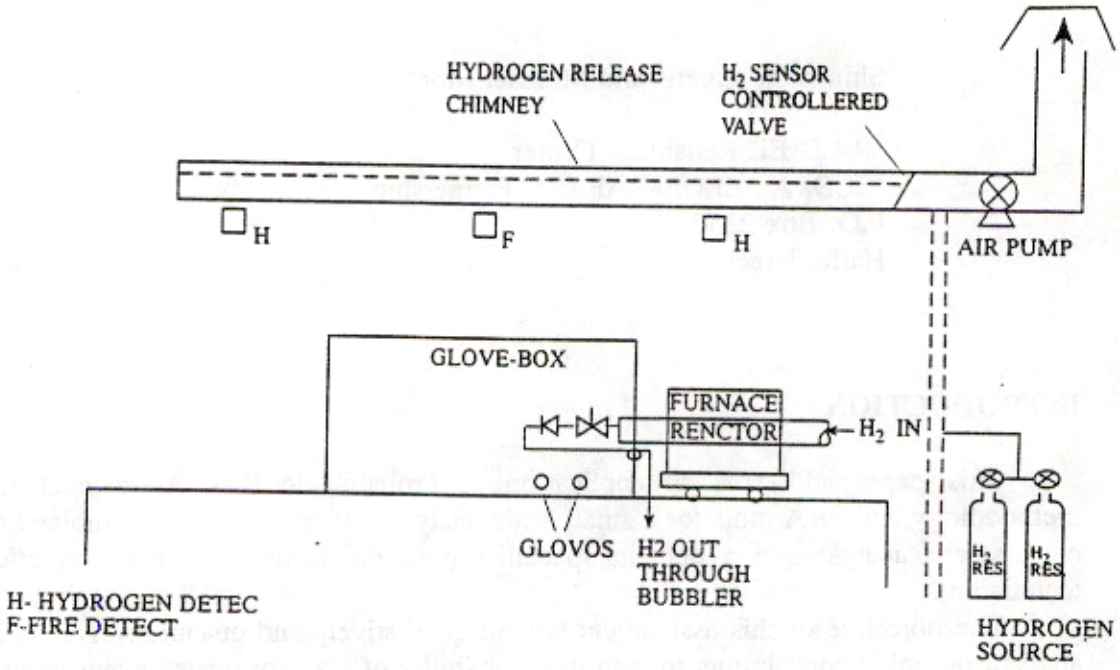


Figure 1. LPE process flow diagram.

LABORATORY SAFETY FEATURES

Some of the important safety related features in the laboratory are listed below:

- The piping and valves used to control the process are located in a glove box (GB). The GB environment is constantly monitored to detect excessive pressure and hydrogen concentration.
- Laboratory air is constantly pumped out by an electric blower.
- Hydrogen concentration in the laboratory atmosphere is monitored by a system which increases the blower's rate if H_2 is sensed above a certain threshold concentration.

USE OF PRA TOOLS

The main analysis tools, i.e., event trees (ETs) and fault trees (FTs), are no different than those used for the analysis of large systems such as nuclear power plants (NPPs), but the method of application is quite different. In this application the use of these tools and the data gathering process were simplified.

In NPP PRAs, ETs are used as qualitative and quantitative tools for plant analysis. FTs are used for system analysis, i.e., for qualitatively and quantitatively analyzing each of the ET top events. The analysis of a relatively simple system such as the LPE

laboratory did not require such a complex analysis. Nevertheless, we found the application of both techniques very useful. ETs were applied as a qualitative tool for two major purposes:

- For tracking event sequences, from initiating events to system failure modes. In that sense they replaced event sequence diagrams as a structured method for guiding the analyst through all the subsystem success/failure combinations.
- For constructing FTs, which were then used as a tool for the quantitative analysis. The safety related consequences identified in the ET became FT top events and ET sequences were translated into FT cut–sets.

This method of analysis, combined with simplified data analysis, has several important advantages. It is fast and inexpensive to implement and thus is not an obstacle to the laboratory design and construction process. The close cooperation with the laboratory operators and the simplified analysis procedure, made the results clear and acceptable to management. As a result analysis findings were incorporation in the laboratory in real–time.

METHOD OF ANALYSIS

Initiating Events and Event Trees

The first major step in the analysis was the construction of three event trees, one for each of the following initiating events:

- Pipe (or piping device) leakage.
- Uncontrolled Hydrogen release from the GB.
- Failure of the reactor or bubbler.

The event tree for reactor or bubbler failure is presented in Figure 2 below.

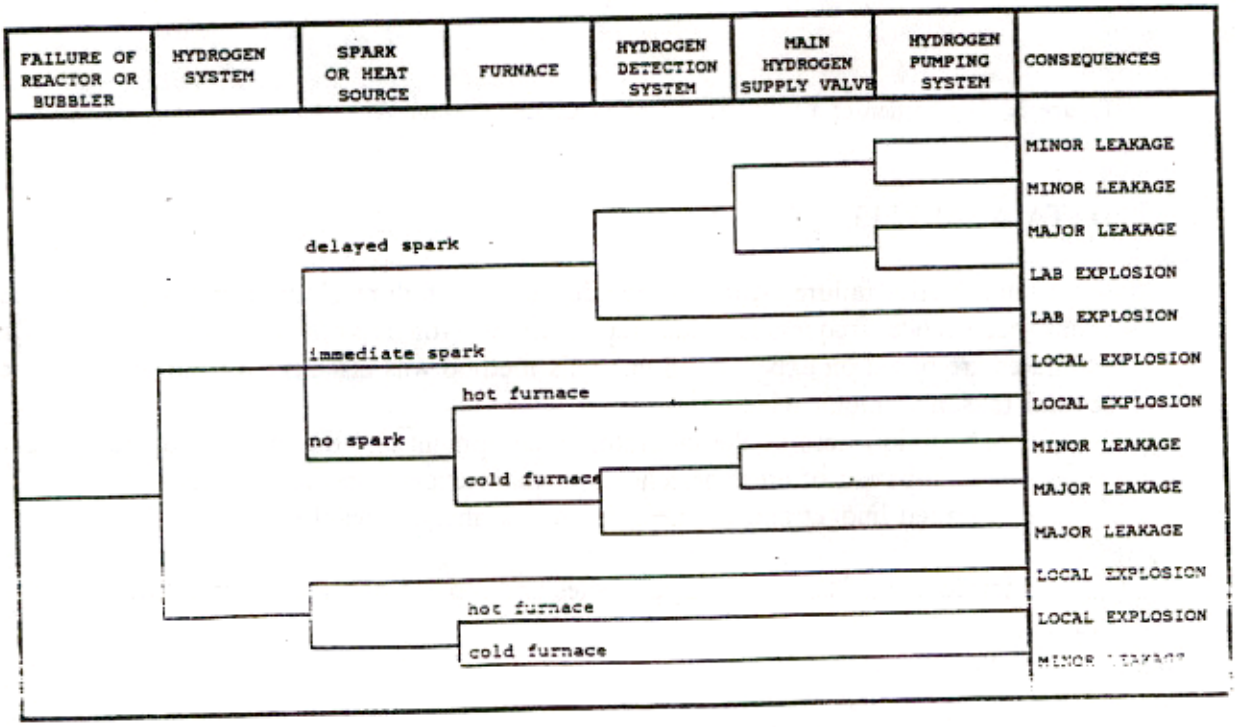


Figure 2. Event tree for the initiating event "reactor or bubbler failure".

At the next major step, safety related events of interest were identified. These events were then quantitatively analyzed via FTs. The FT top events were chosen from the possible consequences in the ETs. The three events listed in the Introduction as the main risks of concern were then identified and used as FT top events. The FT for the top event LOCALEXP is presented in Figure 3.

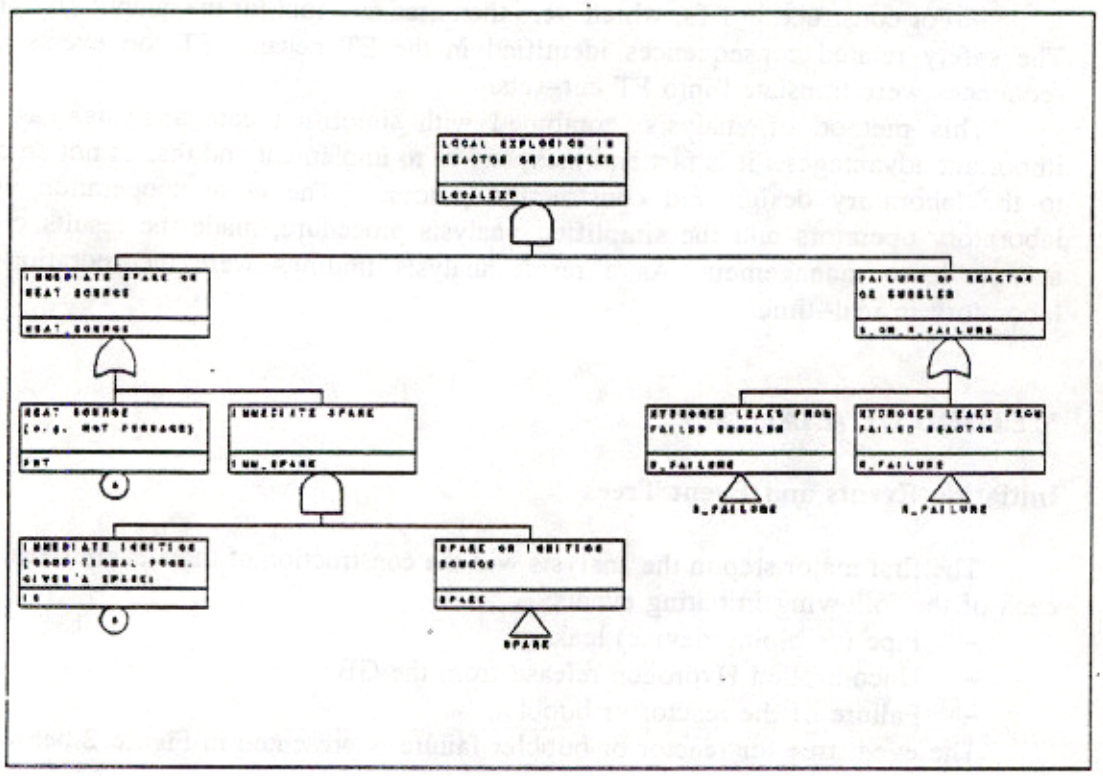


Figure 3. Top portion of a fault tree for the LOCALEXP event.

DATA ANALYSIS

Quantitative failure estimates include hardware failures, human errors and other basic event occurrence frequencies and repair times (for repairable components). These estimates are based on expert opinion. This method was effective for our analysis due to several reasons, among which are:

- The uniqueness of the laboratory's equipment and the lack of "objective" data.
- Participation of an experienced "domain expert" in the analysis.
- Limited budget and the need for quick analysis results.

Therefore, the basic event frequencies and repair times are the result of a three-step process:

- Primary expert estimates.
- Experts' verification.
- Consistency check by the safety analyst and the domain expert team.

Many of the failure rates and repair times were derived from actual failures experienced in the laboratory over the past twenty years (e.g. hydrogen detection system failures and some human errors.) Other estimates are purely based on conservative expert judgement.

QUANTITATIVE ANALYSIS

The fault trees were quantified with three products in mind:

1. Estimation of the frequency of occurrence of each of the three top events.
2. Identification of major contributors to risk.
3. Proposal of measures for reducing risk.

The second product was derived via Importance analysis. Based on its results some simple measures were proposed, which considerably reduced the predicted top event occurrence frequencies. LABEXP's frequency, for example, was reduced by two orders of magnitude.

CONCLUSIONS AND RECOMMENDATIONS

Recommendations derived from the analysis results are of two major classes:

- Addition of safety devices or improvement of existing ones. These include a flow limiter, a needle valve to create a constant leak from the GB to the atmosphere (outside the laboratory), shields to protect the reactor and the bubbler from falling objects and from human errors, active hydrogen detectors for the GB and for the laboratory's atmosphere (e.g., by an audio signal), and improved anti-spark protection to all electrical devices.
- Some improvement in procedures and in operator training, to raise awareness to human errors.

As a final note, one can draw an encouraging conclusion from the analysis results. A significant improvement in safety has been reached by an inexpensive analysis procedure. More importantly, the recommended safety means were simple and inexpensive and their importance could be appreciated only as a result of such a structured analysis.

Close cooperation between the safety analyst and the domain expert was crucial not only to the effective derivation of safety recommendations, but also to the acceptance of the results by the Customer, and to their quick and effective implementation.

HANFORD HIGH LEVEL WASTE (HLW) TANK MIXER PUMP SAFE OPERATING ENVELOPE RELIABILITY ASSESSMENT

Stewart R. Fischer

Probabilistic Safety Assessment Section
Engineering and Safety Analysis Group
Nuclear Technology and Engineering Division
Los Alamos National Laboratory
Los Alamos, New Mexico 87545

James Clark

Science & Engineering Associates
6100 Uptown Blvd., N.E.
Suite 700
Albuquerque, New Mexico 87110

INTRODUCTION

The US Department of Energy and its contractor, Westinghouse Corp., are responsible for the management and safe storage of waste accumulated from processing defense-reactor irradiated fuels for plutonium recovery at the Hanford Site. These wastes, which consist of liquids and precipitated solids, are stored in underground storage tanks pending final disposition.

Currently, 23 waste tanks have been placed on a safety watch list because of their potential for generating, storing, and periodically releasing various quantities of hydrogen and other gases. Tank 101-SY in the Hanford SY Tank Farm has been found to release hydrogen concentrations greater than the lower flammable limit (LFL) during periodic gas release events. In the unlikely event that an ignition source is present during a hydrogen release, a hydrogen burn could occur with a potential to release nuclear waste materials. To mitigate the periodic gas releases occurring from Tank 101-SY, a large mixer pump currently is being installed in the tank to promote a sustained release of hydrogen gas to the tank dome space.

An extensive safety analysis (SA) effort was undertaken and documented to ensure the safe operation of the mixer pump after it is installed in Tank 101-SY.[1] The SA identified a need for detailed operating, alarm, and abort limits to ensure that analyzed safety limits were not exceeded during pump operations. To further ensure that pump operations were being carried out safely, the Los Alamos National Laboratory Engineering and Safety Analysis Group Probabilistic Safety Assessment Section has reviewed the mixer pump initial, or Phase A operations, to determine the conditional probability of exceeding a prescribed set of safe operating envelope (SOE) boundaries. These boundaries were defined to be the operating, alarm, and abort parameters as monitored by mixer pump and other in-tank and ex-tank instrumentation and as specified by Chap. 6 of the mixer pump SA, operating procedures, and preprogrammed abort and alarm limits for pump operation.

The SA assessment was intended to identify any credible single or multiple failures that would result in an unacceptably high probability of exceeding instrument-monitored operating limits. This review only analyzed the conditional probabilities of failure to remain within the SOE per pump operation as defined by instrumentation alarm and abort limits during the short-duration Phase A pump operations. No consideration was given to the likelihood of individual initiators nor to coupling them to the conditional failures required to lead to conditions outside the SOE boundaries. Similarly, we did not consider the consequences of possible failures in this assessment.

METHODOLOGY

A fault-tree approach was used to assess the potential failure for key control parameters that were implemented procedurally or controlled with the computer-based Data Acquisition and Control System (DACS). The assessment considered potential failures in both manual and automatic abort functions, as well as human errors and hardware failures during startup (i.e., preexisting conditions) and operating phases. Numerous assumptions were made in developing the fault trees; a primary one was that the reliability assessment represented a "snapshot" in time (with respect to procedure development) and is only applicable to Phase A testing. Fault-tree quantification was based on generic hardware failure data and on THERP[2] human reliability techniques.

Because of the nature of the fault-tree analysis used in this assessment, a strong dependence on the operating procedures was inherent. This dependence also meant that subtle changes in procedures may render the fault-tree analysis incorrect or inadequate; thus, for the purpose of this analysis, four procedural documents were used.[3–6] These procedures had been approved by the Westinghouse Hanford Company (WHC) Test Review Group (TRG) and were the most recent procedures available at the time of this analysis. In these procedures, there are automatic pump aborts with manual abort backup, manually directed pump aborts with and without automatic alarm indications, and requirements to prohibit pump operation based on preexisting conditions and instrumentation readings. The SOE fault tree was structured around these considerations. Where system details were uncertain, we attempted to apply conservative assumptions and to document such modeling.

Operator training sessions, in which the DACS was used as a training simulator with a variable-speed drive and a motor simulator were observed to help quantify human error probabilities. These observations also identified several significant areas where human actions could defeat the instrumentation and abort protective logic established in the SA easily. These items, which resulted from the flexibility of the DACS system, included capabilities to easily disable aborts and to place instrumentation into a "manual," or instrumentation signal bypass, mode. Additionally, our understanding of the DACS/operator control process was enhanced through numerous detailed conversations with test engineers, DACS engineers and technicians, and safety analysts.

The scope of this reliability analysis included a review of both the DACS design as well as the interface between DACS and the test engineers or operators. The DACS system interfaces with all in-tank, ex-tank, and pump instrumentation and provides data monitoring, recording, and control of pump operation. This effort focused on the alarm and abort parameter monitoring and operational controls that ensure that the SOE is not exceeded.

RESULTS

The overall results of the fault-tree analysis indicated that the conditional (i.e., assuming all initiating events are equally likely with a probability of a specific initiating event being 1.0) probability of operating outside the SOE is dominated by human error. Implementation of extensive operational/safety controls defined by Chap. 6 of the SA have resulted in detailed procedural requirements. These procedural efforts have helped to reduce the potential for human/operator error significantly. However, the Phase A test procedure,[3] coupled with the highly versatile and flexible DACS system, still provides numerous opportunities for inadvertent human error. Despite numerous single failures, the number of actual hardware failures that could conditionally result in the SOE being exceeded is relatively small.

Selected Qualitative Insights

Because of the iterative nature of this reliability assessment (which started before the development of the test procedure), numerous insights and recommendations evolved that resulted in design and administrative changes. Some of our qualitative insights include the following.

1. A preliminary failure mode analysis of the DACS/operator system and control hardware [the variable speed drive (VSD) and instrumentation] was performed with respect to control of pump speed and test duration. In addition, a high-level fault tree of the DACS hardware control functions was coupled with operator actions to provide qualitative insight to mixer pump control. This review indicated a possible single failure of the VSD speed-sensing circuit that could result in pump overspeed. A single speed sensor was used to provide speed indication for monitoring and control purposes on DACS; it also was used by the VSD to control pump speed. To remedy this situation, a backup-motor frequency readout was installed in the DACS trailer, and it will be used to provide independent monitoring of pump speed.

2. The assessment identified possible communication delays associated with the DACS computer that could result in timing delays (up to 10 s or more) associated with pump shutdown actions. To remedy this problem, the final system design controls pump operation timing and provides alarms and abort signals from the programmable logic control (PLC) units, which have adequate frequency response.

3. The assessment suggested that possible single failures of the DACS timer circuit could result in extended pump run times unless backup timing is provided. To remedy this situation, an operator will monitor DACS control of the pump via independent readouts of time (stopwatch) and pump speed. The operator is required by the Phase A test procedure to abort the test if either of these parameters exceeds established limits.

4. The assessment indicated the need to establish a "Minimum Instrument List" to ensure that primary and backup instrumentation for maximum waste level, rate of level rise [i.e., radar gauge/Food Instrument Corporation (FIC) gauge], waste density [i.e., redundant Velocity Density Thermocouple Trees (VDTT) strings], etc. are fully operational during testing.

5. The preliminary assessment indicated a need to ensure that administrative controls for setting the maximum speed, the alarm/abort limits, and all operating limits are implemented. Acceptance test procedures have been implemented to provide assurance that instrumentation is functioning and that alarms and abort limits are set properly.

Numerous other insights identified specific problems for which corrective actions in the form of hardware, software, or administrative changes were taken.

Quantitative Insights—Individual Control Parameters

Numerous single hardware failures for individual sensor circuits were identified; however, their failure probabilities are in general less than 10^{-4}. In addition, operator errors are associated with each individual circuit or prestart calculation that could lead to failure of a given sensor circuit or failure to secure startup of the mixer pump without proper verification of prestart conditions. Both the preexisting failure of each instrumentation circuit and the failure of the operator to correctly verify prestart conditions before mixer pump operation dominate the individual sensor circuit or calculation failures. In addition, human errors associated with programming and set point entry errors contribute significantly to individual circuit failure. Table 1 shows the conditional failure probability for each individual test control parameter (i.e., each control parameter is considered separately). Each control parameter probability is the sum of the individual fault-tree cut sets for each parameter modeled. The manual abort item in Table 1 includes preexisting and operational

Table 1. Conditional failure probability of individual Phase A SOE test parameters

Parameter	Conditional Total Failure Probability
Automatic Aborts	
2/3 Vent Flow Split (SY-102, 103)	1.0e-02
Tank Level High	5.4e-04
Motor Amps	5.1e-04
Pump Speed	4.8e-04
High/Low 101-SY Vent Flow	3.0e-04
Column Pressure	2.3e-04
VDTT Strain	1.6e-04
Discharge Pressure	7.5e-05
MIT Strain	6.4e-05
Oil Moisture	6.2e-05
Column Strain	5.8e-05
Hydrogen Concentration High	5.6e-05
Pump Vibration	5.4e-05
Oil Temperature	5.3e-05
Dome Pressure	3.6e-05
Waste Temperature	2.7e-05
Pump Flow	1.7e-05
Test Time	6.3e-06
Manual Aborts	
Foaming	1.0e-02
Hydrogen Concentration Low	3.0e-03
Dome-to-Ambient ΔT	1.0e-03
Level Rise Rate	1.0e-03
Operator Fail to Abort on Alarm	7.0e-04
Operator Fails to Verify No Adverse Weather	1.0e-04

failure probabilities for the following items: the dome-to-ambient-temperature difference; the low initial hydrogen concentration; the level rise rate; the waste density; the weather conditions; and foaming. The single largest contributor to the manual abort failure probability is failure of the operator to monitor the camera during the short Phase A tests. Also, no significant cut sets appear for waste density because of extensive redundancy of this parameter.

As summarized in Table 1, conditional sensor/circuit failures range from 1.0E-2 to 6.3E-6, depending on the individual parameter. For some sensor/circuit failures, recovery by the operator may be possible before the SOE is exceeded. This is particularly true if the evolving condition is slow in its rate of progression toward exceeding the SOE condition. An example would be waste tank temperature, where because of the total mass of waste, temperature rise rates generally would be expected to be slow. This could be contrasted with the mixer pump speed circuit, which could see a rapid rate of rise in speed, and thus, the operator would have very little time to react to an evolving situation. However, no credit has been given to the relative factors. It is interesting to note that those circuits where failure probabilities are less than 1.0E-4 generally are dominated by a single failure or a few operator errors, whereas those where failures are greater than 1.0e-04 are dominated by operator errors. Finally, as was previously mentioned, giving no credit for redundancy in similar types of conditions monitored (i.e., speed, pump flow, pump current, etc.) introduces additional conservatisms into this analysis. No attempt has been made to correlate sensors to fundamental parameters monitored.

The conditional failure probability of individual sensors and associated circuits is dominated by operator errors such as misreading instruments or miscalculations during the 2/3 vent flow calculation, the level-rise calculation, or the dome-to-ambient-temperature-difference calculation. In addition, dominant contributors include failure of the operator to monitor and discover foaming, failure of the operator to verify that weather conditions are adequate before pump operation (the product of two operator errors), failure of the operator to shut the system down upon reaching an abort limit, preexisting loss of control power to mixer pump interrupt circuit breakers, and miscalibration of sensors and associated circuits. Preexisting hardware failures of individual sensors, I/Os, I/O power supplies, alarm and abort circuits, and the video camera are significant contributors to conditional failures.

Finally, some common-cause failures contribute slightly to circuit failures. These consist primarily of common-cause miscalibration of sensors/circuits, a common-cause DACS programming error; a preexisting common-cause failure of both PLCs; and, a preexisting common-cause failure of some sensors as is, low, or intermittent.

Quantitative Insights—Total System Reliability

Table 2 presents the dominant cut sets and the total conditional failure probability for these test control parameters to remain within the SOE given an initiating event. Table 2 includes common-mode failures such as power supply or PLC failure, which would disable groups of instruments.

The total conditional failure probability for Phase A tests to remain within the SOE was computed to be 0.027. Table 2 lists the dominant cut sets or failure modes, which contribute over 95% of the total conditional failure probability. Including calibration errors for 9 sensors contributes an additional 3.3% of the total conditional failure probability. As discussed before, operator errors associated with detecting out-of-range preexisting conditions during prestart checks dominate. Given equal probability of an initiating event, the failure to identify abnormal ventilation flow (i.e., the 2/3 flow split calculation) has the highest conditional probability for failure to remain within the SOE during the prestart phase. For the pump operational phase, the failure of the operator to monitor the video camera and abort on foaming dominates the probability of the SOE being exceeded. Similarly, during the pump operational phase, the dominant hardware failure is associated with failure of control power to the mixer pump circuit breakers.

When reviewing these results, one must keep in mind the very significant assumptions and/or conservatisms that have been used. Some of these are listed below.

1. All control parameters are assumed to be independent, and no recovery credit was given for sensors that may provide backup indication for the same operating parameter; i.e., motor amps or pump discharge pressure would provide an indication of pump speed.

2. All control parameters were assumed to be equally important. Equal treatment of all control parameters by the operator was assumed.

3. Only conditional probabilities were considered. In effect, all initiating events were assumed to be equally likely. Clearly, some events are more likely than others. To obtain accident probabilities, the study would have needed to include accident initiator frequencies, all mitigation paths, and operator actions and account for redundancy in function, for example, pump speed and flow.

4. No effort was made to distinguish between slow and rapid envelope excursions. For slow evolutions, operator recovery is more likely.

5. Generic hardware failure data were used throughout.

Table 2. Integrated Phase A test total conditional failure probability

Dominant Cut Set	Probability	Importance (%)
Minimum 2/3 flow calculation	0.01	36.4
Video camera observation during testing	0.01	36.4
Preexisting failure of low H_2 sensor	2.88e-03	10.5
Dome-to-ambient-temperature-difference calculation	1.0e-03	3.6
Level rise calculation	1.0e-03	3.6
Operator fails to initiate manual abort	7.0e-04	2.5
Preexisting loss of control power to breaker	3.36e-04	1.2
Video camera fails	2.28e-04	0.8
Operator fails to check natural phenomena	1.0e-04	0.3

CONCLUSIONS

This reliability assessment has examined the operator and equipment capabilities required to maintain the operation of the mitigation test-by-pumping for Tank 101-SY within the specified SOE. The study looked at the conditional probability that the procedures and equipment would accomplish this. The qualitative insights into the DACS/Operator interface that were gained resulted in test procedure development, operator training, strict administrative controls, and design and operational improvements. The quantitative results from the study identified the dominant cut sets that, given the above assumptions, should potentially reflect the test parameters most likely to be exceeded during testing. Unfortunately, the key assumptions make useful interpretation of the quantitative results difficult at best. Additional qualitative arguments were made in an attempt to obtain meaningful results from the quantitative results.

REFERENCES

1. Los Alamos National Laboratory Report LA-UR-92-3196, Revised, "A Safety Assessment for Proposed Pump Mixing Operations to Mitigate Episodic Gas Releases in Tank 241-SY-101: Hanford Site, Richland, Washington," L. H. Sullivan et al.

2. NUREG/CR-1278, SAND80-0200, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," A. D. Swain, H. E. Guttman, June 1983.

2. Westinghouse Hanford Company, "Test Procedure for Tank 101-SY Mitigation-by-Mixing Test Phase A," WHC-SD-WM-TPI-004, Rev. 0 (December 1992).

3. Westinghouse Hanford Company, "Tank 101-SY Mitigation-by-Mixing Test Alarm Response Procedure," WHC-SD-WM-PROC-004, Rev. 0.

4. Westinghouse Hanford Company, "Tank 101-SY Mitigation-by-Mixing Test Abnormal Operating Procedure," WHC-SD-WM-PROC-005, Rev 0.

5. Westinghouse Hanford Company, "101-SY Mitigation Testing Acceptance Test Procedure," WHC-SD-WM-ATP-046, Rev 0.

021 Management of Risk in Chemical Processes

Chair: G.D. Kaiser, SAIC

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

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

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

RISK MANAGEMENT FOR HAZARDOUS MATERIALS WITHIN THE CITY OF TORRANCE

John D. Kulluk, Ph.D.
Hazardous Materials Analyst

Torrance Fire Department
Hazardous Materials Division
3031 Torrance Blvd.
Torrance, CA 90503

INTRODUCTION

Torrance is the fourth largest city within Los Angeles County. It encompasses an area of approximately 20 square miles and has a population of nearly 133,000 permanent residents. Nearly 400,000 people work and shop in Torrance during the day. The City has a mix of family residences, light to moderate manufacturing areas, and large industrial occupancies. There is a petroleum refinery, a plastics manufacturer, paint manufacturers, plating facilities, a can manufacturer, aerospace companies, along with a number of other users of hazardous materials in the City. There are about 500 businesses that use hazardous materials in quantities above 55 gallons, 500 pounds, or 200 cubic feet of compressed gas. About 10 percent of these businesses use hazardous materials that if released could present a risk to the surrounding community.

The Torrance Fire Department has taken a proactive approach in the area of environmental regulations primarily as they relate to public safety. At this time, the Fire Department administers Chapter 6.95 of the California Health and Safety Code, monitors the underground storage tank program, and has its own specially trained hazardous materials response unit.

In the fall of 1987, a devastating fire erupted in the alkylation unit of the Mobil Torrance refinery. The fire burned for several days and caused millions of dollars in damage to the refinery. Subsequent to the fire, it was ascertained that the alkylation unit contained about 25,000 gallons of anhydrous hydrogen fluoride (HF) which was used as the "alkylating agent." Hydrogen Fluoride is a low molecular weight

(molecular weight = 20 grams/mole), low boiling (approximately 60°F) inorganic acid. It is toxic via inhalation or skin contact. Special treatments must be administered immediately following skin contact. Due to its low boiling point, it must be stored under pressure. Any escaping liquid will immediately vaporize into a gaseous toxic cloud. The most surprising characteristic of anhydrous HF is the behavior of the vapors when they are released. Normally, the low molecular weight would indicate that the vapors are lighter than air (average molecular weight about 29 grams/mole) and, if released, the vapors should simply rise into the atmosphere and disperse. However, a series of large scale tests[1] in the desert revealed that when HF vaporizes, it forms a dense cloud that tends to travel on the ground for long distances, potentially affecting the health and safety of large areas of the community.

The Torrance Fire Department, acting as the Administering Agency (AA) for Chapter 6.95 of the California Health and Safety Code, which included the newly enacted Risk Management and Prevention Program (RMPP) provisions, requested an RMPP from the Mobil Refinery for their use of HF in March of 1988. This made Torrance one of the first Administering Agencies to request a RMPP from a facility.

The following article presents an historical view of the RMPP process in the City of Torrance, and how the RMPP process has impacted the City, the Fire Department, the **handlers** of hazardous materials, and the **public.**

HISTORICAL VIEW OF RISK MANAGEMENT FOR HAZARDOUS MATERIALS

Starting in 1985, the State of California passed a number of laws starting with Assembly Bill 2185 (Waters) and created Chapter 6.95 of the California Health and Safety Code. This Chapter required all handlers of hazardous materials to disclose to the local jurisdiction, the types and quantities of hazardous materials they used above certain threshold quantity limits and to develop and implement "Emergency Response Business Plans." The initial intent of this legislation was to provide information to local emergency responders, generally the local fire department, concerning the amounts and types of hazardous materials that were used at each handler's location. It was perceived that the information from the handlers would enable fire departments to more effectively plan, train, and prepare for responding to a release of a hazardous material. For example, if a facility used chlorine, the fire department could train its staff in the use of patch kits for chlorine cylinders. Another purpose of this legislation was to provide information to the public about the types and quantities of hazardous chemicals in their communities.

On January 14, 1986, the City of Torrance adopted Local Ordinance No. 3161, making the Torrance Fire Department the Administering Agency (AA) for Chapter 6.95. The initial duties of the AA involved collecting and storing data on hazardous materials users, and collecting emergency response business plans from businesses in Torrance.

---

[1]Blewitt, D.N., J.F. Yohn, R.P. Koopman, T.C. Brown, "Conduct of Anhydrous Hydrofluoric Acid Spill Experiments," AIChE International Conference on Vapor Cloud Modeling, Boston Mass., Nov. 2-4, 1987.

The same year that the Fire Department was named AA, Assembly Bill 3777 (La Follett) was passed which added Article 2 to Chapter 6.95, titled, Hazardous Materials Management. Article 2 provided new regulations for handlers of a special class of hazardous materials, termed Acutely Hazardous Materials (AHM), and included provisions for the preparation of an RMPP. The list of AHM was taken from the SARA Title III list of Extremely Hazardous Materials and presently consists of 360 solid, liquid and gaseous compounds. If a handler's use of AHM was above the State reporting threshold amount, the handler was required to "file" an AHM Registration Form with the local administering agency and with the State. Any handler that had filed an AHM Registration Form could be requested by the AA to prepare an RMPP.

Since the original 1986 legislation, the specific elements that make up an RMPP have remained the same; however, many other areas dealing with the scope of the RMPP, amounts of AHM that trigger an RMPP, consideration of sensitive populations near the handler, the role of the public in the RMPP process, along with changing RMPP requirements for new and modified facilities, have taken place. These revisions have not only produced a continuing challenge for handlers of AHM, but also placed a burden on the City of Torrance in trying to keep up with the changes.

What is a Risk Management and Prevention Program?

The RMPP is a technical assessment of how the facility has used and managed acutely hazardous materials in the past and how their process can be modified to lower the risk to the community in the future. The legislative intent[2] of Article 2 was based on the idea that the most effective means to protect the environment and the health and safety of the community from releases of toxic and hazardous materials was for the handler to have programs in place to prevent these accidents from occurring. Section 25532 of the California Health and Safety Code defines a Risk Management and Prevention Program as:

> **"...all of the administrative and operational programs of a business which are designed to prevent acutely hazardous materials accident risks[3], including, but not limited to, programs which include design safety of new and existing equipment, standard operating procedures, preventive maintenance programs, operator training and accident investigation procedures, risk assessment for unit operations, or operating alternatives, emergency response planning, and internal or external audit procedures to ensure that these programs are being executed as planned."**

THE AHM HANDLERS

[2]See Section 25531, Legislative Findings and Declarations, for the complete preamble to Article 2.

[3]This is defined in Chapter 6.95 as: a potential for the release of an AHM into the environment which could produce a significant likelihood that persons exposed may suffer acute health effects resulting in significant injury or death.

Preparation of an RMPP begins with a qualitative technical assessment, called a guide word hazard and operability study[4]. The assessment includes the process, the operations, and the procedures of the business, along with the various programs in place for the safe management of the AHM. The assessment must also consider all plausible external events[5] which could disrupt the process and lead to a release of AHM. From this assessment the handler develops a set of the most likely release scenarios and then, using an air dispersion model, graphically places the scenarios on a map showing the distance that the AHM will travel. The law specifically precludes the AA from disclosing the hazard and operability study and the off-site consequence analysis to the public. This process will allow the handlers to be better able to make informed decisions concerning how and where to most effectively spend money for risk reduction.

Upon completion , the handler submits a "certified complete"[6] copy of the RMPP to the AA. The RMPP must contain all of the elements given in Section 25534(c) of the Health and Safety Code, as shown in Table 1.

Table 1. Required elements of an RMPP from Section 25534(c) of Article 2 of Chapter 6.95 of the California Health and Safety Code.

Section	Element
1	Three-year accident history, causes, prevention methods
2	Status report on nature, age, and conditions of the equipment
3	Design, maintenance, and operating controls
4	Detection, monitoring, or automatic controls that minimize releases
5	Implementation schedule from the hazop
6	Audit and inspection programs for the RMPP
7	Record keeping procedures for the RMPP
8	Seismic assessments*
9	Responsibility table for RMPP implementation*
10	Certification page*

Submittal of the RMPP signifies that the handler is operating under all conditions, caveats and recommendations in the RMPP. The law requires that the RMPP be submitted within one year of the request. The law allows the handler one additional year to implement all recommendations arising from the RMPP process.

[4]The hazop is specified in the American Institute of Chemical Engineers, 1985 Guidelines for Chemical Hazard Evaluation Procedures, prepared by the Center for Chemical Process Safety.
[5]External events are events such as earthquakes, tidal waves, fires, airplane accidents, etc.
[6]Section 25534(h) requires that the RMPP be certified complete by a qualified person and the facility operator.

THE ADMINISTERING AGENCY VIEW

Presently, the AA is required to go through a three-step process before requesting an RMPP. First, the AA must make a preliminary determination of which handlers of AHM present a significant likelihood that their use of the AHM poses an **acutely hazardous materials accident risk**. After this preliminary determination, those handlers that pose an acutely hazardous materials accident risk must be ranked relative to each other and to each use of AHM. The ranking is based on worst case assumptions regarding the quantity and rate of release, air dispersion, toxicity, and meteorological conditions. From this ranked list the AA then develops a timetable for requesting the RMPP.

The Torrance Fire Department initially ranked the facilities by assuming that any handler with an amount of an AHM at or above the TPQ[7] presented an acutely hazardous materials accident risk. The second part of the ranking was done using an off-the-shelf computer program titled "Risk Rank" developed by Battelle Labs[8]. This program required that each handler of an AHM complete a survey form regarding their use of the AHM. The survey included information on the accident history, location, quantity of AHM and mitigation hardware at the site. The Fire Department visited each user to verify the survey information.

The Torrance Fire Department requires that the handler present the results of their RMPP study in two separate written volumes: a **technical** document based on the hazard assessment and the off-site consequence analysis, and a **public** document containing all of the other required elements in Section 25534. After completing the RMPP study, the handler submits both of these volumes and "certifies" that the RMPP is complete. A notice is placed in the local newspaper stating that the RMPP Public Document is complete and available for review and comment for 45 days.

After the public review period, the Fire Department reviews the submitted **Public** and **Technical** documents for deficiencies. The AA must consider any public comments in their final review. After the final review by the Fire Department, the handler is sent either a "Notice of Compliance" or "Notification of Defects" letter. The handler has 60 days to correct any deficiencies in the RMPP.

THE PUBLIC AND THE RMPP PROCESS

Recent changes to Chapter 6.95 have dealt with the public's right to know on decisions concerning risks of hazardous materials in their community. Section 25531 states "....the public has a right to participate in decisions about risk reduction options and measures to be taken to reduce the risk or severity of acutely hazardous materials accidents." The public was given the right to submit written comments regarding the RMPP to the AA, and the AA must consider these comments in the final review. This, it was assumed, would allow the

---

[7]The TPQ or Threshold Planning Quantity represents the amount of material that, if released, will reach a toxic concentration 100 meters from the release site.

[8]Battelle Process Risk Management Services, Columbus, Ohio, RISK RANK, Version 1.0.

public greater input into exploring the risks a handler's use of an acutely hazardous material would present and permit the public to have a say in any risk reduction measures that the facility could take.

RISK MANAGEMENT AND PREVENTION PROGRAMS WITHIN THE CITY OF TORRANCE

Torrance was the second AA to receive an RMPP. The request was made in March of 1988 after the devastating fire in the alkylation unit. During this time there was a strong nationwide interest about the risk to the public from the use of hazardous materials, and numerous articles appeared in newspapers and magazines on risks to the public from facilities using HF and other toxic chemicals . Stories about Love Canal, Bophal, and the Marathon Oil, Texas HF release were shown on national television.

In March 1989, one year from the date of request, the RMPP was presented to the Torrance Fire Department. The Fire Department and our consultant reviewed the document and then decided upon a course of action. There were three choices that ranged from sending the refinery a long list of corrections to be made within 60 days, issuing them a noncompliance citation, or to work together with the refinery personnel to prepare a mutually acceptable RMPP. The latter course was selected.

To further complicate the RMPP review process, the City Council filed a law suit against the refinery as a Public Nuisance; a ballot measure was placed on the pending (April) City election to restrict the amount of HF that could be stored in the City; and the South Coast Air Quality Management District (SCAQMD) was vigorously pressing to regulate all HF users in the South Coast Basin.

Over the course of the next two years, the RMPP was reviewed, rewritten and portions were redone. Eventually the RMPP review was completed to the satisfaction of the Fire Department, and the ballot measure to limit the use of HF was defeated. The refinery and the City of Torrance settled the law suit and entered into a consent decree which set up an independent Safety Advisor who reports to the court on various safety matters at the refinery.

In Our Own Backyard

The handler that posed the next greatest risk to the community was the City of Torrance Water Department. The Fire Department requested an RMPP for chlorine gas use at two well sites. Chlorine had been used by the Water Department for 30 years as a disinfectant. The chlorinating equipment was outdated, and the Water Department had no safety procedures, maintenance schedules, accident investigation procedures or training with proper safety equipment. Even though the Water Department had used chlorine for many years without serious mishap, the sites were surrounded by residential housing. At one site, one-ton cylinders of chlorine were within 50 feet of a day care facility.

The hazards analysis and the off-site consequence analysis determined that if the main line to the chlorinator broke from an earthquake, human error, etc., the leak could continue undetected for 15 minutes and the response to stop the leak could take up to 45 minutes. This release could expose the populations living around the facilities to concentrations of chlorine gas that could cause an acutely hazardous materials accident risk.

The Torrance Fire Department served not only as the AA, but also as the project manager, and sent out bids for an RMPP consultant, chose the consultant and specified what technical assessments were required for the RMPP.

Since this beginning, other RMPPs have followed for hydrazine, sulfuric acid, and ammonia.

CONCLUSIONS

The RMPP process allows the handler to review their use of acutely hazardous materials and develop programs from which they can manage their use of the AHM. These programs provide the handler with the tools to manage their use of the AHM, and assure the public that the handling of the AHM is done as safely as possible and that the operators are properly trained. These programs also assure that any modifications to the equipment, operating procedures, training content, etc., is considered and done effectively.

The RMPP will assure the public and the handler that their operations are "state of the art" in safety and that there are management programs and techniques in place to prevent releases of AHM into the community. The off-site consequence analysis allows the Fire Department to see what areas of the community will be affected by a release. Further the Fire Department will be better able to respond to releases of AHM and to train and prepare for an emergency. The Fire Department also gains in the knowledge of how to plan for evacuations and other emergency response actions.

DIFFICULTIES IN DECISION MAKING WITHOUT CONSIDERATION OF RISK

Geoffrey D. Kaiser

Science Applications International Corporation
11251 Roger Bacon Drive
Reston, VA 22090

INTRODUCTION

During the two decades since the Flixborough and Seveso accidents in Europe, and during the decade since the Bhopal accident, the introduction of regulations for facilities handling highly hazardous chemicals has proceeded rapidly. Examples include the Seveso directive in Europe and national programs such as the Dutch requirement for Quantitative Risk Assessment (QRA), which has legislated targets of tolerable risk. In the USA in the late 1980s there were initially three state-mandated Risk Management Programs, in California, Delaware and New Jersey. During the 1990s, US Federal Agencies have issued regulations as required by the Clean Air Act Amendments of 1990 - the Occupational Health and Safety Administration's (OSHA's) Process Safety Management (PSM) Standard and the Environmental Protection Agency's Risk Management Program (RMP).

In addition, in the US there are sometimes local programs that may or may not be consistent with state and federal regulations. One example - developed by the City of Torrance - is described in another paper in this session.[1] In another, the South Coast Air Quality Management district has issued its Rule 1410, which focuses on a single chemical - anhydrous hydrogen fluoride (HF) - and demands that its use on a large scale in the Los Angeles Basin be phased out by the end of the decade.[2]

Taken as a whole, these and other regulations span a wide range of attitudes towards the desirability and feasibility of the use of explicit risk-based targets. At one extreme, there is the Dutch national program,[3] which legislates acceptable targets of individual and societal risk. The British program, described elsewhere in these proceedings,[4] also makes use of quantitative risk. By contrast, the EPA's RMP, in spite of the use of the word "risk" in its title, avoids talking explicitly about quantitative risk - see below. SCAQMD's Rule 1410 is essentially based on the requirement that only zero risk is acceptable for HF, even though this is not stated explicitly in the rule or its accompanying documentation.

The purpose of this paper is to show that risk management and process safety regulations implicitly require that there be risk based judgements, and that those who implement such regulations make explicit or implicit risk-based judgements all the time. Where there is a reluctance to admit that there are such risk-based judgements, there can be poor decision making and inconsistent regulation.

RECOMMENDATIONS FROM HAZOPS

Many of the programs mentioned above require Process Hazards Analyses (PHAs), such as the Hazard and Operability Review (HazOp). These are team efforts to identify what can go wrong in a process and to identify recommendations for design and procedural changes that will enhance safety and the efficiency of operation. Many companies in the USA perform HazOps to comply with OSHA's PSM standard. It is not unusual for large sites to accumulate hundreds or even thousands of recommendations. The company will almost certainly be in a position in which: a) it cannot implement all of the recommendations quickly, even if it wants to do so; b) the cost of all of the recommendations may be excessive; and c) not all of the recommendations have equal value. The answer to this dilemma is to prioritize. Clearly, recommendations of high priority will include those that, if left unaddressed, will allow a risky situation to persist. That is, no matter how it is done, a risk-based judgement has to be made. If the need for this kind of judgement is not explicitly recognized, poor decision making may result.

It is becoming increasingly common for the HazOp team to provide input for risk based decisions. Many companies provide the HazOp team with a semi-quantitative risk matrix, which will be used to assign priorities to recommendations. An example is given in Figure 1. Some of the more sophisticated companies may also perform QRA and cost benefit analyses to prioritize and choose between recommendations. These companies often have internal quantitative targets of individual risk and societal risk (f-n lines or complementary cumulative distribution functions (CCDFs)), although in general they do not publish them.

It is therefore very likely that, as EPA and OSHA audit compliance with PSM and RMP, they will find an increasing number of companies who talk to them about compliance within an explicit, risk-based framework. That is, even those agencies that currently are reluctant to move towards QRA as an aid to sound regulation - as, for example, appears to be the case with EPA - will find the need to react to risk-based decision making.

THE EPA's RISK MANAGEMENT PROGRAM

The EPA's proposed rule for "Risk Management Programs for Accident Release Prevention" requires that "Hazard Assessments shall be conducted for each regulated substance present at the stationary source above the threshold quantity. For each regulated substance, the hazard assessment shall include the following steps:

"(1) Determine a worst-case release scenario for the regulated substance at the stationary source;

"(2) Identify other more likely significant accidental releases for each process where the regulated substance is present above the threshold quantity, including processes where the substance is manufactured, processed, or used, and where the regulated substance is stored, loaded or unloaded;

"(3) Analyze the offsite consequences of the worst-case release scenario and the other more likely accidental release scenarios --."

In its supplementary information, EPA states:

> " Information on the worst-case scenario will help public emergency planners and responders recognize the maximum hazard potential surrounding the facility. The Agency recognizes, however, that the

worst-case scenario may often be highly unlikely in comparison to other release scenarios with lesser potential consequences. Focusing on the worst-case scenario alone, therefore, could lead public agencies to overestimate the threat posed to a facility. For this reason, EPA believes that facilities must examine a range of events in addition to the worst-case scenario and communicate information on these events to public agencies and the public to provide additional information on the hazards posed by the facility. In addition, EPA does not want facilities to focus solely on the worst-case release because other scenarios are of concern, are generally far more likely than a worst-case release scenario, and must be addressed in the prevention program. Therefore, EPA is requiring facilities to analyze hazards associated not only with the worst-case scenario, but also with more likely significant releases."

This guidance studiously avoids mentioning the word "risk" - but in fact it is all about risk. For example, it recognizes that worst-case accident scenarios are not necessarily the greatest contributors to risk: that is why EPA is asking for analysis of a range of other scenarios. In addition, asking industry to communicate information on potential events to public agencies and the public requires risk based judgement, as the following example shows:

Suppose that the worst-case scenario could affect a large number of people above some level of concern out to a distance of several miles. If that information is simply presented to the public, the response is likely to be "that's intolerable" or "what are you doing about it!" The response from industry may then be to point to mitigation systems. But how will industry, agencies and the public know that enough has been done? The simple statement that "enough has been done" is an implicit judgement that the risk is tolerably small: but how can this be known without targets of acceptability? Without such targets, decisions may be made which may vary either way, being too lax or too stringent. As noted above, large, sophisticated industries may choose to adopt a risk-based framework of their own. Small users of highly hazardous materials, which make up the bulk of the 140,000 facilities that will be affected by the RMP, will need guidance that itself will, of necessity, contain risk-based judgements.

THE SOUTH COAST AIR QUALITY MANAGEMENT DISTRICT'S RULE 1410

In 1991, SCAQMD introduced a rule which will effectively ban the large scale use of anhydrous HF in the Los Angeles Basin. This affects four refineries (now three, since one, Golden West, has since shut down) that use HF as a catalyst in the alkylation process and one producer of hydrochlorofluorocarbons. (Note that, at the time of writing, the rule is in abeyance because of a court challenge by one of the affected refineries.)

There is no logical reason why SCAQMD should have singled out HF in this way. The EPA, in its recent report to Congress,[5] does not recommend a unique approach to HF but rather indicates that current regulations, such as OSHA's PSM standard and EPA's RMP, which apply equally to a large number of highly hazardous chemicals, are adequate for the protection of workers and the public. Furthermore, the accident record does not show that HF is uniquely dangerous to the public.

SCAQMD justifies its authority to regulate HF by stating that:

"The District is empowered to adopt rules and regulations necessary to execute the powers and duties granted to and imposed upon the District by law (Health &

Safety Code Section 40702). Pursuant to Health and Safety Code Section 40752, the District must enforce the air pollution nuisance laws (Health and Safety Code, Section 41700) which states:

> "No person shall discharge from any source whatsoever such quantities of air contaminants or other materials which cause injury, detriment, nuisance or annoyance to any considerable number of persons or to the public, or which endanger the comfort, response, health or safety of such persons or the public.

"Accordingly, the District may adopt rules and regulations designed to prevent the occurrence of a nuisance such as would occur in the event of an accidental release of HF."

The possibility that an accidental release of HF might cause a "nuisance" is logically insufficient to single out HF, since the same statement applies to many other chemicals.

SCAQMD also sponsored the performance of some of the elements of a QRA, focusing on "near worst-case" releases which were essentially ruptures of 1" - 2" diameter in pipework or vessels, leading to releases of anhydrous liquid HF of up to about 1,000 gallons per minute.[6] It was estimated that such releases might occur in refineries with alkylation units about once in ten thousand years. Needless to say, the consequences, in terms of the number of people affected by airborne HF at a "nuisance" or "irritation" threshold of 20 ppm for a 5 minute exposure, were predicted to be large. The results of these calculations were not taken any further in Ref. (6) - that is, SCAQMD did not make quantitative estimates of risk and did not compare those estimates with any targets of tolerable risk. Nonetheless, the judgement was made that the implied risks are unacceptable.

SIGNIFICANCE-BASED REGULATION

To return to the Los Angeles Basin and SCAQMD, decisions in the process industries are being driven by the concept of "significance." New industrial construction requires the submittal of an Environmental Impact Report (EIR) through SCAQMD. The EIR must contain a section on "Risk of Upset," which is to say consideration of accidental releases of highly hazardous materials. Three examples for which SCAQMD has required an EIR are on the use of anhydrous ammonia at the Redondo Generating Station,[7] on the use of aqueous ammonia at the Alamitos Generating Station[8] and the above referenced Rule 1410. These studies adopted the following approach:

Determine Scenarios and Develop Frequency Estimates

Chemical release scenarios were developed for each affected facility. As noted above, these were "serious near worst-case" releases that could result from a large rupture in a pipe or a vessel. The frequency of occurrence of these "near worst-case" releases was estimated.

Choose Exposure Limits

Two potential health impacts were considered in the ammonia and HF documents. The first was for irritation to exposed populations and the second was for the probable occurrence of serious injury and mortality. For example, for ammonia,

a ten-minute, 100 ppm exposure was chosen as the irritation threshold and a ten minute, 4,700 ppm exposure was chosen as the serious injury threshold. The number of people at the irritation and serious injury thresholds was estimated for a range of weather conditions including "near-worst case."

Assess Significance

Significance is then assessed by the magnitude of the consequences, essentially discounting the above referenced frequency calculations. For the anhydrous ammonia facility at the Redondo site, a "near worst-case" rupture of the storage vessel was predicted to lead to about 5,000 people being affected at the 4,700 ppm level and about 33,000 people being affected at the 100 ppm level. If, however, a water spray system designed for 90 percent efficiency were installed, these predictions would be reduced to less than one person at the 4,700 ppm level and about 6,000 at the 100 ppm level. The project was allowed to proceed configured as an above ground storage vessel with a water spray system.

For the aqueous ammonia (30%) storage facility at the Alamitos site, there are no explicit calculations for an above ground aqueous storage vessel. However, it can be inferred from transportation calculations that, for the "near worst-case," less than one person would be exposed at the 100 ppm level and about 5,000 at the 100 ppm level. The "significance" of an above ground aqueous storage system with no further protective measures would appear to be about the same as for an anhydrous ammonia vessel with a water spray: however, at Alamitos an additional protective feature was added: the tank was buried.

There is no space here to describe a quantitative risk assessment. Nevertheless, it is clear that the implicit target of acceptable risk is much more stringent at the Alamitos site than it is at the Redondo site.

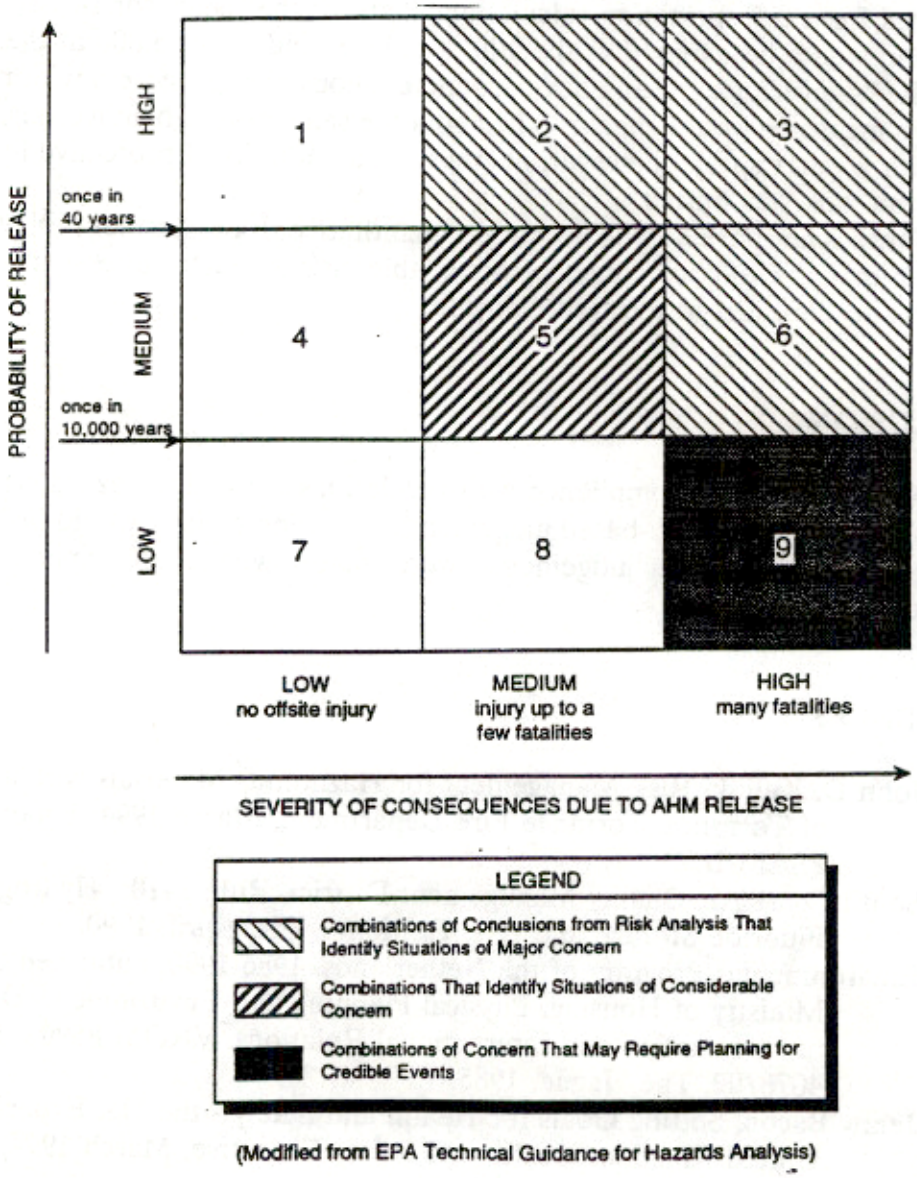
CONCLUSION

As shown above, compliance with regulations for highly hazardous materials requires the exercise of risk-based judgements. Decision making would be better and more consistent if these judgements were made within an explicit-risk-based framework.

REFERENCES

1. John D. Kulluk, Risk Management for Hazardous Materials within the City of Torrance, Torrance Fire Department, March 1994; Paper 239 in PSAM-II.
2. South Coast Air Quality Management District, Rule 1410: Hydrogen Fluoride Storage and Use, El Monte, CA, April, 1990.
3. Environmental Program of the Netherlands, 1986-1990, published by the Ministry of Housing, Physical Planning and Environment, Department of Information and International Relations, VROM 85902/12-85, 4078/92, The Hague, 1985.
4. Jenny Bacon, Setting Goals for Health and Safety - the UK Experience, United Kingdom Health and Safety Executive, March 1994; Paper 232 in PSAM-II.

5. U.S. Environmental Protection Agency, Hydrogen Fluoride Study, EPA 550-R-93-001, Washington, D.C., September, 1993.
6. M.R. Beychok el at., Source Terms and Frequency Estimates of Scheduled Accidental Hydrofluoric Acid Release Scenarios in the South Coast Basin, prepared for the South Coast Air Quality Management District by PLG, Newport Beach, CA, December 1990.
7. South Coast Air Quality Management District, Final Subsequent Environmental Impact Report: Anhydrous Ammonia Storage Tanks Installation at Redondo Generating Station, Diamond Bar, CA, December, 1992.
8. South Coast Air Quality Management District, Final Subsequent Environmental Impact Report: Aqueous Ammonia Tank Installation at Alamitos Generating Station, Diamond Bar, CA, January, 1993.



(Modified from EPA Technical Guidance for Hazards Analysis)

Figure 1. Example of a Risk Analysis Matrix

RISK-BASED REGULATION
SETTING GOALS FOR HEALTH AND SAFETY

Jenny Bacon

Deputy Director General
Health & Safety Executive
London, United Kingdom

INTRODUCTION

This paper describes some key aspects of the regulatory regime for health and safety in the UK; considers the role of risk assessment within it; and assesses advantages and disadvantages for the regulator and the regulated. It concludes that a statutory framework defining goals rather than means of achieving them, supported by 'self-regulation' in industry based on identification and control of risks and by a regulatory approach which balances degree of risk and costs of risk avoidance, is cost-effective for all parties - including those protected by regulation.

Health and safety law in the UK goes back to the start of the last century. However, by the late 1960s, the accretion of law, relatively poor performance in reducing deaths and injury, and new concerns about the potential impact of high hazard industries on public safety, led to the setting up of a Committee of Inquiry under Lord Robens.

The Robens Committee concluded, first, that the single most important cause of accidents was apathy - on the part of all concerned in industry; and second, that a major cause of this was that there was simply too much law. Moreover, the elaboration, detail and complexity of the law resulted in its rapid obsolescence. The regulatory regime was perceived as detailed rules imposed by external agencies. It placed too little reliance on personal responsibility and voluntary effort to control risks: health and safety were "someone else's problem". The Committee affirmed as a guiding principle that "primary responsibility for controlling hazards lies with those who create the risks and those who work with them", and set out recommendations for a regime to support that principle.

The recommendations rested on creating conditions for a more self-regulatory system: self-regulatory not only in the sense of putting more responsibility back with the risk-creators in industry, but also in the sense of continuously adjusting solutions to match problems. The essentials for the system were: clear definition of responsibilities, awareness, and methodical assessment of the nature of a problem. The law should provide a statement of principles and definition of duties of general application, with regulations setting more specific goals and standards. Codes of practice and guidance drawn up by or with industry should set out good practice on processes and means of achieving the goals. Enforcers should concentrate preventive effort on known high-risk

activities and premises, and rely on 'enforcement on complaint' in lower risk areas. Industry should take an active role in setting standards and developing guidance on good practice; but - more important - should make health and safety a normal part of the management function and of systematic approaches to loss control.

Those recommendations made in 1972 shape the system we have today in the UK. They were enshrined in the Health and Safety at Work etc Act 1974. The Act sets out general duties on employers, employees, the self-employed and other risk-controllers. It gives powers progressively to replace the welter of old industry or process-based laws with modern, goal-setting regulation supported by codes of practice and guidance. It set up a Health and Safety Commission (HSC) with representation from industry and the community; and a Health and Safety Executive (HSE) which, crucially, brought together the Inspectorates and policy advisers responsible for regulating hazards to health and safety - of the public as well as work people - in the great majority of industrial processes and activities.

THE SYSTEM IN OPERATION

So how, 20 years on, does it work? The parameters remain clear. The state, through the regulatory authority (HSC/E) sets the standards, ie. the goals of regulation - what has to be achieved. It then concentrates on securing compliance - not on enforcing sanctions against those who fail to comply, though that last resort is available. (All health and safety law attracts criminal penalties.) The practicalities within each industry and workplace determine the means of achieving health and safety goals in the context of each business' own operations and management systems, against the regulatory principle that risks must be reduced to as low as is reasonably practicable.

The benefits of the system - where it is fully operational - are widely recognised by all parties: there is less law; it is more easily comprehended, more flexible and capable of proving fit for purpose, better able to accommodate technological and other changes. There is greater commitment by top management in industry, more thought given to control of hazards and risk reduction rather than slavish adherence (or not) to possibly irrelevant proscriptions and requirements. Hence there is less cost to industry of health and safety measures: safety can be designed-in with other loss control measures and management systems. We are nearer to this state of Nirvana in some industries - particularly high hazard areas - than in others. But the principles remain largely unchallenged.

Two ingredients are essential for the 'self-regulatory' system to work: a risk-based approach to determine what action has to be taken to secure health and safety; and a cost-benefit approach applied to acceptance of risk and decisions on measures needed to prevent or mitigate it. Proportionality of response is the key to both. I examine below how these ingredients work in the legislative framework, in industry's actions, and in enforcement.

The legislative framework

The Health and Safety at Work, etc Act places what are, in effect, general duties of care on each of the main parties to industrial activity - employers, self employed, employees, manufacturers and designers, and owners of dangerous premises. These are completely general in application: there is no discrimination by level of hazard or risk. That is the bed-rock for securing compliance with generally accepted standards of health and safety when more specific requirements are absent. But all the duties are subject to a key qualification: that the end-result is to be achieved "so far as is reasonably practicable". The recognised interpretation of this qualification is that there must be a computation of risk and cost, and the onus is on the risk-creator to show that the risk is insignificant in relation to the cost of averting it - bearing in mind the overall benefit of conducting the

activity which gives rise to the risk. So risk assessment and cost-benefit analysis come in on the ground floor of the legislative framework.

The general duties are supported by regulations dealing with specific hazards, industries, processes, substances, situations or persons. They set standards to be achieved. They may prescribe or proscribe in dealing with incontrovertible risks where control measures are unlikely to change, or where a step-change in behaviour is needed. They ensure consistency of approach, which has market benefits beyond the regulation of health and safety. Some impose absolute duties; others are qualified by the idea of 'reasonable practicability'. The modern sets of regulations are firmly based on risk assessment: in the standards they set which reflect scientific evidence and evaluation of risks; in decisions about whether to impose absolute duties, bans or proscriptions etc; and in the choice of how to control - by licences, approvals, safety case regimes, notification systems or other "permissioning" of higher-hazard activities, or by straightforward duties on those responsible without recourse to permissioning.

An aspect of goal-setting regulations which is increasingly being adopted, particularly for higher hazard industries and for dealing with hazards to health, is a requirement for the main duty-holder to identify hazards and assess risks in his operations. He or she may also be required to prepare a safety case demonstrating how the risks will be prevented or otherwise controlled, and to set out a safety management system showing how the safety case will be implemented and maintained. The safety case and safety management system may need to be notified to the regulator who can intervene but does not have to (chemical industries); or may require acceptance (offshore installations) or validation (proposed for regulation of the privatised railway system). The strongest form of the 'statutory risk assessment' approach is licensing, as for nuclear sites, where risk assessment, a safety case and operation in accordance with it form part of the licence conditions. The precise form of regulation varies with history and circumstance; the common features are the primacy of hazard identification and risk assessment, and the onus placed on management to come up with the answers.

Regulations can be bad for your health. We currently have some 400 sets on the statute book - compared with around 700 20 years ago. We are still clearing out the historical legacy of detailed specifics intended to control every last move in a factory. At the same time we face a new wave from the East of prescriptive legislation - in the form of European Community Directives which are based on a regulatory approach at right angles to our own goal-setting approach. Risk assessment and cost-benefit analysis are essential tools for reconciling the different approaches.

Amplifying the general duties and regulations are Approved Codes of Practice (ACOPs), authoritative guidance and advice. These deal with ways, means and processes rather than end-goals. They aim to reflect good - sometimes best - practice in industry in control of risks. They can be relatively easily updated to adjust for changes in knowledge of hazards and in technologies to deal with them. They offer clarity and certainty to those regulated ("do this and you'll be alright") while allowing for different approaches by the more enterprising. The differences between them are important, if not always fully appreciated. ACOPs have evidential status: duty-holders must do what an ACOP suggests or show that an alternative approach works at least as well. So they set a base standard of acceptable practice and, in effect, define what is "reasonably practicable". Authoritative guidance has no evidential status: the regulator must show why a duty-holder should have followed the guidance rather than another approach - and that the guidance represented what was 'reasonably practicable' in the circumstances. But guidance can set out best practice as well as good or acceptable practice and can be used as a voluntary means to raise standards. Advice is frequently technical and sets out best practice as found in an industry. It helps the process of self-regulation rather than that of enforcement.

When to use regulations (and in what form) rather than ACOPs, and when to use ACOPs rather than relying on guidance and advice, are themselves key decisions for the regulator in offering policy advice. Other determinants being equal (and often they are

not for reasons of history, foreign policy, politics and resources) the choice of approach will also be based on a full assessment of risks, costs and benefits.

Self-regulation in industry

The legislative framework described above leaves industry with a number of clear 'givens' - pin-pointing responsibilities especially at owner/Director level; specifying goals; and in some cases specifying the main processes - risk assessment, preparation of a safety case - that must be used to respond to the general duties and requirements of regulations. It also allows for considerable discretion in approaches to dealing with risks, and indeed in interpretation of what is 'reasonably practicable' where statutory duties are qualified. This in turn allows for easy adaptation to changes in technology. In the absence of specific requirements which can be delegated to others to follow, managements are compelled to think, at senior levels, about health and safety arrangements and how they tie in with management and production systems overall. The impact of these arrangements is to draw industry into all aspects of the regulatory process: the definition of workable standards and statutory goals; the preparation of ACOPs that will define 'reasonable practicability'; the writing of guidance and advice that will spell out good and best practice. Still more, risk assessment/safety case requirements propel the regulated and regulator into a dialogue about the nature of hazards and the consequences and degree of risk, about control measures and about the relative acceptability of risks and costs. Thus the law is used as a basis for discussion and diagnosis rather more than for enforcement and sanctions by the regulator.

Risk assessment in Enforcement

As stated above, the main emphasis of the Health and Safety Executive's enforcement arm is on securing compliance through preventive inspection and audit, rather than on post-incident investigation and enforcement by prosecution or other sanctions. Risk assessment is used to target preventive inspection on high-hazard industries and processes, and on firms with a poor history of compliance or with management systems and structures which appear defective. Increasingly, safety cases and safety management systems notified to the HSE provide a basis both for decisions about inspection programmes, and for identifying in advance the areas to be examined. The documentary evidence in a safety case of hazards identified and ways of tackling them also enables Inspectors selectively to undertake safety audits rather than conventional inspection in high hazard areas - focusing on management systems and the success with which they are put into operation.

Risk analysis and risk assessment techniques are also increasingly used by the HSE in assessing, accepting, or validating safety cases and in other 'permissioning' activities. Inspectors and assessors must be able to discuss issues with the duty holder on at least an equally well-informed basis. They must also be sure of their ground in exploring the nature of a hazard, its consequences for workpeople and the public, and the effectiveness of control measures in reaching discretionary decisions about what is 'reasonably practicable' and whether risks have been reduced as low as reasonably practicable or to a level of acceptability beyond which further expenditure to achieve further reductions would not be justifiable. Discretionary decisions are increasingly subjected to public inquiry or judicial review: risk assessment and cost-benefit analysis are important sources of defence for the regulator if so challenged.

One area in which relative risk has not taken hold as the basis for decisions is in national resource allocation. Some attempt has been made at 'cost per statistical life saved' comparisons of government interventions in, for example, investment in road programmes, the health services and health and safety regulation. But there are intrinsic difficulties in reconciling the 'statistical life' approach with public perceptions of tolerable

risk. There are also difficulties in arriving at acceptable comparative data when dealing with very different risks and levels of certainty in their calculation. And the answers provided by quantified risk analysis are frequently not those provided by the political process. So while risk-based cost-benefit analyses may come to figure more in debate about national resource allocation, they seem unlikely to determine the outcome.

DISCUSSION: PROS AND CONS OF RISK-BASED REGULATION

Does the combination of goal-setting legislation with risk/cost/benefit-based approaches to securing compliance help self-regulation? Does self-regulation protect work people and the public effectively from harm? Is it cost-effective for industry and the tax-payer? I assess below the pros and cons - for the regulator, the regulated, and those who both pay for and benefit from the regulation.

For the regulator, there is no doubt that a goal-setting approach poses difficulties. It places very heavy reliance upon the exercise of discretion by inspectors and assessors in judging whether standards have been complied with, whether risks have been properly identified and quantified, and whether enough preventive or mitigatory measures have been taken to satisfy the proper balancing of costs and risks. This dependence on discretion in turn means that the regulator's forces have to be extremely well-informed scientifically and technologically, to be highly trained to produce consistent application of standards, and to be economically and legally literate as well. The goal-setting, risk-based approach is also relatively time-consuming - in ensuring a sound data-base for decisions about risk and methods of control in assessing safety cases and undertaking other more complex 'permissioning' activities, and in carrying out management systems audits rather than conventional shop-floor inspections. Cut and dried prescription and proscription in law undoubtedly makes for easier, check-list inspection.

There are other drawbacks. For the small firm without a management structure and functional specialisms, the approach may simply be too sophisticated and time consuming, so health and safety get ignored: by high risk as well as low-risk small firms. Secondly, the concentration on Director-level involvement may place the understanding and ownership of safety problems too high up the chain and away from the source of hazard. It then requires very good management systems and communications to ensure that those at operator/supervisor level carry through senior management's best intentions. The problems are multiplied when work is sub-contracted. Moreover, relying on firms themselves to fill in the details on how safety goals will be achieved and to operate effective safety management systems makes firms extremely vulnerable over time to "the human factor" - ie simple human error and propensity to forget or circumvent.

Third, when the regulator becomes involved in assessment of company safety cases, or acceptance - passive as well as active - of a firm's own risk assessment, there is some danger of a transfer of responsibilities (and liabilities) from the risk-creator to the regulator. A concomitant risk is the 'captive regulator', especially in high-hazard industries where inspectors/enforcers may be on-site on a frequent and regular basis working with local site managers. Avoiding these dangers puts great pressure on the regulator to be scrupulous in recording the basis of all decisions and also the matters on which managers' assurances are accepted without full investigation.

A further problem for the regulator can be securing convictions on the bases of general duties rather than specifics; of likelihood or potential to cause harm rather than actual blood on the floor; and of senior management responsibility for safe systems rather than responsibilities of those most directly concerned with the cause of an accident.

For the regulated in industry and commerce, there are also difficulties as well as advantages. "Judging risks" is common sense; risk assessment, particularly in its more sophisticated manifestations (QRA, PRA etc) can be off-putting for smaller firms: many would prefer the certainties of a prescriptive "tell me what to do" approach. Risk assessment can also be hair raising for those in higher hazard industries simply because of

the degrees of uncertainty involved in the calculations. That in turn imparts a high degree of uncertainty into computations of whether risks have been reduced as low as is reasonably practicable, or whether more (expensive) work should be undertaken. This is fertile ground for endless debate with the regulator, and time equals money. It is also without doubt time-consuming to prepare properly a safety case and description of a safety management system. And making sure that operations conform with the safety case needs considerable expenditure of management time. Because legal responsibilities are placed at owner/director level, that management time is expensive.

However, for all firms, regardless of size or sector, goal-based regulation means less law to cope with and understand. And for the firms who are willing to exploit the flexibility which a goal-setting, risk-based approach offers, the expenditure is an investment not an overhead. Managerial approaches to loss control, and quality management approaches more generally, eg. ISO 9000, can be used to secure compliance with health and safety goals in ways which do not conflict with procedures, processes and technologies which are best from the business point of view. The lack of prescription of means rather than ends allows for technological updating and for the design of solutions to risk prevention and control which are fit for purpose and proportionate to the degree of risk.

For the public and work people protected, the tax-payer and the state, the regulatory regime described above appears to be effective in prevention of accidents and ill-health - by comparison with earlier practice in the UK and with, for example, the record of other Member States of the European Community which rely to a much greater extent on prescription, "enforcement by insurance" and prosecution. Since the mid-1970s the fatal injury rate for employees in Britain has halved (to 1.4 per 100,000) and a recent comparison has shown that the rate of deaths in Britain is at least two to three times lower than in France, Spain, Italy and West Germany.

Despite the heavy investment in an expert, knowledge-based, health and safety-dedicated regulatory body, the UK system also appears cost-effective - in terms both of cost to the tax-payer and of impact on business costs. Direct and detailed comparisons of the resources committed to health and safety by EC Member States are notoriously difficult - not least because the legal and institutional arrangements differ so much. But in countries such as France and Germany the direct input to health and safety by Governments, employees and other institutions - including resources going into health and safety inspection from Government and insurance sources - are significantly greater proportionately than in the UK. In part at least this reflects the fact that in the UK inspection and other activity is concentrated where it will make most impact in preventing harm, and much of the detailed work of securing compliance is left to industry to take forward as part of its normal loss-control measures.

Because the regulatory regime extends across all of industry and covers both people at work and the public affected by work activities, it is increasingly possible to control sources of hazard at the design stage or at the point of supply, rather than at the point of use. That has wider benefits for domestic consumers, and in some cases for the environment.

In conclusion: the legal framework for regulation of health and safety at work is still in the process of modernisation and "deprescription". Outside the high hazard sectors, use of risk assessment by businesses is not yet normal practice. At the national level balancing costs against risks is not a well developed tool. Nevertheless the essential elements are in place for a system which ensures that regulation is proportionate to risks and to costs - and hence that the interests of the state, of work people and the public, and of business are properly balanced.

022 Risk Management in DOE (I)

Chair: K. Murphy, USDOE

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

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

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

RISK MANAGEMENT AT THE OAK RIDGE NATIONAL LABORATORY RESEARCH REACTORS

G. F. Flanagan,[1] M. A. Linn,[1] L. D. Proctor,[1] and D. H. Cook[1]

[1]Research Reactors Division
Oak Ridge National Laboratory
Oak Ridge, Tennessee 37831

INTRODUCTION

In November of 1986, the High Flux Isotope Reactor (HFIR) was shut down by Oak Ridge National Laboratory (ORNL) due to a concern regarding embrittlement of the reactor vessel. A massive review effort was undertaken by ORNL and the Department of Energy (DOE). This review resulted in an extensive list of analyses and design modifications to be completed before restart could take place. The review also focused on the improvement of management practices including implementation of several of the Institute of Nuclear Power Operations (INPO) requirements.

One of the early items identified was the need to perform a Probabilistic Risk Assessment (PRA)[1] on the reactor. It was decided by ORNL management that this PRA would not be just an exercise to assess the "bottom" line in order to restart, but would be used to improve the overall safety of the reactor, especially since resources (both manpower and dollars) were severely limited. The PRA would become a basic safety tool to be used instead of a more standard deterministic approach to safety used in commercial reactor power plants. This approach was further reinforced, because the reactor was nearly 25 years old at this time, and the design standards and regulations had changed significantly since the original design, and many of the safety issues could not be addressed by compliance to codes and standards.

HIGH FLUX ISOTOPE REACTOR DESIGN

The HFIR is an 85-MW flux trap reactor. A schematic of the reactor is contained in Figure 1. It is light water cooled and beryllium (Be) moderated. It operates at 468 psi pressure with an inlet temperature of 120°F and outlet temperature about 155°F. The peak thermal flux in the flux trap is 5×10^{15} n/cm^2-sec, which makes HFIR the highest thermal flux reactor in the world. The core of the reactor is small (17-1/2 inches in diameter, 24 inches in height) with a 5-inch diameter target hole through its center. The core contains 9.4 kg of highly enriched (93%) U^{235}, arranged in two concentric cylindrical elements. The inner element contains 171 involuted plates and the outer element contains 369 involuted plates. The core is made up of U_3O_8/Al mixture clad in aluminum. The core is replaced every 24 days. The Be reflector surrounds the core and is about 1-foot thick. Control is achieved by four control plates

arranged in a cylinder around a solid control cylinder. The outer control plates are raised and the inner cylinder lowered to increase reactivity. These control plates/cylinders are sandwiched between the core and the Be reflector.

The reactor core is contained in an 8-foot diameter pressure vessel which is 19 feet high. The pressure vessel is located in the bottom of a large pool (36 feet deep and about 18 feet across) containing 85,000 gallons of water.

The pressure of 468 psi is maintained by compressing the primary system water using a pressurizer pump in combination with a system of flow letdown valves. The flow (16,000 gal/min) is achieved by three out of four AC-motor-driven primary pumps and is downward through the core and target regions. Shutdown decay heat is removed using a DC motor to drive the primary pumps. The DC motor is supplied with a dedicated battery power supply that is charged using off-site power, on-site diesel generators, or portable diesel generators.

A schematic of the HFIR process flow system is included in Figure 1.

The reactor is contained in a large reactor building 128 x 160 x 110 feet that is maintained at a slight vacuum. Exhaust fans pull air from the building though a series of filters and exhaust up a 250-foot stack. The building, filters, fans, and stack act as a dynamic confinement in the event of an accident.

The level 1 PRA (excluding external events) was finished in 1988, and the external event analysis was completed in 1990. The final PRA report (including responses to the extensive peer reviews) was published in 1991 (ORNL/RRD/INT-36, Rev. 1). In addition to the level 1 document, a modified level 3 analysis was published and results were compared to the 10 CFR 100 regulations. The HFIR PRA is intended to be a living document that changes to reflect design changes, procedures, and dates.

One of the most dramatic examples of risk management occurred early in the data gathering and analysis stage of the PRA. The risk analysis indicated that the HFIR had a very dominant accident sequence initiated by flow blockage.

FLOW BLOCKAGE

Because of the very high power density and narrow fuel channels in the HFIR, it was acknowledged by the original designers that core damage could occur as a result of small flow blockages. In order to reduce the vulnerability, a strainer containing small orifices was inserted in the inlet primary coolant pipe, and the plant confinement, shielding and water clean-up systems were designed to accommodate a core melt that might be expected to occur during the lifetime of the plant.

There are no systems models or explicit data to use for modeling and quantifying flow-blockage scenarios, since such blockages are not expected in the commercial nuclear power plants.

A very structured expert opinion approach was developed by S. Kaplan of PL&G, Inc., that used the HFIR designers, operators, and engineers as the knowledge base. Figure 2 shows the general form of the flow blockage scenario event tree.

The first step in the process was to define where the debris that could cause a flow blockage originates. Internal debris refer to material that is a part of the system (gaskets, bolts, small pieces of metal, etc.) and external material is material that enters the system unintentionally, for example, from the reactor pool (tools, plants, rags, cigarette packages, watch crystals, etc.).

The second step was to divide the primary loop into locations as shown in Figure 3. The L3 location was used for all external debris.

The third step was to define a set of material types. Five types were defined: (1) elastomer material (gaskets and seals), (2) small metal parts, (3) large metal parts, (4) corrosion and erosion products, and (5) plastic, glass, paper, fabrics, etc.

Detailed event trees were formulated.

The HFIR experts then were used to evaluate the branch-point split fractions. Several iterations were performed before consensus was reached. The initial results indicated a frequency of 2.6×10^{-2}/year for core damage. The HFIR staff then identified several potential modifications in the design and administrative procedures, and the evaluation process was

repeated. The modifications reduced the core damage frequency due to flow blockage to 9×10^{-5}/year.

Loss-of-coolant flow blockage was the most dramatic example of risk management; however, the PRA revealed several other risk management opportunities of the HFIR. The loss-of-coolant accident for the HFIR was considered improbable by early accident analysts; however, the HFIR PRA indicated that such an event was not improbable, but a detailed analysis indicated that the reactor was able to withstand a break in any primary pipe of 2 inches in diameter or smaller because of a "pool-to-vessel" check valve that had been installed by the designers. As a result, the valve was subsequently classified as safety related, and a surveillance test procedure was initiated to periodically validate its operability. Taking advantage of an existing design feature prevented a costly design change to accommodate a small break loss-of-coolant accident.

LOSS OF POWER

A third area of risk management was the response to the risk imposed by an extended loss-of-power event primarily due to a seismic or tornado event. The HFIR has a set of uninterruptible power supplies (ups) for DC pony motors used to remove decay heat from the reactor core for at 6 hours. However, the on-site diesel generators were not contained in a seismically/tornado hardened building and these would not be available to provide backup power for recharging the ups. Instead of a costly upgrade of the normal emergency power system estimated to cost $2M, ORNL chose to purchase two portable diesel generators, which could be brought to the site using one of several vehicles on site. These can be connected to the pony motor battery chargers/pony motor pumps and can be fueled from the existing underground fuel storage tanks. Use of one of the two portable generators can provide greater than 7 days of uninterruptible power in case of an extended loss of off-site power. The cost was less than $100K. The avoidance of the costly seismic upgrades to the normal emergency system and structures offset the cost of the entire PRA by a factor of two.

VESSEL PRESSURE RELIEF

One of the compensatory actions associated with the vessel embrittlement was the installation of an emergency depressurization system. The PRA analysis of the system revealed that this new system as designed and installed could result in a small break loss-of-coolant accident due to the loss of instrument air that had a higher probability of occurrence than the likelihood of a vessel rupture due to low-temperature, high-pressure operation. As a result, the failure mode of the system due to a loss of instrument air was reversed to prevent a small loss-of-coolant accident.

TEMPERATURE TRIP

In another case, a primary coolant pump trip was added for bearing high temperatures. Also, the PRA dictated that the primary coolant pumps should be rebuilt and a new type of bearing material used that would allow the pumps to operate without bearing cooling.

DEFINITION OF CRITICAL SAFETY FUNCTIONS

Immediately prior to restart, the DOE requested a detailed description as to how the four critical safety functions (reactor protection, emergency core cooling, decay heat removal, and confinement) were achieved in the HFIR design. The PRA was used as the basis for the description rather than a much more costly design reconstitution based on a deterministic approach.

POST RESTART ISSUES

After restart, the results of the PRA continued to be used. A safety-related equipment list was created using the PRA results. Emergency Action Guidelines were developed using the PRA and results incorporated in the Emergency Response Plan.

A post-restart requirement was to upgrade the Safety Analysis Report (SAR). The PRA was used to select the accident scenarios analyzed in Chapter 15 of the SAR. The approach involved evaluating all PRA-identified scenarios down to a core damage probability below 10^{-6} per year. Consequently, Chapter 15 of the SAR includes sequences involving initiating events plus multiple failures, rather than the traditional single-failure analysis approach.

PRA is a part of the training of operators and shift technical advisors and for technical staff training. The PRA was used as the basis for the Environmental Qualification Program. The PRA is currently being used to provide a basis to remove the poison-injection tank from the Technical Specifications.

The PRA has also been used to address the need for and degree of compliance to recent DOE orders, codes, and standards as they affect an older plant such as HFIR. In several cases, the PRA was used to provide a risk perspective in sections of the SAR that address these recent requirements.

The PRA has also been used to provide an analytical basis for the continued transport of heavy loads during refueling activities at the HFIR. Seismic and high-wind event preventative/mitigative upgrades were also dictated by the PRA.

The modified level 3^2 analysis was used as a basis for an unreviewed safety question determination for several issues that evolved from the SAR upgrade analysis.

Finally, the PRA has most recently been used to change the frequency of a technical specification surveillance procedure as described below.

To reduce unscheduled shutdowns at the High Flux Isotope Reactor (HFIR), it was proposed that the periodic testing frequency for the HFIR protection system be decreased. Over the years, a number of unscheduled shutdowns have occurred during these safety tests, primarily due to the high sensitivity of the HFIR protection system and the test configuration of the channel undergoing test. The HFIR has three safety channels which normally function as a 2-out-of-3 general coincidence trip logic to trip the reactor. However, during safety channel tests, the channel undergoing testing is placed in a "tripped" condition and all trip parameters for that channel (e. g., flux, pressures, temperatures, etc.) are tested. This tripping of the channel being tested effectively changes the protection system to a 1-out-of-2 logic. Thus, any signal, including signal noise, on either of the two operational channels during the test will result in trip of the reactor. Over the years, this situation has resulted in many unnecessary trips of the reactor. With a 20- to 30-minute window before xenon buildup (significant enough to prevent recriticality), the likelihood for an extended shutdown ($\sim$60 hours) deriving from a safety channel test was considerable. This led to a need to reduce the frequency of placing the trip system in the test mode.

The previous testing requirements for the HFIR safety channels were specified in the HFIR technical specifications and required the channels to be tested once per week using a simultaneous testing pattern (each of the channels was tested sequentially).

For a two-out-of-three channel logic using simultaneous testing, the system unavailability can be calculated by the formula found in Table 2 of ANSI/IEEE Std. 352-1987:

$$\bar{A} = (\lambda\,\theta)^2$$

where,

$\bar{A}$ = Overall unavailability goal of the HFIR protection system
λ = Failure rate of an individual safety channel
θ = Test interval

This formula was used to calculate the acceptable test interval given a HFIR protection system unavailability goal and the failure rate for a single channel.

From HFIR PRA, the demand frequency of the protection system to fail to trip was estimated to be approximately 3.6×10^{-5}. This value was estimated using industry and HFIR-

specific failure data. The failure value of 3.6×10^{-5} includes both independent and dependent failure mechanisms of the protection system components and instrumentation from the sensors to the safety plates. Of this 3.6×10^{-5} total, there is a 3.7×10^{-6} contribution from a common mode mechanical failure of the safety plates to drop which is a failure mode unrelated to failure of the HFIR protection system. Consequently, the portion of the overall protection system failure attributable to failure of the safety channels instrumentation is:

$$3.6 \times 10^{-5} - 3.7 \times 10^{-6} = 3.2 \times 10^{-5}$$

This value of 3.2×10^{-5} was used as the unavailability goal for calculating the new test interval for the HFIR protection system.

The failure rate for the individual safety channels was estimated by an examination of the quarterly and weekly reports for the HFIR operational period from January 1968 to July 1992. Significant shutdown periods were not included in the data base. Failures of components that have been replaced with a completely different type of component were also not included in the failure database. The plant shift supervisor log books were also examined to provide additional information and clarification to the quarterly and weekly report data.

Failures pertinent to this evaluation were those that were unannounced to the operators and were not identified until the performance of the protection system test. Announced failures are defined as those failures where it was apparent from indications in the control room that some sort of failure had occurred. Also, abnormal plant parameter indications would most likely be detected during the operator's hourly control room parameter recording requirements. Therefore, announced failures of the protection system were not considered to be failures for the purposes of this evaluation. The potential unannounced failure events were then reviewed by experienced HFIR design and operations personnel from the Research Reactors Division and personnel from the Instrument and Control Division.

As a result of these reviews, four unannounced failures were identified. The failure rate for the safety channels was calculated by taking the total number of unannounced failures and the total operating hours over which those failures were obtained, multiplied by 3 for three safety channels, and performing a Bayesian estimation of the protection system failure frequency. The total protection system operating hours used in the estimation was 458,436 hours. From this estimation process, a channel failure rate of 8.3×10^{-6} per hour was obtained.

The unavailability goal for the HFIR protection system ($\bar{A} = 3.2 \times 10^{-5}$) and the failure rate for an individual safety channel ($\lambda = 8.3 \times 10^{-6}$/hr) were then used in the formula above to estimate θ. Substitution of values produces the following equation:

$$\sqrt{3.2 \times 10^{-5}} = 8.3 \times 10^{-6}/hr \times \theta$$

Solving for θ gives a value of 681 hours or 681/24 = 28 days.

Because the HFIR has a operating cycle of approximately 21 days, this calculated test frequency of 28 days allows the HFIR to perform its safety channel tests at the time of startup for a new fuel cycle when xenon is not yet a problem, and run for an entire cycle without retesting. Using this evaluation as the basis for the change, the HFIR staff formally requested a change in the HFIR technical specifications to extend safety channel test frequency from once every 7 days to once every 28 days. On May 14, 1993, DOE approved this request.

This latter application resulted in a significant increase in operational availability and avoided costly design changes.

CONCLUSIONS

As originally planned, the PRA has been and continues to be an invaluable tool in addressing risk management issues at the HFIR, ranging from safety, design, operations, testing, and regulations.

ORNL has also used limited risk assessments to address specific issues at the smaller "B" reactors. The positive experience gained with the PRA at HFIR has led to a commitment to use the PRA as an integral part of the design and safety process for the Advanced Neutron Source Reactor currently being designed at ORNL.

REFERENCES

1. D. H. Johnson, et al., *The High Flux Isotope Reactor Probabilistic Risk Assessment*, ORNL/RRD/INT-36, Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab., January 1988.

2. C. E. Winters, et al., *The High Flux Isotope Reactor Accident Analysis*, ORNL-3573, Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab., 1967.

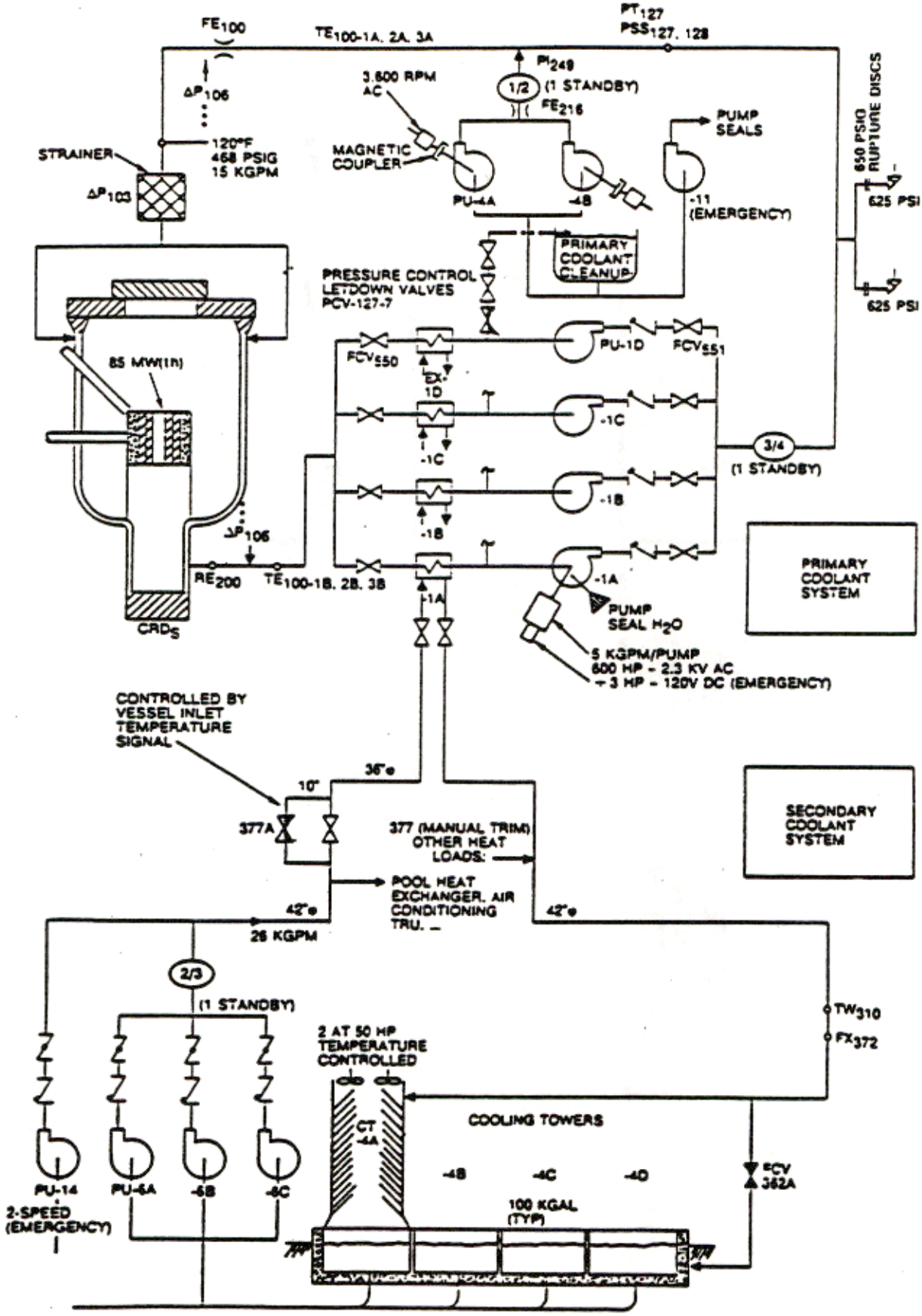


Figure 1. Simplified HFIR process flow diagram.

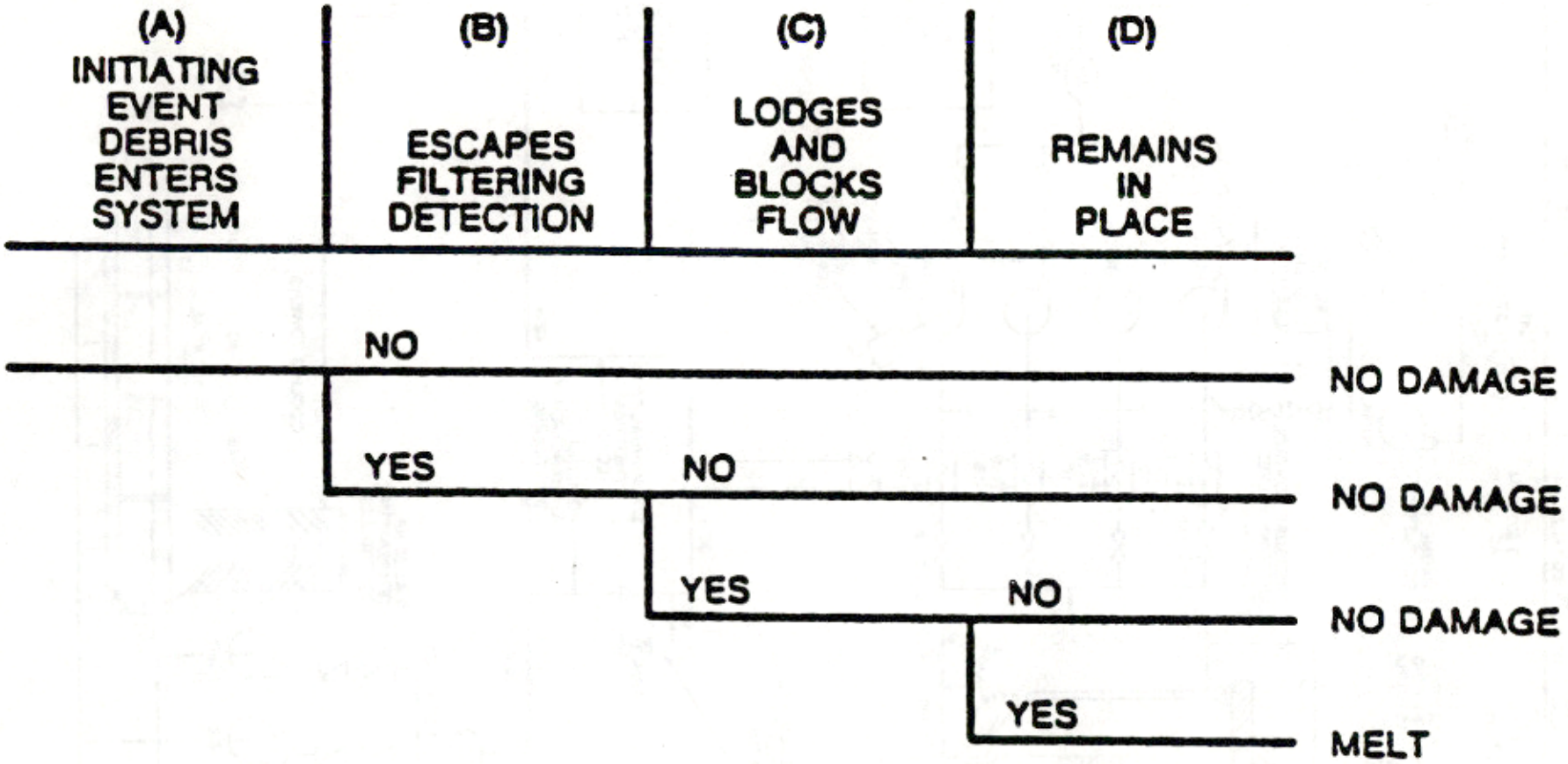


Figure 2. Event tree showing general form of flow blockage scenario logic.

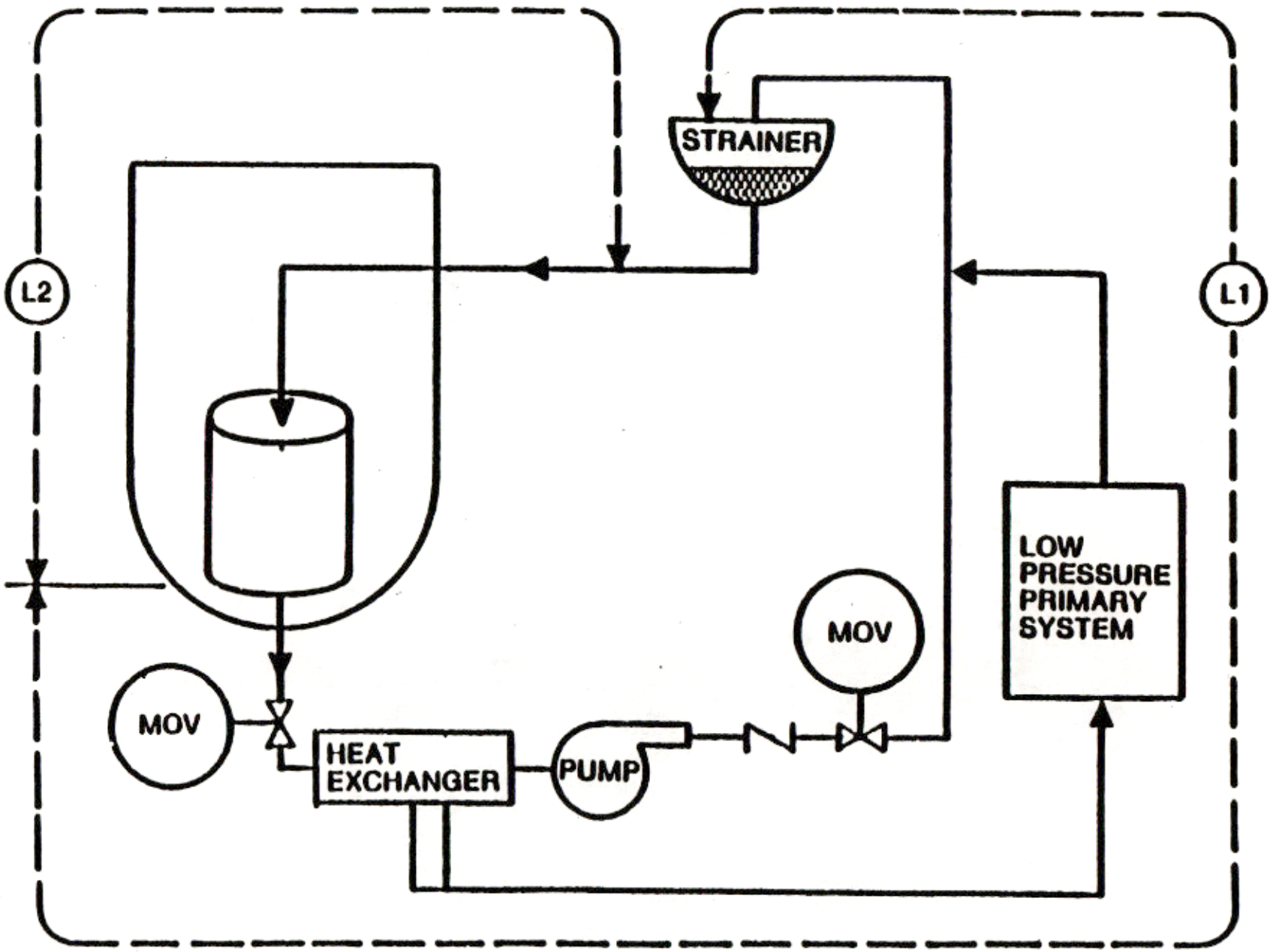
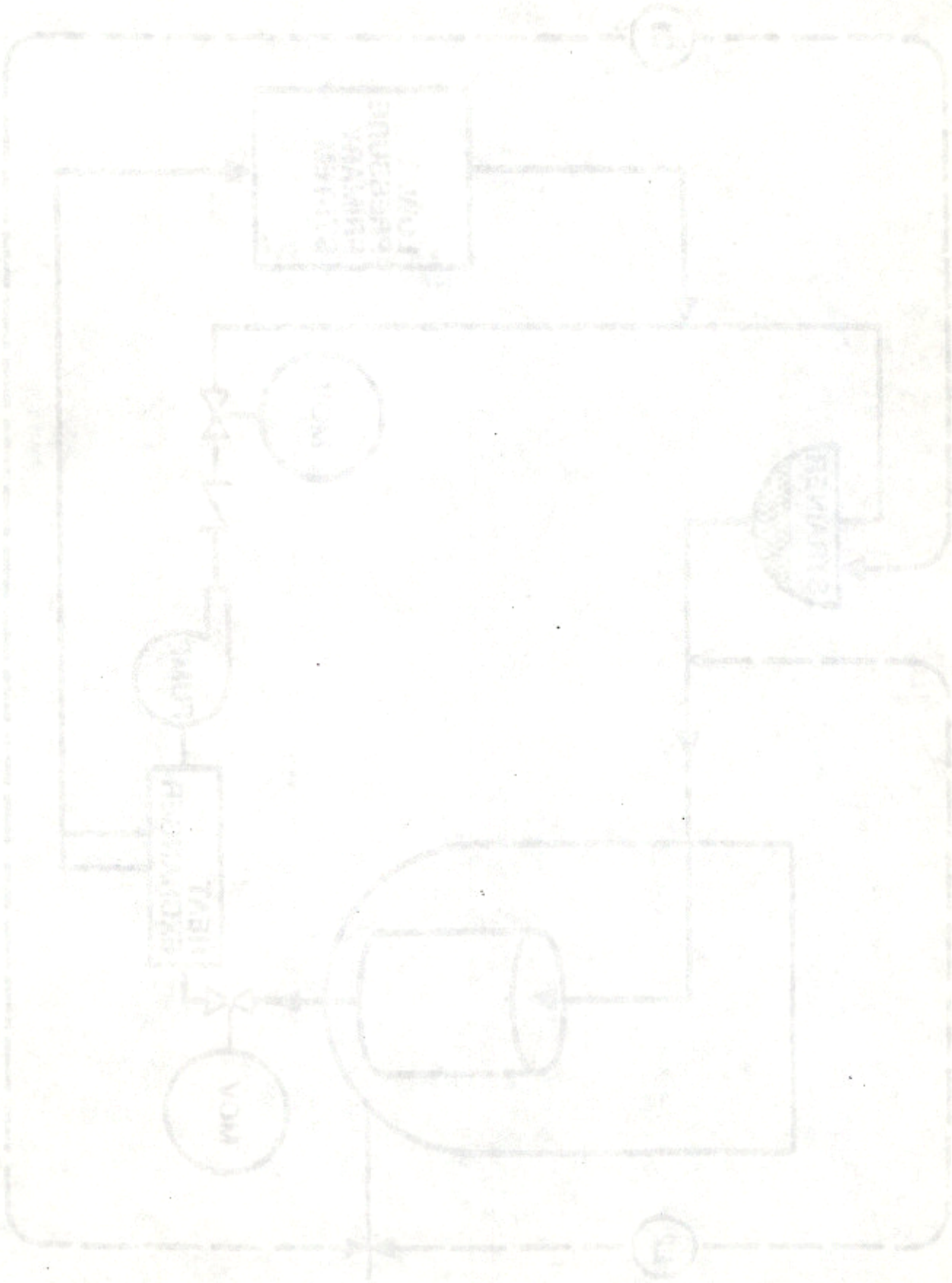


Figure 3. Primary flow loop schematic showing breakdown into location categories 1.2 and 1.3.



RISK MANAGEMENT AT LLNL[1]

Garth E. Cummings and R. Scott Strait

Lawrence Livermore National Laboratory
Livermore, California 94551

INTRODUCTION

Managing risks at a large national laboratory presents a unique set of challenges. These challenges include the management of a broad diversity of activities, the need to balance researcher flexibility against management control, and a plethora of requirements flowing from regulatory and oversight bodies. This paper will present the experiences of Lawrence Livermore National Laboratory (LLNL) in risk management and in dealing with these challenges. While general risk management has been practiced successfully by all levels of Laboratory management, this talk will focus on the Laboratory's use of probabilistic safety assessment and prioritization techniques and the integration of these techniques into Laboratory operations.

Probabilistic safety assessment and prioritization techniques are applied at LLNL in five general areas: (1) facility operations; (2) functional management; (3) program management; (4) budgeting and (5) work for outside sponsors. This paper will focus on LLNL risk management in the first four areas, i.e., those that are internally focused. However, the Laboratory does provide a wide range of risk analysis research and application capabilities for outside sponsors, mostly the DOE and other Federal agencies, and LLNL expertise in many areas of risk assessment is widely recognized. For example, risk assessment methods have been developed at LLNL for estimating seismic risk at commercial nuclear power plants and DOE facilities and to help in the safeguarding of nuclear materials at DOE and commercial nuclear facilities (Cummings and Al-Ayat, 1989). Another example is the environmental risk assessment methods being developed for the

[1]Work performed under the auspices of the U.S. Department of Energy by the Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

State of California Environmental Protection Agency (McKone, 1993) and for the DOE (Daniels, 1993).

FACILITY OPERATIONS

The use of probabilistic safety assessment techniques at the facility operations level is part of a multi-step process of categorizing the hazards of individual LLNL facilities, identifying the higher hazard facilities, preparing safety analysis reports, and performing in-depth risk analysis of important aspects of the facilities. Often, such risk analyses are done for specific purposes, including the evaluation of facility upgrades. The focus of such analyses is usually safety systems designed to protect employee and public health. An example of such an analysis is the fault-tree analysis of the Plutonium Facility's electrical distribution system.

There are several levels of risk analysis done for LLNL facilities depending on the potential for harm of the hazard involved. For all facilities with a hazard classification and for other prescribed hazardous operations, the Laboratory requires that safety procedures be written. These procedures are of two types. Facility Safety Procedures (FSP) define basic ground rules to be followed in a facility. Operational Safety Procedures (OSP) are specific to a particular activity and are used to add to or modify FSP requirements. Both types of procedures require a qualitative evaluation of risk. The level of approval is graduated depending upon the level of risk involved.

In recent safety analyses a risk matrix has been constructed and used to determine the acceptability of results. In this approach bounding accidents are postulated, a subjective estimate made of their probability of occurrence and their consequences quantitatively evaluated. Each accident is put into a bin based on its probability level (4 levels) and consequence rating (4 levels) and each bin defined as either of high, medium, low or negligible risk. Safety features are added and Operational Safety Requirements defined to assure that all accidents are of low or negligible risk.

Such a risk matrix was constructed for LLNL's High Explosives Application Facility, which supports HE formulation and testing to 10 kg quantities. Formal analysis of consequences were performed on eight identifies hazards, e.g., HE transport, seismic, and six bounding accidents, e.g., explosive detonation, toxic material spill, fire. Of these six bounding accidents, only one fell into the low risk bin. The others were in negligible risk bins (Morse and Weingert, 1989).

Probabilistic safety assessment techniques have been used to analyze specific types of hazards such as an aircraft accident involving our Plutonium Facility and a toxic gas release from our Microfabrication Facility. The aircraft accident study (Vogt, 1991) was done to support accident analyses for the LLNL Environmental Impact Statement/Environmental Impact Report published in 1992.

Since the 1980 Livermore earthquake, whose epicenter was located a few miles from LLNL, extensive upgrades and retrofits have been made to certain LLNL facilities. Although risk assessments were not done to support the selection of these modifications the choices were based, in part, on risk assessment results. More recent upgrades and evaluations are based on seismic design guides prepared by LLNL for use at DOE facilities (Kennedy, 1990). These are based on both risk assessment experience as well as engineering judgment.

FUNCTIONAL MANAGEMENT

Risk assessment techniques are a key part of functional management in several areas of Lab operations. The environmental protection department personnel use probabilistic safety assessment techniques for monitoring and managing environmental issues. Often these risk analyses are done to respond to requests from regulators. They vary in size and complexity from large, comprehensive models of the transport and health effects of Superfund Site groundwater contamination to pro forma analyses required by the Clean Air Act. Frequently, risk analyses are required by the NEPA for new Laboratory facilities and operations.

Safeguards and Security Department personnel use probabilistic safety assessment techniques to prioritize their efforts and to choose among alternative procedures. Formal risk assessments for the vulnerabilities of key facilities against malevolent acts, particularly attempted theft of nuclear materials, are performed and updated regularly. Following DOE policy, these assessments estimate the probability of a successful malevolent act assuming that such an act is attempted. The probability of adversary success is determined using traditional risk assessment techniques, including fault trees. However, unlike most safety risk assessments, the adversaries are assumed to be rational and to maximize their probability of success. These analyses are often facilitated by the use of the ASSESS methodology and computer software for performing vulnerability assessments (Al-Ayat, Cousins, and Matter, 1989). The Laboratory risk, as determined by these risk assessments, is an important part of the Laboratory's Site Safeguards and Security Plan that is approved by DOE and is a large factor in DOE's assessment of Laboratory safeguards and security performance. Risk reduction as determined by such risk assessments is the means for ascertaining the cost effectiveness of upgrades and adjustments to the Laboratory safeguards and security system.

PROGRAM MANAGEMENT

Several large Laboratory programs use probabilistic safety assessment techniques to choose among alternative technical directions, particularly when the options vary greatly in the end technologies' impacts on safety and health. One example is the choice of enhanced safety concepts to incorporate into existing nuclear weapons or into possible future designs (Bookless, 1992). Both existing and proposed weapons systems are analyzed using techniques of varying complexity. Probabilistic safety assessment techniques, similar to what were developed for nuclear reactor safety studies, are used to assess risk scenarios involving weapons. First, accident scenarios are identified and their occurrence frequencies estimated. Second, calculations and experiments are used to assess the environment created by the accident. Third, the weapon's response is calculated using chemical, thermal, and structural computer codes. Fourth, the amount of radioactive material release and the consequences of that release are estimated.

Because few of the probabilities are precise, probabilistic safety assessment is viewed as a tool to make relative evaluations of nuclear weapons systems, not as an absolute measure of the risk associated with a given system. Assessment

results are used to identify those operations that present the highest risk, to judge the value of design features in reducing risk, and to assess the effectiveness of operational measures in reducing risks.

BUDGETING

Risk-based prioritization is playing an increasing role in Laboratory overhead budgeting. Last year the Plant Operations Directorate, which includes the Laboratory's plant engineering and environmental, safety, and health support departments, used a "risk totem" approach (Grose, 1987) to allocate funding among departments. This year most of the Laboratory's indirect overhead budget, including Plant Operations, was evaluated using averted risk and a multi-attribute utility function. (The Laboratory's indirect overhead budget is in excess of $200 million.) All activities covered by the budget were defined functionally using a work breakdown structure, the risk reduction expected from funding each activity was analyzed, and activities were prioritized according to their benefit (i.e., risk reduction) to cost ratios.

Risk reduction from overhead budget items were evaluated in ten areas, reflecting Laboratory management's objectives for overhead funding:

Employee health and safety
Public health and safety
Environment
Safeguards and security
Regulatory compliance
Public concerns and understanding
Employee skills and motivation
Facilities and equipment
Business management
Mission objectives

For each of these areas, criteria and scales were developed to measure how an activity contributes to risk reduction. In some instances, the appropriate unit of measurement was readily available, but for others, special scales needed to be constructed. A multi-attribute utility function was assessed from Laboratory management and used to aggregate the scores for each activity to obtain an overall measure of the benefit of each activity. The utility function is a mathematical formula that reflects the Laboratory management's value judgments about the relative desirability of different levels of risk reduction in each area, and the relative importance of the different types of risk reduction (Keeney and Raiffa, 1976).

Each overhead organization was responsible for developing its own work breakdown structure and scoring its own budget activities on the risk reduction scales and criteria. The 1994 indirect overhead budget consisted of over 700 separate budget items to be evaluated. Training was given to appropriate staff; software was provided for documenting budget activities and facilitating scoring; and guidance and advice was available upon request. The documentation and scoring was then collected in a central database and analyzed by the Laboratory Budget Office. The initial prioritizations were distributed to the overhead

organizations for review, revision of scores, and qualitative re-prioritization of budget items judged to be improperly evaluated by the quantitative model. All such qualitative re-prioritizations were justified and documented.

Based on the experience with the 1994 overhead budget, the Laboratory is considering a number of changes to the process for the 1995 budget. These include improvements in the model for measuring risk reduction; adoption of a two-tiered approach with different levels of detail; and centralization of scoring to improve its consistency and accuracy.

A similar risk-based prioritization approach is also used to schedule responses to recommendations and findings by outside review groups (e.g. DOE "Tiger Teams"). Within the constraints of a fixed budget, this helps ensure that the most cost effective actions are performed first. For such prioritizations, risk reduction is usually evaluated for a more narrow set of objectives commensurate with the more limited nature of the activities. In most of these exercises, scoring was performed by a single group of individuals.

CONCLUSIONS

LLNL has always carefully assessed the risks of its activities to assure proper protection of its workers and the public. These assessments have and continue to take different forms depending on the nature and severity of the risks involved. In the early days of the Laboratory, risk assessment tended to be informal and based on the informed judgment of the scientists involved. This was suitable when risk management techniques were in their infancy and the analysis of the researchers involved was often the best guide to the safeguards required.

As technologies matured more formal analyses were required in both safety documentation and risk assessment. This process is still evolving and is becoming more comprehensive as regulatory bodies push for more accurate quantification of the risk being accepted on behalf of the activity undertaken.

REFERENCES

Al-Ayat, R., T. Cousins, and J. Matter, 1989, "An Overview of ASSESS - Analytic System and Software for Evaluating Safeguards and Security," *Proceedings of the 30th Annual Meeting of the Institute of Nuclear Materials Management*, Vol. XVIII, July 1989.

Bookless, W.A., 1992, "Nuclear Weapons Safety," *Energy & Technology Review* (UCRL-52000-92-1.2)

Cummings, G.E. and Al-Ayat, R.A., 1989, "Designing Effective Protection Against Threats at Nuclear Facilities (UCRL-101627)", Conference on Technology-Based Confidence Building: Energy and the Environment, Santa Fe, New Mexico, July 9-14, 1989

Daniels, J. I., Editor, 1993, *Pilot Study Risk Assessment for Selected Problems at the Nevada Test Site (NTS)*, Lawrence Livermore National Laboratory, Livermore, CA, UCRL-LR-113891

Grose, V.L., 1987, *Managing Risk: Systematic Loss Prevention for Executives*, Prentice Hall, New York

Keeney, R and H. Raiffa, 1976, *Decisions with Multiple Objectives*, Wiley, New York.

Kennedy, R.P. et al., 1990, *Guidelines for Department of Energy Facilities Subjected to Natural Phenomena Hazards*, Lawrence Livermore National Laboratory, Livermore, CA, UCRL-15910

McKone, T.E., 1993, *CalTOX, A Multimedia Total-Exposure Model for Hazardous-Wastes Sites - Part I: Executive Summary*, Lawrence Livermore National Laboratory, Livermore, CA, UCRL-CR-111456PtI

Morse, J.L. and Weingert, R.C., 1989, *High Explosive Application Facility (HEAF), Final Safety Analysis Report*, Lawrence Livermore National Laboratory, Livermore, CA

Vogt, D.K. et. al., 1991, *Report on Aircraft Accident Probability Study Using Typical EIS Aircraft Accident Analysis Methodology for Building 332*, Lawrence Livermore National Laboratory, CA, UCRL-CR-108423

RISK MANAGEMENT AT LOS ALAMOS NATIONAL LABORATORY

Daniel G. Brooks

Arizona State University
Tempe, AZ 85287-4206

Desmond W. Stack

Los Alamos National Laboratory
Engineering and Safety Analysis Group
Los Alamos, NM 87515

INTRODUCTION

Los Alamos National Laboratory has risk management programs at a number of administrative levels. Each line organization has responsibility for risk management for routine operations. The Facility Risk Management Group is the Los Alamos organization having primary responsibility for risk management, including providing input and expertise to facilities and line managers in the management and documentation of ES&H hazards and risks associated with existing and new activities. This includes program plans and schedules for implementing nuclear facility orders that involve risk management such as SAR (DOE 5480.23), TSR (DOE 5489.22), USQ (DOE 5480.21), and ORR(ALSD 54XA). One of the major contributions this group has made to the Laboratory risk management program is to develop and implement a hazard identification and classification methodology that is readily adaptable to continuously changing classification guidelines such as DOE-STD-1027. This methodology is described in Ref. 1.

The increased emphasis on safety at Los Alamos has led to the formation of additional safety oversight organizations such as the Integration and Coordination Office (ICO), which is responsible for prioritizing risk management activities. In the fall of 1991, nearly 170 DOE inspectors spent 6 weeks analyzing the environmental, safety, and health activities at Los Alamos. This audit resulted in a list of over 1000 findings, each indicating some deficiency in current Laboratory operations relative to DOE and other government regulation. The audit team's findings were consolidated and "action plans" were developed to address the findings. This resulted in over 200 action plans with a total estimated cost of almost $1 billion. The Laboratory adopted a risk-based prioritization process to attempt to achieve as much risk reduction as possible with the available resources. This paper describes the risk-based prioritization model that was developed

METHODOLOGY

The methodology developed for the risk-based prioritization process is based on multiattribute preference theory. Multiattribute preference theory provides a logical and consistent

basis for solving prioritization problems. The methodology quantifies uncertainty as probabilities, using the axiomatic logic of probability theory dating back to the 1700s. It quantifies objectives and values using axiomatic reasoning developed by John von Neumann in the 1940s during the time when he was working at Los Alamos on the Manhattan Project. Together, these two methodologies allow the user to combine the technical assessments of scientists with the policy judgments of risk managers. The approach ensures that prioritization decisions have documented objectives and technical assessments and an "auditable" logic to support the choices made by the decision makers.

Although several of the methodologies reviewed by the Laboratory claimed to be based on multiattribute preference theory, few actually were. Most of these methodologies confuse multiple-criteria models—models having more than one evaluation criterion scored and then combined to give an overall evaluation score—with multicriteria models that are in fact based on the axioms of multiattribute theory. Independent outside technical review committees studied the application of multiattribute theory to the prioritization problem at the Laboratory, and the National Academy of Science reviewed the appropriateness of the application of the theory as it is to the prioritization problem within DOE.

Evaluation Categories

The development of a model to quantify the benefits of averting risk begins with the determination of the evaluation categories to be included in the definition of risk. Because the Laboratory was interested in the full spectrum of undesirable ES&H occurrences, senior management eventually identified the categories shown in Fig. 1 as being complete in representing "risk."

These categories resulted from a series of interviews with Laboratory Associate Directors and ES&H Council members. After the first round of interviews, further interaction with special technical groups helped provide more detailed and quantitative descriptions of the categories. For example, a Laboratory organization called "Our Common Ground," devoted to working with the Laboratory community to understand their concerns and the Laboratory's role in influencing their quality of life, was consulted as the basis for developing an operational way of measuring community concerns. Laboratory legal council was consulted in developing measures of compliance issues, and health and safety managers were involved in health and safety measures. The full development of evaluation criteria is shown in Fig. 2.

Measurement Scales and Value Functions

A series of meetings with Laboratory subject matter experts in each of the categories produced a quantitative measurement scale for each evaluation criterion. These scales measure

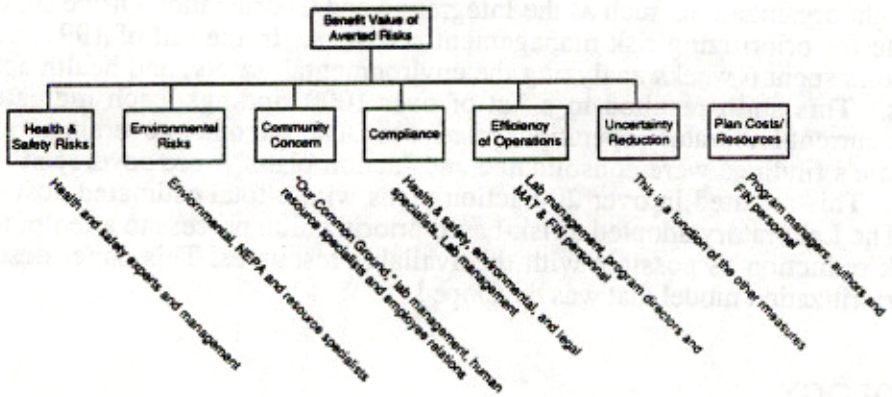


Fig. 1

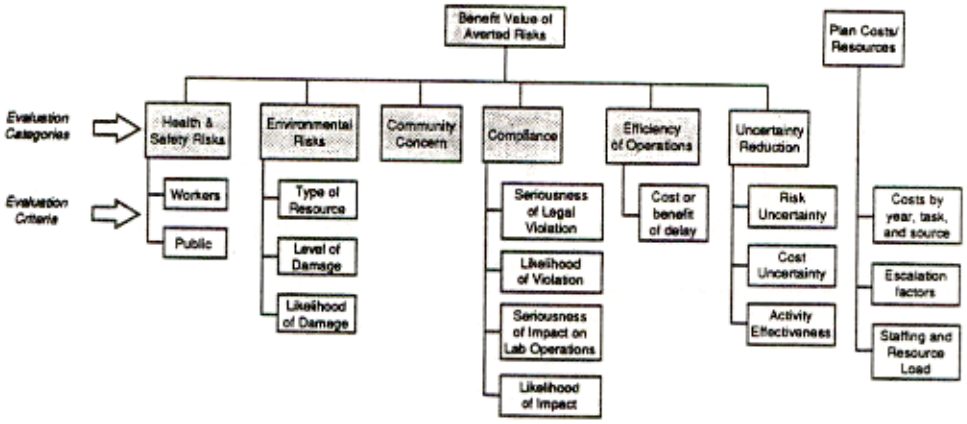


Figure 2. Risks are defined by the set of evaluation categories.

the degree to which an action plan addresses the evaluation criterion. The measurement scales and value functions for worker health and safety, public health and safety, and environmental insult are described below.

Quantifying Worker Health and Safety Risks

Worker health and safety risks are quantified using a simplified health-risk assessment model developed with the health and safety technical experts at the Laboratory. The model is as follows.

Severity of Effect	x	Probability of Exposure	x	Probability of Effect Given Exposure	x	Number of Workers at Risk	x	Time of Exposure

The measurement scales and associated value functions for each of the evaluation criteria are shown in Fig. 3.

Multiplying these scales yields an estimate of the expected number of "effects," which is quantified next. The "severity of effect" scale was quantified by eliciting from Laboratory Senior Management, using standard decision analytic procedures, the value of preventing each of the effects relative to a standardize tradeoff activity (in this case, number of jobs lost as a result of higher costs of doing business in the marginally safer environment).
The Laboratory's value function for severity of health effects is given in Fig. 4.

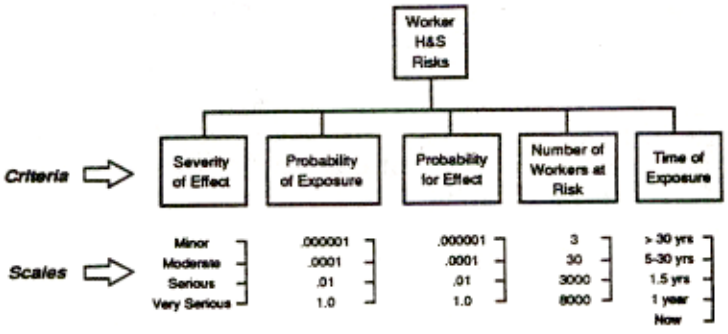


Fig. 3

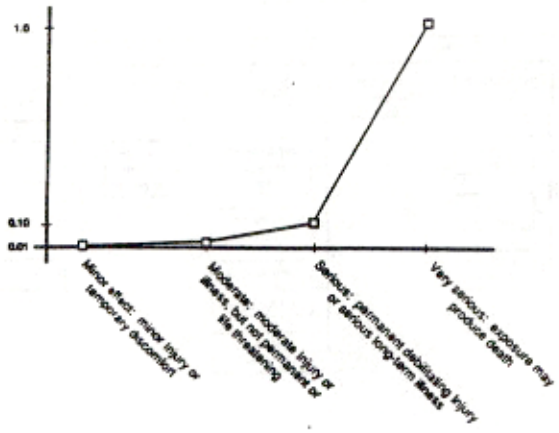


Figure 4. Value function showing the relative value of preventing health effects.

The value function is scaled to the range of 0 to 1 because the tradeoff coefficients will reflect the relative importance of each of the categories. From this value function, it is clear that the value tradeoff between statistical fatalities and permanent debilitating injuries is 10 injuries to 1 statistical fatality. The implication is that a health and safety risk to workers with an expected outcome of 20 debilitating injuries is worse, in the value structure of Laboratory management, than a health and safety risk with an expected outcome of 1 statistical fatality for example. The important point about the model made here is that although fatalities are worse than permanent debilitating injuries, a fatality by itself is not worse than *any number* of permanent debilitating injuries.

The computation of the expected number of statistical fatality equivalents for each activity allows noninteger scores on each of the scales. The computer calculation uses either linear or geometric interpolation, as appropriate, for assigning values for intermediate scores on each of the scales.

Quantifying Pubic Health and Safety Risks

Health and safety risks to the public are quantified in the same way, except that the population at risk can be much larger—up to the population of Los Alamos County. Figure 5 shows the quantification logic for the public health and safety risk category.

Quantifying Environmental Risks

A measurement scale based on sensitive environmental resources was developed by adapting an appropriate structure from "Final Hazard Ranking System for Uncontrolled, Hazardous Substance Releases, Final Rule," from U.S. EPA, 1990, in the *Federal Register.* The scale is applied to each instance of a sensitive resource affected by an activity. If a single resource qualifies for two different scores (e.g., a resource on both the state and Federal registers), then the scores are added. The use of this scale is illustrated in Fig. 6, and the logic for the full quantification is shown in Fig. 7.

Measuring Risk (The "Risk Scoring" Process)

The person most familiar with each action plan uses the measurement scales to "score" the effect on total risk if the action plan is implemented. The scorers provide two sets of scores for each plan: the first set gives an estimate of the "baseline risk," the risk level if the deficiencies addressed by the action plan were left alone; the second set estimates the the ct on total risk if the action plan is implemented. The scorers provide two sets of modi

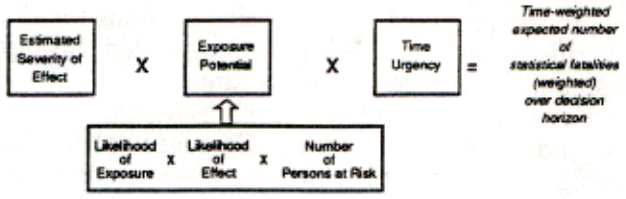


Figure 5. Logic for quantifying health and safety effects.

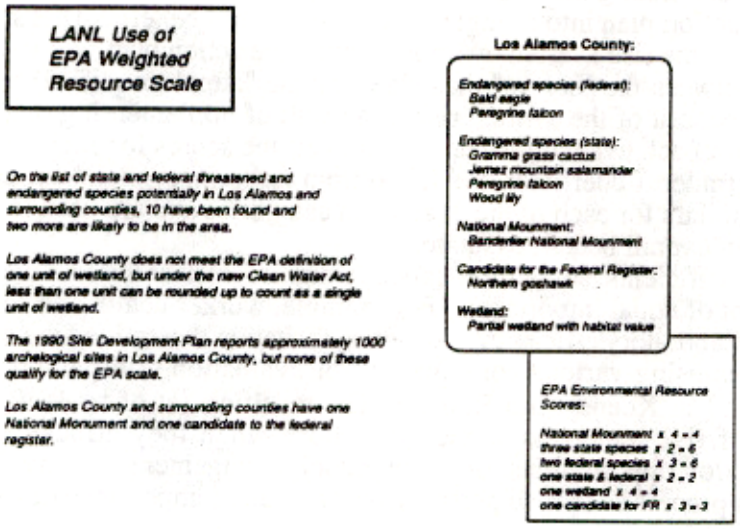
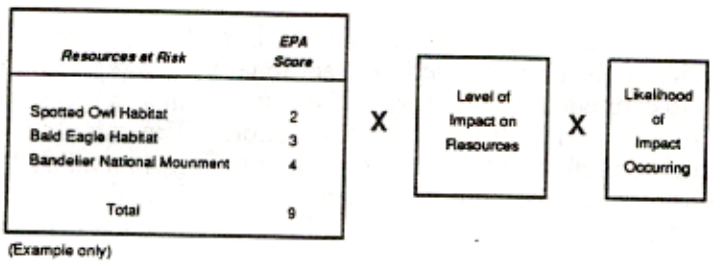


Figure 6. Use of adapted EPA scale for quantifying the value of sensitive environmental resources.



(Example only)

Fig. 7

fied risk, the risk level after the action plan is fully implemented. The difference between these two sets of scores is the averted risk attributable to the action plan.

The scoring process was not designed to be conducted as a "mail-out questionnaire." A team overseeing the scoring process provided group training sessions for all action plan scorers, and then individual training was needed. Help was provided throughout the scoring process and many scorers came in for guided scoring sessions.

There is always the concern that the person scoring an action plan, although well informed about the plan, may not score it objectively. To guard against this kind of "advocacy" scoring, both the scoring process and the resulting scores were reviewed thoroughly. The underlying value model is not known to the scorers, so "gaming" the system to get a higher score is not a straightforward process because the best way to "game" the system is not known. Moreover, because the scores are subject to repeated reviews, it is very difficult for scores not supported by data and logic to remain unchanged.

The scoring was reviewed to control internal consistency across evaluation criteria (this is within-action-plan variance) and to control consistency across action plans (this is between-action-plan variation).

Combining Evaluation Measurements

The next step in estimating the overall value of an action plan is combining the scores associated with each action plan into a single measure of overall benefit. This single number represents the benefit of the risk averted by implementing the action plan.

The difference between the "before" (baseline) and the "after" (modified) risk scores for an action plan is the benefit of the averted risk as a result of implementing that action plan. The value functions for each evaluation category convert the scores for each category into a value measure. The tradeoff coefficients, elicited from Laboratory management, represent the relative value in dollars for each of the evaluation categories and are used to combine the category scores into an overall benefit estimate.

These tradeoff coefficients, sometimes called "weights," reflect the fact that the evaluation categories are not of equal importance. For example, worker health and safety is much more important than Laboratory efficiency. A formal elicitation determined the set of weights for the risk categories using various combinations of evaluation criteria and full tradeoff questions as discussed in Keeney and Raiffa.[2] The resulting set of tradeoff coefficients reflects the values of risk managers at the Laboratory when they allocate resources to competing risk reduction opportunities. All Laboratory management was involved in some part of this elicitation process so that all perspectives on relative importance of risk categories were taken into account.

In addition to determining the relative weights for the evaluation categories, the assessments also produced a rule for combining these weighted risk category measures. By testing for preference independence and additive independence in a series of tradeoff exercises, it was determined that it was valid to use a linear combination of category scores.

Combining Benefit and Resource Estimates for an Action Plan

The relative priority of an action plan depends on both the benefits that it produces and the resources that it requires to be implemented. A traditional way to represent the attractiveness of an action plan is to estimate the net return of the action plan as a proportion of its total cost. This is one form of a "return on investment calculation." The calculation associates a single number with each action plan. The number is the benefit produced by the action plan divided by the cost to implement the plan. If an action plan's benefit is less than its total cost, this number is less than 1, indicating a return on investment that is less than the investment itself.

The straight prioritization of action plans can be based on ranking the action plans according to benefit-to-cost ratio. The implicit optimization rule for this approach is that we wish to optimize the risk reduced by each dollar spent. An alternative to this optimization rule is to optimize the total amount of benefit that can be obtained over a set of years and a set of budget constraints. Although each dollar spent in each year may not be optimal, the total benefit obtained over all the years is optimized.

Obtaining the Maximum Benefit for Given Resources

Selecting a set of action plans that yields the greatest total benefit for given resources (by year and by source) is an optimization problem sometimes referred to as a portfolio problem. Because resources come from different sources with different limitations in different years, it is not possible to just "follow a list" of action plan priorities based on benefit-to-cost ratio and stop when the money runs out. Instead, a collection of plans consistent with the funding sources and timing constraints must be determined to maximize the total benefit achievable. Linear (and integer) optimization computer codes can solve this problem and find the portfolio of action plans to implement for any set of resource constraints over the planning horizon.

To solve this portfolio optimization problem, it was formulated as a mixed-integer problem where small action plans can either be done or not in any given year (the integer portion of the problem), and large action plans can have yearly portions done without committing to the entire action plan for contiguous years (that means that later years can be delayed in implementation, although they must be done in the proper order; years can be skipped in the implementation of a plan, if necessary). Future costs were discounted at the Laboratory discount rate, and future benefits were discounted at the same rate. The solution of this optimization problem relied on a powerful library of optimization software capable of solving problems with thousands of action plans, funding sources (by time period), and constraints. The problem was solved using IBM's optimization software OSL (Optimization Software Library) on a large IBM personal computer.

CONCLUSIONS

The risk-pased prioritization procedure allowed the Laboratory to responsibly address all the ES&H risks identified by the DOE audit, systematically plan for the future implementation of action plans and document the basis upon which it allocates resources to reduce risk. The model provides an auditable system for defining risk, measuring its reduction, and effectively allocating resources over time. The model used to combine all this information into a decision-aiding tool is based on a sound methodological foundation of multiattribute preference theory. The procedure serves as a powerful communication tool for making the Laboratory's risk reduction objectives, priorities and risk measurements explicit.

REFERENCES

1. J. C. Elder, "Radiological Hazard Classification of DOE Facilities by DOE STD-1027-92:LANL Nuclear Facility List," Los Alamos National Laboratory report LA-UR-93-1366 (1993).

2. R. L. Keeney and H. Raiffa, "Decisions with Multiple Objectives: Preferences and Value Tradeoffs," John Wiley and Sons, New York (1976).

023 Environmental Consequence Analysis

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

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

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

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

MACCS USAGE AT ROCKY FLATS PLANT FOR CONSEQUENCE ANALYSIS OF POSTULATED ACCIDENTS

Terry L. Foppe and Vern L. Peterson

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

ABSTRACT

The MELCOR Accident Consequence Code System (MACCS) has been applied to the radiological consequence assessment of potential accidents from a non-reactor nuclear facility. MACCS has been used in a variety of applications to evaluate radiological dose and health effects to the public from postulated plutonium releases and from postulated criticalities. These applications were conducted to support deterministic and probabilistic accident analyses for safety analysis reports, radiological sabotage studies, and other regulatory requests.

INTRODUCTION

The MELCOR Accident Consequence Code System (MACCS)[1] has been adopted as the Rocky Flats Plant (RFP) standard for analyzing the consequences to the public of postulated accidental releases of radionuclides, including plutonium (Pu) and fission products from metal and solution criticalities. This paper discusses the various uses to which MACCS has been put at RFP, including both probabilistic and deterministic calculations. (A site-specific code, known as the Terrain Responsive Atmospheric Code, has also been developed for similar purposes. It is still awaiting approval by the Department of Energy (DOE) and the Colorado Department of Health.)

CAPABILITIES

MACCS was developed at the Sandia National Laboratories for the Nuclear Regulatory Commission (NRC) for the evaluation of the consequences to the public

of accidents at nuclear power plants. It has also been adopted for use at a number of DOE nuclear facilities. It uses the straight-line Gaussian plume model for a flat terrain to compute the transport and diffusion of radionuclides and the dose conversion factors derived from the ICRP-26[2] and ICRP-30[3] reports to evaluate the doses and health consequences from inhalation, ingestion, groundshine, and cloudshine, including both acute and chronic health effects. The most common scenarios evaluated using MACCS deal with an atmospheric release of small quantities of Pu. Table 1 gives the isotopic mix of generic weapons-grade Pu, the activities and half lives of these isotopes, and the inhalation dose conversion factors (DCFs) for the three most important organs for Pu exposure (lungs, liver, and skeleton) and for CEDE, as taken from the input files used by MACCS. The DCFs are shown for two dose commitment periods, 50 years and 70 years. The 50-year commitment period is used for Safety Analysis Reports (SARs) and the 70-year commitment period for Environmental Assessments (EAs). The DCFs shown in Table 1 are taken from the latest version of MACCS, soon to be released, called MACCS2; the DCFs used in earlier versions of MACCS are slightly smaller, except for lungs, for which the DCFs are essentially the same.

TABLE 1. Isotopic Mix of Generic Weapons-Grade Plutonium. For the DCFs, the first entry is for a 50-year commitment period and the second for 70 years.

Isotope	Activity (Ci/gram)	Half-Life (years)	Inhalation Dose Conversion Factors 50-year and 70-year commitments (rem/Ci)			
			Lungs	Liver	Skeleton	CEDE
^{238}Pu	5.00×10^{-3}	87.74	1.2×10^{9} 1.3×10^{9}	6.8×10^{8} 8.1×10^{8}	3.1×10^{9} 3.9×10^{9}	3.1×10^{8} 3.7×10^{8}
^{239}Pu	5.76×10^{-1}	24,065	1.2×10^{9} 1.3×10^{9}	8.7×10^{8} 9.6×10^{8}	3.5×10^{9} 4.7×10^{9}	3.4×10^{8} 4.2×10^{8}
^{240}Pu	1.29×10^{-2}	6537	1.2×10^{9} 1.3×10^{9}	7.7×10^{8} 9.5×10^{8}	3.5×10^{9} 4.7×10^{9}	3.4×10^{8} 4.2×10^{8}
^{241}Pu	3.36×10^{-1}	14.4	1.2×10^{7} 1.6×10^{7}	1.6×10^{7} 2.2×10^{7}	7.8×10^{7} 1.2×10^{8}	5.7×10^{6} 8.3×10^{6}
^{242}Pu	1.20×10^{-6}	37,630	1.1×10^{9} 1.3×10^{9}	7.3×10^{8} 9.1×10^{8}	3.3×10^{9} 4.5×10^{9}	3.2×10^{8} 4.0×10^{8}
^{241}Am	6.00×10^{-4}	432.2	6.9×10^{7} 6.9×10^{7}	2.0×10^{9} 2.4×10^{9}	9.5×10^{9} 1.2×10^{10}	5.3×10^{8} 6.8×10^{8}

MACCS gives the user a great deal of flexibility in choosing the parameters of the computations and what type of output is desired. Of particular interest is the flexibility offered in the use of weather data. For deterministic calculations, three options are offered: user-selected constant weather; a user-created variable weather sequence; and, a user-selected starting time from real weather data in which 120 hours of weather data are processed. For the probabilistic calculations, two options are offered, both of which involve random sampling of weather data throughout the year: a Monte-Carlo, latin-hypercube sampling of one-year of weather data that has been "binned" according to stability class, wind speed, and precipitation; and, a random sampling of starting times from each day of the year. For the probabilistic calculations, only the weather is considered the uncertain variable; other uncertainties, such as in source term, deposition rates, or release rate, must be calculated outside of MACCS. Multiple runs with MACCS, bracketing these uncertainties, could then be performed.

The output from MACCS is under user control. The usual output includes centerline doses and health risks as a function of distance from the accident site, the total population dose and number of cancer fatalities within 50 miles of RFP, and the dose to the Maximum Offsite Individual (MOI), a hypothetical person at or beyond the plant boundary in the plume centerline during the entire time of passage of the plume. These consequences are broken down into those that result from doses received during and shortly after plume passage (inhalation, cloudshine, and groundshine) and those received later from ingestion, groundshine, and inhalation of resuspended particles. The early consequences can also be broken into prompt and latent health effects whereas the later consequences consider only latent health effects.

APPLICATIONS

Some of the specific uses of MACCS and the relevant input/output parameters are given below.

Hazard Classifications

Hazard classifications were required for non-reactor nuclear facility SARs to determine the level of additional accident analyses that may be required and to define the approval authority. For many hazard classifications, credit is not taken for safety systems to mitigate accidents and "worst-case meteorology" is used to evaluate the consequences of an accident. This "worst-case" is typically taken to be a wind speed of 1 m/s and an atmospheric stability class of F (stable). At RFP, the minimum offsite distance, which is used in the MOI evaluations, is approximately 1.9 km from the plutonium facilities, for which MACCS calculated approximately one rem Committed Effective Dose Equivalent (CEDE) to the MOI per gram of Pu released, for a deposition velocity of 1 cm/s, or two rem CEDE for a 0.1 cm/s deposition velocity. (The deposition velocity depends upon the sizes of the particles released, which can vary with the accident scenario.)

Rebaselining of Building 707

In late 1989, all production work involving Pu was halted at RFP in order to put into place additional safety features and practices. In early 1992, President Bush announced that nuclear weapons production would cease in the United States. Subsequently, most production buildings at RFP were slated for decontamination and decommissioning, with a few to be placed in a production contingency mode in case they were needed again. Building 707 at RFP was one of the buildings placed in this mode, with a limited resumption mission to thermally stabilize pyrophoric forms of Pu. Its SAR was therefore updated taking into account the new mission for the building and the latest information regarding natural phenomena, in particular, revised estimates of seismic activity and potential damage. MACCS was used by a subcontractor, Stone and Webster Engineering Corporation, to evaluate the revised accident scenarios. Application of recent weather data and current dose assessment methodologies resulted in about a factor of ten increase over the original SAR radiological consequences, which were based on probabilistic analyses. However, because of MACCS's more realistic dispersion modeling, the MACCS estimates of mean consequences to the public reduced this potential increase to about a factor of two. For example, for a release of one gram of Pu and a deposition velocity of 1 cm/s, MACCS estimated the mean bone dose to the MOI as 0.86 rem (equivalent to about 0.9 rem CEDE), compared to 0.37 rem based on the original SAR method. MACCS

occurrence of accident scenarios for comparison to the original SAR risk curves, and an additional comparison to the WASH-1400[4] and NUREG-1150[5] reactor risk curves. Finally, the MACCS results were compared with the quantitative safety goals promulgated in DOE SEN-35-91[6]. The latter states that additional cancer fatalities from operations for persons within 10 miles of the plant should be less than 0.1% of the normal cancer risk in the U.S. from all other causes; it also states that prompt fatalities from accidents for persons within one mile of the plant should be less than 0.1% of the sum of prompt fatalities from all other accidents to which the public is exposed. The MACCS calculations showed that these goals would be met by the seismically-upgraded Building 707 under its new mission.

Environmental Assessment

Plutonium presents a potential fire hazard because of its pyrophoric nature when not in a stable chemical form. To reduce this hazard, it has been standard practice to thermally stabilize it, that is, reduce it to this stable form through controlled heating. This process was discontinued in 1989, when plutonium manufacturing operations were ceased at RFP. There are plans to restart this process but an Environmental Assessment of this operation was required before approval would be granted. MACCS has been used to evaluate the consequences of a variety of accidents that could conceivably occur during thermal stabilization. The MACCS computations involved the atmospheric release of one gram of weapons-grade Pu; the various accident scenarios were then evaluated by scaling the MACCS results to the amount of Pu postulated released in that scenario.

Table 2 shows the results from MACCS computations for the consequences to the MOI from an atmospheric release of one gram of respirable weapons-grade Pu; "respirable" means that the aerodynamic equivalent diameter is less than 10 μm. The results from two different weather scenarios, unfavorable and typical, and two different accident scenarios, no-fire and with-fire, are shown; the fire chosen releases sensible heat at a rate of 6 MW, which is appropriate for a medium-sized fire. These results are for a ground-based, 10-minute release. When a fire is involved, the plume is lofted over the heads of persons nearby and the MOI dose is accordingly smaller.

TABLE 2. MOI Doses, CEDE (rem) per Gram WG Pu

WEATHER CONDITION	NO FIRE	WITH 6 MW FIRE
Unfavorable (class F, 1 m/s)	2	0.15
Typical (class D, 4 m/s)	0.15	2×10^{-2}

These results are based on a dose-commitment period of 70 years, which is a current requirement for EAs. The number of Latent Cancer Fatalities (LCFs) in the general public within 50 miles of RFP expected from this release are shown in Table 3. For this case, weather data from 1990 were used as the basis of the statistics shown. In Table 3, "Typical" is defined as the median, that is 50% of the time the values are higher than the values shown and 50% of the time they are lower. "Unfavorable" is

defined as the 95th percentile level, that is, 5% of the time the values are higher than the values shown and 95% of the time they are lower. The stochastic risk factors used in generating the results shown in Table 3 are 6.0×10^{-7} LCF/rem for the bone skeleton, 8.0×10^{-5} LCF/rem for the lungs, and 1.5×10^{-5} LCF/rem for the liver. These are significantly higher than used in the earlier SARs and in earlier versions of MACCS.

TABLE 3. Latent Cancer Fatalities (LCFs) per Gram WG Pu for Population Within 50 Miles of RFP

WEATHER CONDITION	NO FIRE	WITH 6 MW FIRE
Unfavorable (95th Percentile)	0.1	0.1
Typical (Median)	0.01	0.01

Based on these results, when scaled to the various accident scenarios postulated in the EA, it was determined that the thermal stabilization process presents no significant threat to the public.

Pu in Ducts

The Environmental Protection Agency (EPA) requested an evaluation of the potential hazard to the public posed by the Pu that has been trapped in the primary confinement ventilation ductwork at RFP over the many years of its operations. The particular accident scenario defined by the EPA was one in which a large airplane, fully loaded with fuel, crashes into the building under consideration, causing a fire and breach in the ductwork and subsequent unfiltered release of Pu into the atmosphere. Two buildings were considered, the building having the greatest amount of ductwork that has not yet been remediated (cleaned up), and a building in which the ducts have been cleaned to an accepted level. Through the use of MACCS, it was shown that the Pu in the ducts poses no significant threat to the public, even under worst-case meteorological conditions, like those used for hazard classifications.

Sabotage

The health and safety of persons living in the communities surrounding RFP is of enormous concern to the operators of RFP. Therefore, extraordinary precautions are taken to see that saboteurs or terrorists would have an exceedingly difficult time in releasing enough Pu into the air to cause a significant health problem to the public. Part of the precautions taken include the determination with MACCS of the maximum airborne release that would cause a given MOI dose under worst-case meteorological conditions, accounting for fires and elevated releases from explosions. From this, one can work backward through the accident scenario to determine the maximum material at risk that could be allowed in an area that may come under attack. This information was used by safeguards analysts to assure that sufficient barriers and deterrents are in place to prevent the incident.

Criticalities

One set of accident scenarios evaluated involve metal and water-moderated criticalities. The isotope inventory and activities input to MACCS are taken from the output of computations made with a criticality code, such as ORIGEN2[7]. Because the currently-released version of MACCS (Version 1.5.11.1) has only 60 isotopes in its library, not all of the important fission products from a Pu criticality could be included in the MACCS calculations. We therefore had to estimate by hand calculation the magnitude of the "correction factor" that would have to be applied to the results to get a more realistic estimate of dosage. Also, the current version of MACCS does not contain liver in its organ list, so this had to be simulated as having a response to radiation similar to that of another organ, such as red marrow. These correction factors were 1.35 for bone doses or 3.0 for CEDE. From the MACCS computations, it is estimated that for the MOI, a CEDE of 4×10^{-3} rem results from a metal criticality of 1×10^{19} fissions and 1×10^{-2} rem results from a solution criticality of 1×10^{18} fissions; these are less than the original SAR results.

SUMMARY

In summary, MACCS has been used for both deterministic and probabilistic accident analyses and risk assessments of non-reactor nuclear facilities. Future applications of MACCS include: (1) evaluation of radiological consequences to workers in collocated facilities at the RFP, which requires a plant demography by shift and location, and building-specific construction data for building shielding and wake effect calculations; and, (2) the criticality calculations need to be repeated using MACCS2 to see how accurate our earlier estimates were.

REFERENCES

1. D. I. Chanin, J. L. Sprung, L. T. Ritchie, H-N Jow, and J. A. Rollstin, "MELCOR Accident Consequence Code System (MACCS). Volume 1: User's Guide; Volume 2: Model Description; Volume 3: Programmer's Reference Manual," NUREG/CR-4691, Sandia National Laboratories, published by the U. S. Nuclear Regulatory Commission, Washington, D.C. (1990).

2. "Recommendations of the ICRP," ICRP Publication 26 (Annals of the ICRP Vol. 1 No. 3), published for the International Commission for Radiological Protection by Pergamon Press, Oxford, England (1977).

3. "Limits for Intakes of Radionuclides by Workers," ICRP Publication 30 (Annals of the ICRP Vol. 2 No.3/4, Vol. 4 No. 3/4, Vol. 6 No. 2/3, Vol. 7, Vol. 8 No. 1-4, and Vol. 19 No.4), published for the International Commission for Radiological Protection by Pergamon Press, Oxford, England (1979 - 1982).

4. "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).

5. "Reactor Risk Reference Document", NUREG-1150, U. S. Nuclear Regulatory Commission, Washington, D.C. (1987).

6. Nuclear safety policy, *Secretary of Energy Notice* SEN-35-91, U. S. Department of Energy, Washington, D.C. (1991).

7. "ORIGEN2 - Isotope Generation and Depletion Code," RSIC Computer Collection, CCC-371, Oak Ridge National Laboratory, Oak Ridge, Tennessee (1989).

PRACTICAL APPLICATION OF PROBABILISTIC RISK ANALYSIS FOR MARINE OIL-SPILLS

David J. Winfield[1] and David F. Dickins[2]

[1]AECL Research
Chalk River Laboratories
Chalk River
Ontario
KOJ 1JO

[2]D.F. Dickins and Associates
Suite 210, 1290 Hornby St.
Vancouver
British Columbia
V6Z 1W2

INTRODUCTION

A frequency versus consequence (risk diagram) approach for assessing marine oil-spills was proposed by Joksimovitch[1] in PSAM-I, to obtain a perspective on desired risk reduction in the marine oil-transportation industry. In the present paper a practical application of a risk diagram is applied to potential large oil spills in the waters of the Canadian East and West Coasts, and the St. Lawrence River as far as Montreal, omitting the Great Lakes and regions north of 60 degrees latitude. The work was initiated and supported by the Canadian Coast Guard. The objective was to rank oil-spill risk in these marine areas for spills between 5 000 and 30 000 tonnes.

APPROACH

Probabilistic risk assessment methodology was used to determine the risk contributors to oil spills of the defined size. The risk contributors are defined by the predicted frequency of occurrence of oil spills and the potential consequences of the spills. The initial focus of the report was to define suitable geographic areas at risk. Relative spill frequencies in these defined areas were then determined and area-specific consequences determined. Spill frequency aspects were predicted using simple assumptions from marine casualty statistics. Consequence modeling, which involved numerous subjective variables, was performed using the Analytic Hierarchy Process[2] (AHP). A risk map was then produced so that the individual area spill frequency and consequences and overall risk could be seen in the context of constant risk lines.

DEFINITION OF GEOGRAPHIC AREAS AT RISK

The geographic areas at risk were determined from areas chosen by analysis of the locations of 15 years of marine-vessel casualty statistics. Eleven areas with distinct casualty frequencies on the Canadian East Coast and four areas on the West Coast were identified (see Table 1).

Table 1. Geographic areas at risk.

Area	Name
1	Northern Labrador
2	Southern Labrador
3	St. John's
4	Approach to Cabot Strait
5	Southeast Nova Scotia
6	Fundy
7	Northumberland Strait
8	Cabot Strait
9	Strait of Belle Isle
10	Ile d'Anticosti
11	St. Lawrence River
12	Vancouver
13	Rupert
14	West Coast Charlottes
15	West Vancouver Island

Definition of Oil-Spill Range

The spill range for this study was defined as an oil spill of from 5 000 to 30 000 tonnes. This range was intended to encompass the 10 000 tonne spill of the oil-spill response model.[3] Spill volumes outside this range have significantly different frequencies. Figure 1 data[4] summarizes the Canadian and international oil-spill data from 1974 to 1990 June and provides the rationale from which the spill range was chosen. Spill frequencies as a percentage of total events during this time period, in three ranges (136 to 5 000 tonnes, 5 000 to 30 000 tonnes and >30 000 tonnes), are shown, with associated 90% statistical confidence bounds. The international data clearly indicates significant differences in frequency for the three different spill ranges. Canadian data is consistent with the international data within the 90% uncertainty bounds.

Spill Frequency Prediction

Direct use of spill statistics by area could not be used to predict spill frequency by area because of insufficient data. The use of vessel casualty statistics was therefore used to provide adequate statistical accuracy to confidently predict relative spill frequency. The more traditional approach for oil-spill frequency prediction has been to use analytical models of the causal factors influencing spills. These models calculate the fundamental navigational, oceanographical, hydrographical and climatological variables and traffic density factors relevant to oil-spill frequency. Because of the large uncertainties and the large analytical requirements for explicit modelling, the casualty-derived method for spill frequency prediction was used for this work.

Comparisons of oil-spill and vessel casualty root causes enabled reasonable assumptions to be made to justify the basis of the casualty-spill correlation. International oil-spill statistics were then used to provide data, to derive a relationship between vessel size and spill size. For the spill range considered, the spill frequency was found to be independent of vessel size for tankers above 5 000 Gross Registered Tonnage (GRT). The average spill volume within the defined spill range did not vary with vessel size above 5 000 GRT. Both Canadian and international casualty data also indicated that the frequency of

casualties per vessel exposed are vessel independent, within the statistical accuracy of the data.

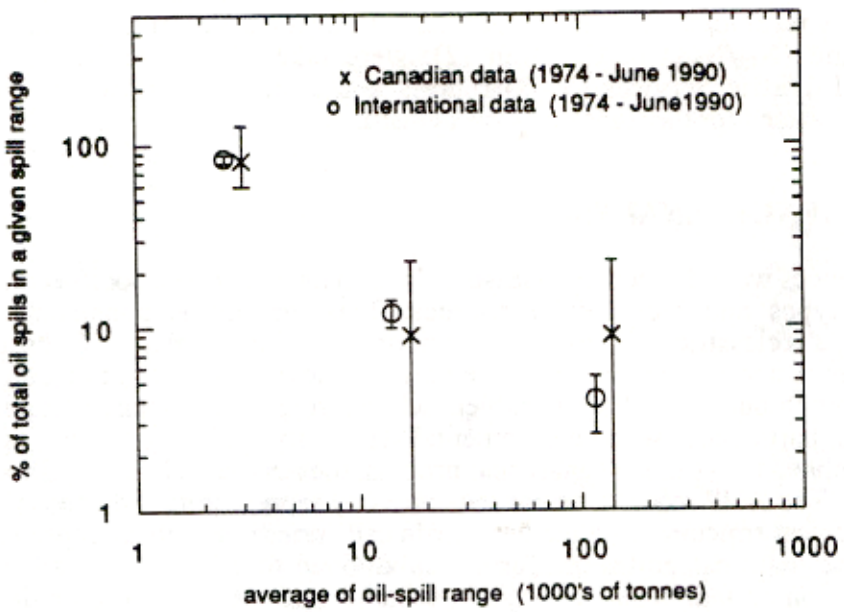


Figure 1. International and Canadian Oil Spills (%) as a Function of Average of Oil-Spill Range.

Spill-Risk Definition

The risk of the given spill scenario for area **a**, R_a consists of a spill frequency index and a spill consequence index, representing the first and second terms, respectively, of the following equation:

$$R_a = (freq)_a \times (conseq)_a \quad ...(1)$$

For this study the area consequences are ranked on a relative numerical scale, normalized to unity for convenience. Similarly, the frequency index was only provided on a relative normalized scale.

Development of Spill Frequency Index

The frequency of oil spills for the defined spill range in a given area **a**, $(freq)_a$ required from Equation (1) to calculate the risk, was calculated from:

$$(freq)_a = (vc_a) \times (N_{ta}/N_{va}) \times p \quad ...(2)$$

where: (vc_a) is the frequency of casualties in all vessel types, >5 000 GRT, in area **a** and (N_{ta}/N_{va}) is the fraction of vessels in area **a** (>5 000 GRT) that are oil tankers, and p is the probability of an oil spill given an oil tanker (>5 000 GRT) casualty. As p is assumed not to depend upon the vessel size or the area, for determining relative risk values it is assumed constant. Only the first two terms therefore have to be obtained from the relevant casualty and traffic statistics data bases.

Casualty and Traffic Statistics Data Sources

Marine casualty positions, for a 15-year period (1977-1991) for vessels >5 000 GRT, from the Canadian Marine Casualty Information System (MCIS), were plotted in a geographic information system by latitude and longitude. This database provided 3 955 casualties of vessels > 5 000 GRT, which was sufficient to establish a statistically adequate annual traffic casualty rate, vc_a in Equation (2), for each study area. Vessel traffic statistics, needed to determine (N_{ta}/N_{va}) in Equation (2), were taken from combinations of documented Vessel Traffic Services (VTS) reports and commodity flow and vessel movement reports produced for the Canadian Coast Guard.

SPILL-CONSEQUENCE ANALYSIS

Spill consequences were derived by assessing three main categories: socio-economic factors, shoreline types and biological resources. This method is consistent with Environment Canada's classification for environmental sensitivity maps. Substantial subjective judgement is necessary to put all these various relevant factors onto a common scale. This is a common but very difficult problem when trying to rank many variables of quite different types, particularly with environmental sensitivity applications such as this. To provide an auditable and systematic analytical process, the Analytic Hierarchy Process[2] (AHP) was chosen. The AHP models the consequences by representing the consequence variables in a hierarchical structure, with the three main categories noted above representing the top level. These main categories are further subdivided to a level of detail where quantitative information on individual data can, in principle, be obtained for each defined area. Where quantitative data was not available, qualitative judgements were made in these cases.

Spill-Consequence Model Structure

The main categories were broken down into sub-categories, as distinct from each other as possible, so that each contains more detailed items that could be distinctly grouped into a further sub-category. The consequence model defined from this hierarchy structure was then analyzed by the software developed for the AHP[5] to produce a relative ranking of the consequences of the different areas at risk, on a common scale. The model uses subjective judgements to pairwise compare the different categories and sub-categories, and then uses primarily objective data comparisons for the sub-categories with the highest level of detail. These latter are at the lowest hierarchy level and are defined in such a way that numerical data for those particular items can be obtained for each of the areas at risk. The hierarchy categories are listed in Table 2.

Final Risk Diagram

The spill risk contributing factors, frequency and consequence for each area were then normalized and represented on a traditional risk profile (frequency/consequence) diagram; these are identified by area number in Figure 2. The six highest risk areas identified were on the East Coast; these areas were also those with the highest predicted oil-spill frequencies. This means that the overall risk for these highest risk areas was dominated by the spill frequency, rather than the spill consequence. Constant risk lines indicating relative risks varying by factors of 10 have been indicated on the risk profile diagram. These lines show the relative location of the individual area risks, with respect to constant risk. No absolute definition of an 'acceptable' risk line is intended to be provided.

As noted by Joksimovitch,[1] attempting to define spill-risk acceptability criteria for the oil-transportation industry on either an absolute basis or by comparison with other transportation industries is not straightforward. However, the risk-diagram approach and results provided in this paper provide a practical example for the basis from which progress towards discussion of a large-spill-risk criteria definition could be made. From similar risk-criteria methods, as developed for the chemical, nuclear and air-transportation industries, for

Table 2. Consequence variables used for the AHP ranking of the study areas.

- **Socio-Economic Features:**

Special Status Areas
- National Parks
- Provincial Parks
- Historic Sites
- Bird/Wildlife Sanctuaries
- Native Reserves

Human-use impacts
- Community-dependent impacts
- Recreational uses

Commercial-use impacts
- Commercial Fisheries
- Tourism Industries

- **Shoreline Types:**
  - Estuaries/marshes
  - Mixed-sediment beaches
  - Sand beaches
- **Biological Resources:**
  - Spawning fish
  - Anadromous fish
  - Breeding birds
  - Migratory birds
  - Endangered (bird) species
  - Reptiles
  - Shellfish
  - Shoreline mammals

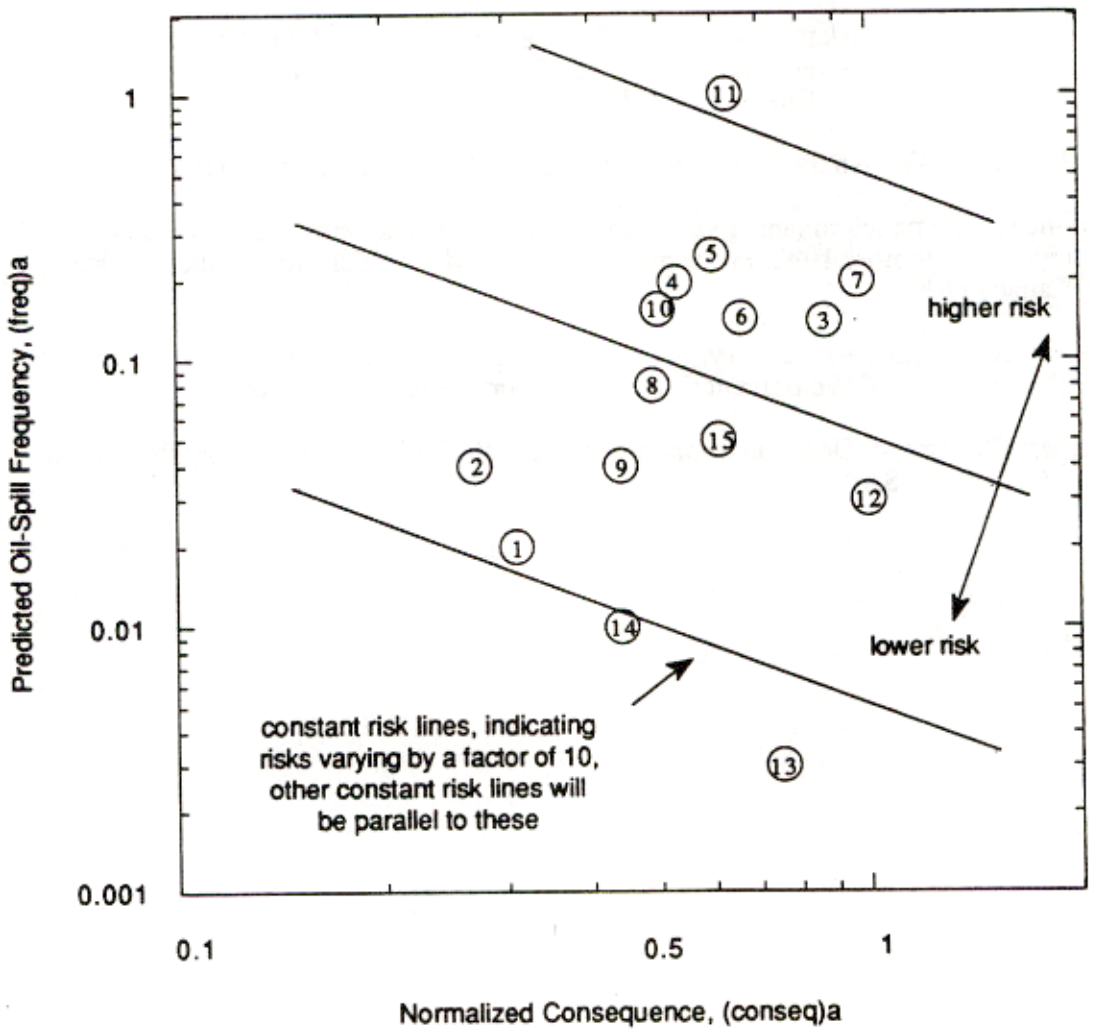


Figure 2. Oil-spill risk profile, of defined areas. Scales are normalized to unity.

example, the cost-effectiveness of potential vessel engineering design options, vessel operational and navigational factors and oil-spill clean-up options could, in principle, be developed and rationalized from risk-based decision-making.

Difficulties in assessing the overall completeness of the spill consequence aspect of the study, because of the wide variety of relevant environmental sensitivity categories and the limited availability of some of the area-specific sensitivity data (in particular, biological resources) were identified and are being addressed in further studies.

In addition to representing the spill frequency and spill consequences quantitatively on a conventional risk diagram and providing a numerical tabular ranking, colored spatial maps showing the predicted oil-spill frequency and oil-spill consequences for the study areas have been produced. This provided an effective means of communicating the risk-study results to non-risk specialist audiences.

Acknowledgements

The assistance of J. Bushek, Ottawa; the staff of Dickins Associates who provided analysis assistance; the federal and provincial organizations that supplied information; and the support of the Canadian Coast Guard are gratefully acknowledged.

REFERENCES

1. V. Joksimovitch. Risk management and Exxon Valdez oil spill, *in:* "Proceedings of the International Conference on Probabilistic Safety Assessment and Management, Beverley Hills, California, 1991", Elsevier, New York (1991).

2. T. L. Saaty, "The Analytic Hierarchy Process", McGraw-Hill, New York (1981).

3. Public review panel on tanker safety and marine spills response capability, 1991, final report, September 1990, Protecting our waters, Ministry of Supply and Services Canada (1990).

4. Monenco Consultants, Calgary, Tanker self-help spill recovery systems, Prepared for Transportation Development Centre, Transport Canada, 1991 November.

5. Expert Choice Inc, Decision Support Software, 4922 Ellsworth Avenue, Pittsburgh, PA, 15213 USA.

ON THE ENVIRONMENTAL RISK OF METHANOL SPILLS AND LEAKS

Peter T. Katsumata[1] and William E. Kastenberg[1]

[1]Mechanical, Aerospace and Nuclear Engineering Department
School of Engineering and Applied Science
University of California
Los Angeles, CA 90024-1597

INTRODUCTION

Methanol has recently gained interest as an alternative to gasoline for several reasons. The automotive industry has shown great interest due to its combustion characteristics. The Department of Energy has been investigating its use to secure the nations energy future because of its possible production from natural gas, coal, and renewable sources. And the auto racing industry has been using methanol for its high energy content and safety characteristics. But possibly the most important reason is the EPA's, as well as state and local air quality agencies, interest in using methanol to address local as well as national air quality problems. Methanol's attractive feature is that it's combustion produces significantly less hydrocarbon emissions than does gasoline's combustion. But, an increased exposure of the public to methanol and perhaps to one of its combustion by-products, formaldehyde, would result from its introduction and widespread use as an alternative fuel. However, insufficient information exists at present as to either the health consequences, particularly of low-level exposures over long periods of time, or likely exposure scenarios and levels to which the general population or sensitive sub-groups may be subjected.

An increased use of methanol will result in an increase in the transportation, distribution, and storage of methanol. This in turn will increase the possibility of accidental releases. The multimedia compartment model called GEOTOX[1] was used to model three types of releases: 1) a large spill of methanol into a body of water, 2) a leaking underground methanol storage tank, and 3) a ruptured above-ground methanol storage tank. In the GEOTOX model, environmental media (e.g., air, soil, ground water, etc.) are lumped into homogeneous compartments that experience exchanges with adjacent compartments. In simulating the first scenario, 5,000 gallons of methanol was assumed released into the surface water over a period of one day. Methanol concentrations were then calculated for a period of 35 days. In modeling the second scenario, 5,000 gallons of methanol was assumed released into the lower soil compartment at a constant rate over a period of one year and the concentrations calculated for 450 days. In modeling the third scenario, 5,000 gallons of

methanol was assumed released into the upper soil compartment at a constant rate over a period of nine days. The concentrations were calculated for a 60 day period. The physiochemical properties of methanol used in the GEOTOX model were obtained from various sources[2,3,4]. The landscape parameters for the California ecoregion contained in the GEOTOX model were used. The landscape size and soil compartment depths were changed slightly for each of the three scenarios. The results from GEOTOX were used to evaluate the fate of methanol in the environment. A human exposure assessment was then performed using the exposure module in GEOTOX. An assessment of the risk using the resulting exposure values was then performed. Since methanol is not a carcinogen and has no unit risk factor, the risk was defined as the ratio between the exposure and the allowable daily intake (ADI). The sensitivity of the first two scenarios to the biological degradation removal rates was also examined.

DISCUSSION

Surface Water Spill

The GEOTOX results for the large surface water spill (5,000 gallons of methanol in one day) show that the concentrations in all of the compartments, except biota, are seen to steadily decrease after an initial increase from the spill. The concentration in the biota compartment is seen to steadily increase.

When methanol is spilled into a body of water it will quickly mix and equalize throughout the entire body of water because it is completely miscible in water. But since its density is less than that of water, most of the methanol will tend to be at the top for early times. The rapid methanol concentration decrease in surface water is due mainly to biodegradation and volatilization. Significant biodegradation was seen to occur in various experiments involving methanol in water[2]. The volatilization of methanol is also a large factor in its removal from surface water because of its high Henry's Law constant (Other factors such as photolysis, oxidation, bioconcentration, aquatic hydrolysis, and adsorption to sediment do not seem to play a major role). As the concentration in the surface water decreases, so too does the concentration in the sediment because the sorbed methanol concentration is linearly related to the aqueous concentration.

Because of methanol's miscibility with water and its low octanol/water partition coefficient, it is expected to be highly mobile for spills upon or within soil matrices. Many studies have also shown significant biodegradation in soil[2]. Another factor affecting the concentration of methanol in the upper soil is its volatility. Because methanol has a high vapor pressure, it evaporates quickly from dry surfaces. Thus, the concentration in the upper soil follows the same trend as that of the surface water.

The methanol that volatilizes from the surface water and the upper soil goes directly into the air. It will remain almost entirely in the vapor phase because of its high vapor pressure (Some degradation due to reaction with photochemically produced hydroxyls may occur). Due to its miscibility with water, some methanol is removed physically with rain[2]. However, most of the methanol is removed from the system by advection. Since methanol is most prevalent in the ambient air in its vapor phase, it is readily carried away by the moving air. Therefore, as the amount of methanol in the system decreases due to its removal, the concentrations in the air and the air particles decreases.

The concentrations in the lower soil and groundwater follow a trend similar to those of the upper soil and the surface water. But, because the lower soil and groundwater lack the

route of removal by volatilization, the concentrations decrease at a slightly slower rate than those of the upper soil or surface water. The concentrations continually decrease because of methanol's high mobility and the significant biodegradations that occur in these compartments.

The concentration of methanol in the biota continually increases because this compartment is deficient of the major route of removal, volatilization. Thus, as the biota is exposed to the various compartments containing higher concentrations of methanol, it accumulates and stores the methanol. A value for the degradation rate or biodegradation rate could not be found for the biota. Hence it was set to zero.

The results in the form of concentration versus time are somewhat deceiving in that the sizes of each compartment vary. Figure 1a shows the percent of methanol in each compartment as a function of time. In this figure, the actual fraction of methanol in each compartment can be seen. Also included in this figure is the total amount removed from the system. The surface water compartment contains almost all of the methanol while the other compartments contain very little. The "total removed" curve is approximately the reciprocal of the surface water curve. The curves show that the methanol introduced into the multimedia environment is either degraded or advected out of the system.

From these results, it can be concluded that from a large spill into a body of water, approximately all of the methanol will be removed due to volatilization and biodegradation. In order to verify these results, various equilibrium calculations were performed on a closed system containing only air, water and soil. These results showed that over 96% of the methanol resided in the air. Thus in an open system with some ambient advection, the results would be very similar to those found from GEOTOX.

Leaking Underground Tank

The results of the second scenario for the leaking underground storage tank, where 5,000 gallons are released into the lower soil over a one year period, shows that the concentrations in each compartment, except that of the biota, initially increases and reaches a constant value before abruptly dropping after the source is removed. This trend during the release period is due to the leaking tank. The similarity in the concentration curves and the sudden decreases in concentration are due to methanol's high mobility, volatility, and biodegradability. The concentration in the biota continually increases for the same reasons it did in the previous simulation (see the section on the **Surface Water Spill**).

Figure 1b shows the percent of methanol in each compartment as a function of time. This figure also includes a curve for the total amount removed. The bulk of the methanol is contained in the lower soil. Very little methanol is seen to be present in the other compartments. Similar to the previous simulation, the curves show that the methanol entering the multimedia environment is either degraded or advected out of the system. Thus, from a leaking underground storage tank, the majority of the methanol will be removed, given sufficient time, through volatilization and biodegradation.

Ruptured Above Ground Tank

The results of the third scenario for the ruptured above ground storage tank (5,000 gallon release onto upper soil over nine days) show that the concentration in the upper soil is very high (9,000 mg/kg of soil) for the release period, but drops off quickly thereafter. The concentrations in the upper soil, air, and air particles compartments, although much

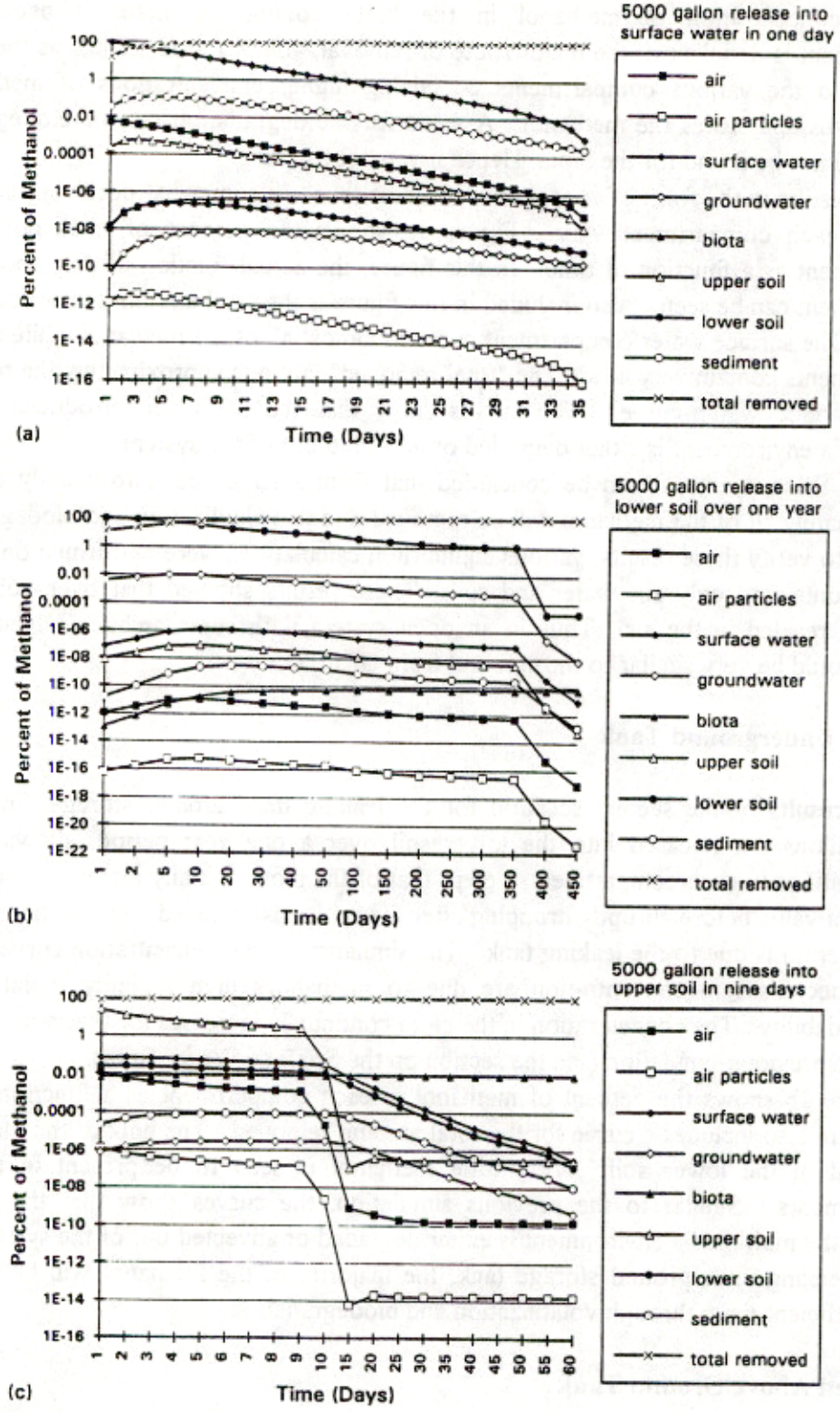


Figure 1. Percent of methanol in each compartment as a function of time for: (a) scenario 1, (b) scenario 2, and (c) scenario 3.

lower, are seen to follow the same trend. They exhibit a constant concentration for the release period, and then decrease by several orders of magnitude. The concentrations in the remaining compartments, except for that of the biota, slowly increases for the release period, and then slowly decreases. The concentration in the biota continually increases.

The constant concentration in the upper soil during the release period is due to the leaking tank. Similar to the previous simulation, the sudden decrease in concentration is due to methanol's high mobility, volatility, and biodegradability. The similarity in the trends for the air and air particles as compared to that of the upper soil is due to methanol's high volatility. It readily volatilizes from the soil into the ambient.

The steady increase and decrease in concentration in the lower soil, surface water, groundwater, and sediment compartments is a result of methanol's miscibility in water and its high Henry's Law constant, as well as its mobility. Since it is very mobile in soil, it will move into other compartments, especially surface water and groundwater. Because of its miscibility, it will spread quickly and increase the concentration in the sediment as the concentration in the surface water increases. But as the concentration in the upper soil decreases, the concentrations in the lower soil, surface water, groundwater, and sediment also decreases.

The concentration in the biota continually increases for the same reasons it did in the first scenario (see the section on the **Surface Water Spill**); i.e. it lacks an explicit removal pathway. Figure 1c shows the percent of methanol in each compartment as a function of time. This figure also includes a curve for the total amount removed. The bulk of the methanol is contained in the upper soil, with the rest seemingly being removed. Very little is seen to be present in the other compartments. As in the two previous simulations, these figures show that the methanol entering the multimedia environment is either degraded or advected out of the system. Thus, from a ruptured above ground storage tank, the methanol will be removed from the environment relatively quickly by volatilization and biodegradation.

Exposure

The time-varying exposure module in GEOTOX was used to assess potential exposures. This module calculates the adult, child, average individual, and cumulative exposures via seven pathways for each time step. The exposure pathways are inhalation, drinking water, biota ingestion, meat and dairy product ingestion, fish ingestion, soil ingestion, and dermal absorption. The adult and child exposures for each time step are found by using the corresponding total exposure for that time step to calculate a lifetime exposure. The average individual exposure is the weighted average of the adult and child exposures. The cumulative exposure is the total exposure accumulated up to the corresponding time step.

The exposure results show that the adult, child, and average individual exposures increase and decrease corresponding to the concentrations in the multimedia system. Because a child is considered to weigh less and have approximately the same uptake, the exposures are correspondingly higher. The cumulative exposure steadily increases, as would be expected.

In order to put these exposure levels into perspective, it would be desirable to compare them to a health based total exposure standard. Unfortunately, one does not exist for methanol. However, an oral "Reference Dose" (RfD), as reported by the EPA in their 1990 Health Effects Assessment (HEA)[5], does exist. "The RfD is an estimate (with uncertainty spanning perhaps an order of magnitude) of the daily exposure to the human population

(including sensitive subgroups) that is likely to be without an appreciable risk of deleterious effects during a portion of the lifetime..."[5].

The value reported for subchronic oral exposures to methanol is 5.0 mg/kg-d. Although this value is only for oral exposures, it can be used to put the results found from GEOTOX into perspective. The total exposures for the first two scenario's are well below the RfD. However, for the third scenario the adult, child, and average individual exposures surpass the RfD at some point, but eventually drop below it. In each scenario, the cumulative exposures are well below the RfD. Because the RfD is for a subchronic exposure, the most accurate comparison would be with the cumulative exposure. Thus, relative to the RfD, the exposure levels in all three scenarios are well within safe limits.

CONCLUSIONS

The results show that approximately all of the methanol introduced into the environment from any of the three scenarios will be removed fairly quickly due to volatilization, advection and degradation. The sensitivity study suggests that the results are somewhat sensitive to the removal rates. It can also be deduced that for the compartments that have no contact with the atmosphere, degradation plays the major role in removal. But, given adequate degradation, the end result will be the same, but at differing rates. Thus taking into consideration the uncertainty in the removal rates, the results should be very similar to the results presented here.

The exposure results indicate that none of the three scenario's produce exposure levels higher than the oral subchronic RfD. Although the third scenario produced surface water concentrations higher than the concentration corresponding to the RfD, it is very unlikely that an above ground storage tank will be placed near a body of surface water. Comparing the maximum cumulative exposure level in each of the three scenarios to the ADI, which is the RfD in this case, the risks were found to be 1.1E-6, 1.9E-6, and 1.4E-3 for scenarios 1, 2, and 3, respectively. These results are not conclusive, but are presented to put the level of exposure found from GEOTOX into perspective.

REFERENCES

1. T.E. McKone, L.B. Gratt, M.J. Lyon, and B.W. Perry. "Geotox: Multimedia Compartment Model, User's Guide," (1984).
2. P.H. Howard, "Handbook of Environmental Fate and Exposure Data for Organic Chemicals, Volume II," Lewis Publishers Inc., Chelsea, MI (1990).
3. B.J. Bauman, "Groundwater Contamination by Methanol Fuels," an unpublished manuscript.
4. P.H. Howard, R.S. Boethling, W.F. Jarvis, W.M. Meylan and E.M. Michalenko, "Handbook of Environmental Degradation Rates," Lewis Publishers Inc., Chelsea, MI (1991).
5. U.S. E.P.A., Health Effects Assessment Summary Tables, (1991).

024 Computerized Monitors and Operator Aids (I)

Chair: A.J. Spurgin, Consultant

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

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

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

OBJECT ORIENTED PLANT MODELS FOR OFF-LINE AND ON-LINE RISK MONITORING

André Poucet[1] and Andrea Carpignano[2]

[1]Commission of the European Communities
Joint Research Centre
Institute for Systems Engineering and Informatics
21020 - Ispra, Italy
[2]Politecnico di Torino
Corso Duca degli Abruzzi, 24
10129- Torino, Italy

INTRODUCTION

Industrial installations get increasingly complex. Therefore it becomes more and more difficult to overview the different ways a plant can behave in case of failures and disturbances and to foresee control or safety measures which prevent these from evolving into incidents or accidents.
Probabilistic Safety Assessment (PSA) methodology offers good tools to identify, structure and analyze failures/disturbances and their effects, and to assess their relative importance to plant safety and reliability. PSA in principle also offers a possible framework for monitoring the safety or operability during the plant life. PSA based models can be used to help to ensure that a plant is kept within its intended safety/operability envelope and any voluntary or involuntary changes that occur over the plant's life do not violate assumptions or rationales that were part of the original design.
Monitoring of operability and safety has become of increasing concern both in the regulatory context (so called "Living PSA" requirements) as well as to the industry in their effort to cut down the cost of production loss and to optimize maintenance schedules (as e.g. in Reliability Centered Maintenance).
One of the major difficulties in using PRA type models for in a more dynamic monitoring mode is the difficulty to include and propagate modifications into such models. Such modifications can be dictated by (involuntary) changing behavior of components (e.g. aging phenomena), and by (voluntary) changes in configuration, in design, in test and maintenance regime or in operation. This requires a new approach to represent PSA data and models and the information that goes along with them: in other words a new approach to represent plant safety information in a safety oriented plant model. This paper takes a look at this problem from the perspective of two projects in which safety oriented plant models with different scope and objectives were developed to support on-line and off-line decision making.

OFF-LINE AND ON-LINE MONITORING

The monitoring activity referred to in this paper consist of identifying or postulating change(s) to the plant and using a safety oriented model to analyze the impact of that change

on safety or operability. Depending on the objective, the monitoring activity can be performed in an on-line or off-line context:

- Off-line monitoring should provide the designer or safety engineer with deep knowledge about the impact of longer term or permanent modifications in system design, behavior or operation, intended (e.g. backfits, procedural changes) or unintended (e.g. equipment aging).
- On-line monitoring has the objective to give advise to the operator concerning optimal system configuration and optimal response to disturbances and failures.

Of course, the level of detail and scope of the safety oriented model upon which the monitoring analysis is based, are rather different in both situations.. On-line activity needs models through which observed changes can be fed and propagated quickly. Also it needs models that are able to produce a clear-cut, transparent and conservative statement about the safety impact of the change and convey that in a convenient way to the operator.
The off-line activity can rely on much more elaborate input and detailed models which then of course require much more processing time as well as more in-depth analysis by the user.

At the JRC, two major projects have studied the problem of risk monitoring:

1. within the frame of the STARS project[1], the problem of off-line risk monitoring and reliability monitoring was addressed and new ways were developed to support this activity. Pilot applications were done in the area of "Living PSA" as well for Reliability Centered Maintenance.
2. the FORMENTOR project[2] addressed the problem of supporting real-time advise to operators in case of disturbance or malfunctioning. Applications included both risk avoidance as well as operability.

TARGET SYSTEM MODELS IN STARS

In the STARS project, a knowledge representation scheme was developed that could act as a "container" for most of the information collected and generated in a PSA, including[3]:

1. data that are used as *input to the PSA*: plant functional and structural descriptions, component data ...
2. information which is generated *during the PSA*: component failure modes and effects, accident scenarios, system models ...
3. operating experience coming from the plant and used to *update the PSA*: such as failure events, abnormal occurrences ...

The safety oriented model in STARS is mainly organized around a structural view on the plant (see fig. 1): the plant's hardware is represented by a ***hierarchical collection of objects*** representing systems, subsystems and components, and representing interconnections between those items.
An object is used to describe a real-world item. A family of objects is represented by a class which is an abstraction of the characteristics that all the objects of this class share. Classes may be structured in hierarchies in which a class at a lower level may inherit (some or all) properties of the parent classes. In this case, properties may refer to e.g. technical characteristics, failure modes, reliability data. Between objects, various types of links may exist. Within the class hierarchies the most common type of link will be of the "**is a**" type (e.g. "solenoid-valve" **is a** "valve"). Between the objects of the structural breakdown other types of links such as "**is part of**" or "**is connected to**" exist.

An attempt was made to store initial information and information gained in the PRA process in a ***declarative*** way (as opposed to procedural) in the safety oriented model: e.g. rather than fault trees or event trees, the model includes the knowledge necessary to derive fault trees and event trees in a rather formal way using generic (computerized) procedures. These procedures themselves contain no plant specific information: they can work on whatever (well formed) safety oriented model. The benefit of this approach is that modifications in the plant can be easily incorporated in the plant's safety oriented model and then automatically propagated into the PRA results by using the computerized procedures guaranteeing internal consistency and coherency.

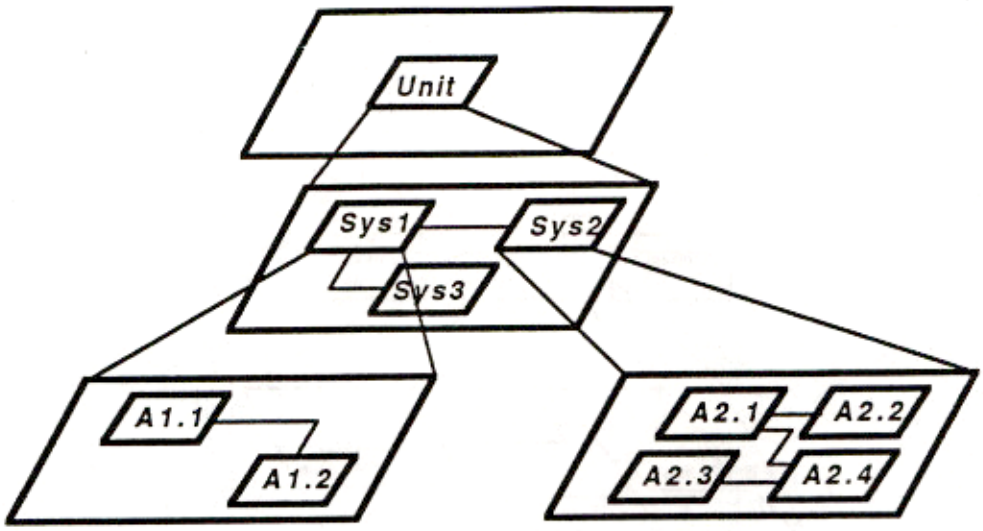


Figure 1. The STARS structural model is hierarchical and represents the plant into different breakdown layers: the plant is seen as composed of functional units, each of them further decomposed into systems, macro components and eventually components. In each of the layers, objects represent the elements of the breakdown and their interconnections. Safety related information is embedded into these objects.

It was soon realized that in addition to the structural information, it was necessary to also include functional information in the safety oriented plant model. In a first attempt, this functional information was embedded within the objects of the structural breakdown.

The structure based approach worked out fine for supporting system level modeling (e.g. fault tree construction). Indeed, a validation exercise[4] was performed in which a declarative STARS model was build for the safety systems of the Surry plant and this model was used to derive fault trees for various configurations of those systems. The constructed fault trees were found to be in very good agreement with the ones reported in the Surry PRA.
However, when the problem of plant level sequence modeling was tackled, the need was felt to include a completely separate functional breakdown in the safety oriented model in order to express the goals of plant operation as a combination of system or sub-system functions.

The functional breakdown studied presents at the upper levels a simple tree structure that relates plant objectives such as "production in safe conditions" to the goals of plant systems. At the lower levels this breakdown becomes more complex (see figure 2) and shows how the elementary functions (redundancies, control of process parameters, protections) collaborate to fulfill the goals of plant systems. The formalism used in these levels is based on Structured Analysis and Design Technique (SADT - a method used for specification and design).
The formalism "explodes" a function (in a similar way as the one described for the structural breakdown) into a diagram describing its sub functions and the interrelationships between these sub functions in terms of required inputs, provided outputs, controlling or triggering mechanisms and redundant sub functions. Any of the sub functions can then be further "exploded" as necessary, whereby necessary care is taken to maintain coherency between the interrelationships as represented on different layers.
Elements of this functional breakdown structure may be marked with pointers to elements of the equipment breakdown structure in order to associate systems or components to the functions they perform.

This global model, including separate functional and equipment breakdown structures, supports a larger set of safety analysis methodologies. In particular it allows to support methodologies whose aim is to relate component failures to global plant effects (e. g. automated Failure Mode, Effect and Criticality Analysis) or to investigate plant level sequence analysis (e.g. Event Tree construction).

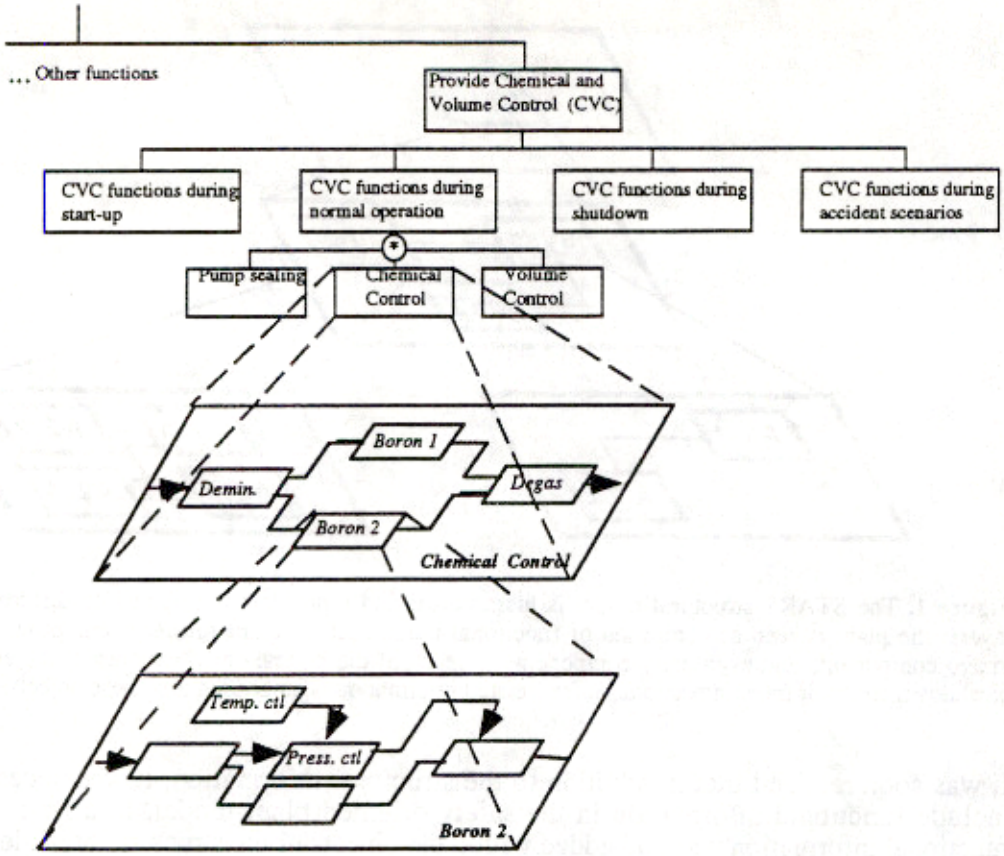


Figure 2. Functional breakdown structure in STARS following a tree representation to model high level objectives and a SADT representation to model lower level functions. The SADT represents the functions (boxes) their inputs (entering boxes at the left), their outputs (leaving the boxes at the right) and the control that act upon the function (entering the boxes at the top).

TARGET SYSTEM MODELS IN FORMENTOR

In the FORMENTOR project, the plant model method was basically developed with the aim to provide real-time support to the operator in case of disturbances or failures in the plant. Unlike in STARS, in FORMENTOR it is the functional representation that is the spine of the safety oriented plant model. The representation scheme chosen is the Goal Tree Success Tree model (GTST)[5].

The Goal Tree part is purely functional. It relates high-level safety and process objectives to the functions and sub functions needed to fulfill these objectives.
The Success Tree part provides the link with the hardware: each low level function is eventually related to the hardware components that implement the function.
Figure 3 gives the top part of the GTST developed for a petrol-chemical pilot application in which the high level objectives were related with safety, operability, product quality and efficiency.

In FORMENTOR, the GTST has dynamic aspects[6]: the safety or process objectives may change with the target plant's state and so may the strategies that are called upon to realize the objectives. This latter is true when several alternative sub functions can be used to fulfill a function or objective. These alternatives describe different operational strategies that can be followed according to the operational context (e.g. maintain steam generator level can be accomplished by using the main feedwater function or in case of incident by using the auxiliary feedwater function).
At any given time, functions can be "dormant" or "live". The set of "live" functions form the "live" part of the GTST and represent the currently followed strategies. These strategies are dynamic and can change under the influence of the dynamics of the target plant.

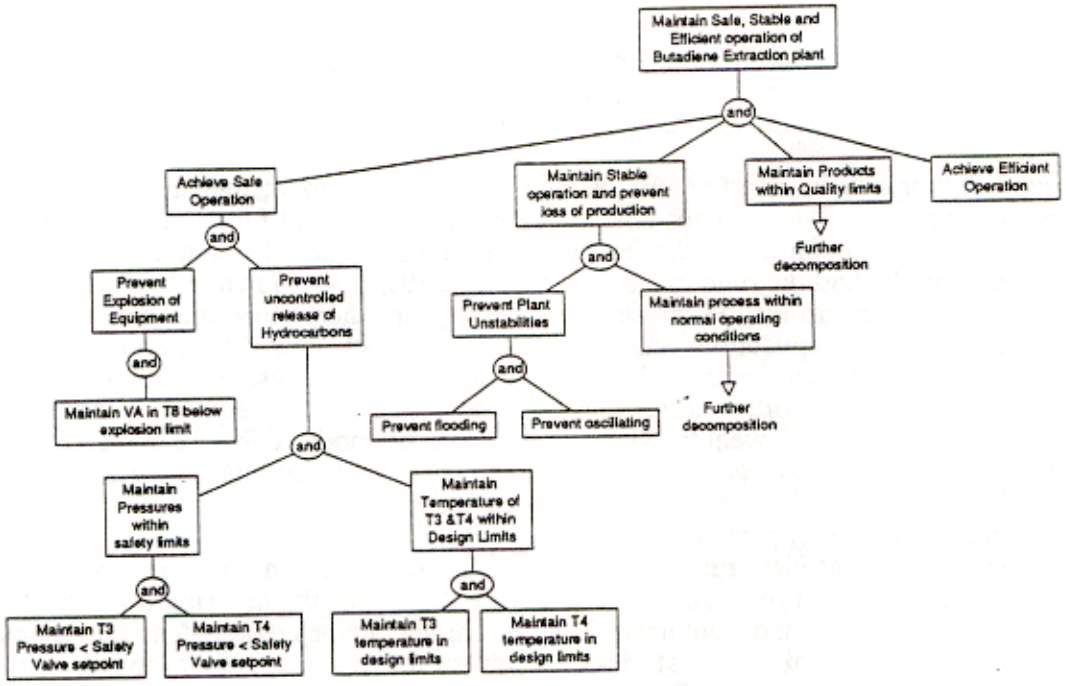


Figure 3. Top portion of Goal Tree Success Tree showing the goals modeled for a petrochemical pilot application of FORMENTOR, and showing the high level functions that implement these goals.

To achieve this dynamicity, a state propagation mechanism has been developed over the GTST model in order to accomplish the switching between life and dormant functions and thereby to follow the dynamically evolving situation of the target system.
The mechanism is fed by observables coming from a monitor-validate module. The observables are used by a diagnosis-situation assessment module to resolve conflicts between the GTST model and the observed situation, and to reflect the actual situation of the plant in the GTST model. A consequence assessor is used on the GTST to asses the future evolution of the situation, to determine the critical paths threatening the high level objectives and to identify alternative success paths which could fulfill these objectives.

The representation of temporal information in the GTST is still a matter of research. A first attempt to represent delays, trends or time lags was made by using a switch mechanism that includes inertia in the state propagation process.

CONCLUSIONS

From the above mentioned projects, some lessons can be learned with respect to target plant representation and a certain number of common features in the models can be identified.

There is no "best model" in general: the best model is the one that serves the specific purpose. However if we think about models to support safety/operability analysis and monitoring, there are a number of recurrent issues.

Hierarchical object oriented representations seem the most promising to represent a complex plant from the safety perspective:

- the hierarchical structure allows to represent a complex reality at different levels of detail and to accommodate the natural tendency to break down a problem in sub problems
- the object oriented approach allows to easily represent the many items that make up a plant (objectives, functions, systems, components, procedures, ..) and the complex relationships that exist among those items. Moreover, the object oriented approach provides the flexibility necessary to follow the different phases in the plant life-cycle: starting with an abstract functional model in the early design phase, more details can be added when specific system design becomes available.

For a comprehensive plant representation it is most useful to include multiple viewpoints:

- a functional view includes objects representing the plant functions with information on the conditions in which the functions are required and information about the system(s) that implement the function and its success criteria. As shown in FORMENTOR, such a view is very useful to represent how (safety or other) objectives are fulfilled by plant functions. In applications related to STARS, the inclusion of a functional breakdown has allowed to better describe the role of component and system in normal or off-normal conditions: the information necessary to model event sequences/scenarios (e.g. to construct function event trees) can be easily accommodated in a functional breakdown.
- the structural view represents the breakdown of the plant's hardware and can be used to host all technical information related with this hardware including possible states, failure modes, reliability parameters.
- the behavioral view represents how the (normal and abnormal) behavior of hardware realizes function (or malfunction): this view includes the description of the process, the process dynamics, the automatic and manual interactions required, and information about how changes (failures, disturbances) impact the process. This view has been the most difficult to catch. In STARS part of this information was embedded in the structural view (e.g. in the rules that model the effects of component failures). In FORMENTOR, the switching on the GTST included part of this information. However, it seems that the representation of behavior merits at least in part a separate view. How to structure this view in order to best capture essential elements, like temporal information and process dynamics, is still a matter of research.

Function, structure and behavior are three essential dimensions in the representation of complex systems. In addition to this triplet, the safety oriented plant model may, depending on the application, need to include also other information like 1) physical/topological information (physical lay-out of the site, plant zones), 2) information about managerial and organizational context that relates with plant operation and safety (e.g. safety culture) and 3) plant experience: abnormal events, failures and information that allows to determine and update plant specific reliability parameters or event frequencies.

REFERENCES

1. A. Poucet. Knowledge based systems for risk assessment and monitoring. Proc. CAES 92. Elsevier Applied Science.
2. M. Wilikens M., J.P. Nordvik and A. Poucet. FORMENTOR: A real-time expert system for risk prevention in complex hazardous environments - A case study, *Control Eng. Practice*, Vol. 1 No. 2: 323. Pergamon Press
3. A. Poucet and A. Besi (1993a). Living PSA and risk management: an object oriented approach, Proc. PSA 93. Clearwater 25-29 Feb.. 1993. ANS - Washington.
4. Dehn M. Applicazione di STARS all'impianto di Surry. Eng. Diss. Politecnico di Milano. 1993
5. D.T. Chung, M. Modarres and R.N. Hunt. Gotres: an expert system for fault detection and analysis, *Reliability Engineering and System Safety*. Vol. 24:113. Elsevier Applied Science.
6. J.P. Nordvik, N. Mitchison.and M. Wilikens, The role of the Goal Tree - Success Tree model in the real-time supervision of hazardous plant, accepted for publication in *Rel. Eng. & System Safety* , Elsevier Applied Science.

OBJECT-ORIENTED TOOLKIT FOR INTELLIGENT PLANT MONITORING SYSTEM : TIPS

Tadashi Ohi, Kazunori Sasaki

Control Systems Department
Industrial Electronics & Systems Development Laboratory
Mitsubishi Electric Corporation, Hyogo, 661, Japan

INTRODUCTION

The supervisory control system in the power generation plant has been automated by computer technology. In the plant control system, the importance of the computer's role has been discussed by many researchers from the viewpoint of plant safety. But there is no design theory for an intelligent plant monitoring system. Therefore, prototyping of the system including operation support facility and man-machine interface design is strongly required.

We have developed an object-oriented toolkit package, called TIPS (Toolkit for Intelligent Plant monitoring System), that supports the effective construction of intelligent systems. To realize intelligent plant monitoring systems, some special requirements must be satisfied[1]. The basic requirements of such an automated system are as follows :

- It must be able to handle various knowledge representations such as linguistic rules or frames. Automatic diagnosis is a typical function of the system.
- It must be able to access process data. Process data is used to decide the intelligent monitoring system's actions .
- It must be user-friendly. In interactive systems such as diagnostic systems, the interface between human and computer is very important.

TIPS is designed to satisfy these requirements. In this paper, first we describe TIPS's features. Next, we present some prototype application systems using TIPS. Finally, we discuss the conclusions of our current work and future research prospects.

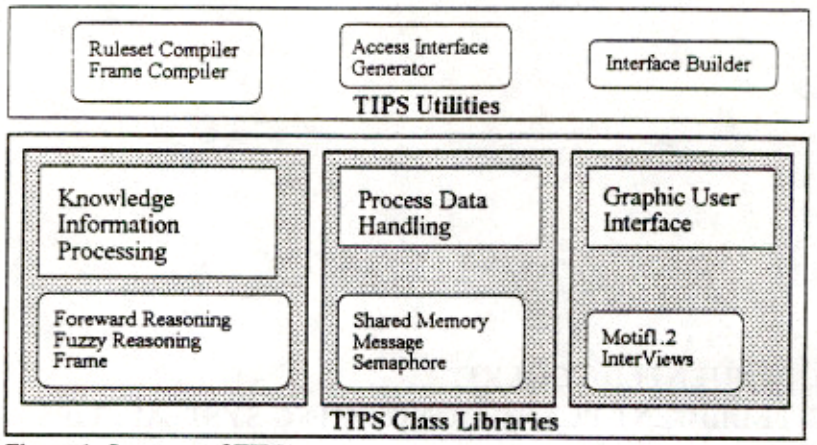


Figure 1. Structure of TIPS

TOOLKIT FEATURES

TIPS is a library of C++[2] objects that includes three object categories. Figure 1 shows TIPS's structure.

- Objects for knowledge information processing
  TIPS supports rule-based and frame-based reasoning. The *Rule-set* class is a base class for rule-based reasoning objects such as *Forward-ruleset* and *Fuzzy-ruleset*. The *Frame* class is a base class for frame-based reasoning.
- Objects for process data handling
  These objects provide the facilities for IPC (Inter Process Communication). For example, *process_data* class manages shared memory mapping information that is used to access real plant data.
- Objects for graphical user interface
  TIPS has many graphic objects such as graphs, component-icons for displaying plant status and the inference results on the X Window system.

Knowledge Information Processing Objects

As stated above TIPS has frame-based and rule-based reasoning classes. A frame-based scheme is a useful way of representing the characteristics of plant components. The frames represent the conditions in the plant and the state of reasoning. TIPS provides an object-oriented frame representation. The *instance* frame is created by the *class* frame information, and it has a name and several attribute variables. The instance frame can be used to represent the components of the plant. The attributes of the component, which reflect its characteristics, are represented as values of the frame attribute variables.

A rule-based scheme is useful in representing the knowledge of human experts. TIPS has a forward reasoning function using *if-then* rules. Certain instance frames are used as the working memory for the rules. The values in the frame are referred to and changed by the rules.

Rules in TIPS are organized into ordered sets of rules called Rulesets, and a Ruleset has a specified control structure for selecting and executing rules (the inference strategy). Similar to SUBROUTINE in FORTRAN programming, Rulesets are used as building blocks for organizing rule-based programs hierarchically. A Ruleset can be invoked in an action of the rule. This provides a way for a Ruleset to control the execution of other Rulesets. Here is a sample Ruleset:

```
rule_name startup_water_line ;
{    { control = do_1 ; }
 rule 1    if {        tank_1.pressure < 10.0 }
           then {      set(tank_1.status, ``low_pressure) ;
                       set(alarm.component,tank_1) ;
                       r_fork(display_alarm) ;          }
 rule 2    if {        tank_1.pressure > 20.0 ;
                       plant.operation_mode == ``startup ;    }
           then {      set(pump1.rpm, 3000) ; }
}
```

The declaration of *control* determines the inference strategy in the Ruleset. There are five inference strategies. Like LOOPS[3], the *do_1* strategy means that the inference engine executes one possible rule in a Ruleset. The *do_all* strategy means that the inference engine executes all possible rules. The *while_1* and *while_all* strategies mean that the inference engine repeats the do_1 or do_all strategy until the *while_conditions* are satisfied. In this example, the inference engine checks the conditions of each rule and executes the action of the rule that is fired first. If 'rule 1' is fired, the system call function *r_fork* invokes another Ruleset named 'display_alarm'.

The fuzzy strategy is provided for *fuzzy* reasoning[4,5]. A membership function of fuzzy reasoning is represented as a special attribute of the variable in the frame. Here is a fuzzy rule sample.

```
rule_name example_of_fuzzy_reasoning ;
{    { control = fuzzy ; }
rule 1     if  { input.error is negative_small }
           then { fset ( output.change,  positive_small ) ; }
rule 2     if  { input.error is positive_small }
           then { fset ( output.change, negative_small ) ;}
rule 3     if  { input.error is zero }
           then { fset(output.change, zero) ;}
}
```

Figure 2 illustrates how fuzzy reasoning is done. Membership functions, *positive_small, negative_small* and *zero*, are defined for the frame variables; *input.error* and *output.change*. In fuzzy reasoning, each shape of the membership function for the output (*output.change*) is calculated using grade value of the input (*input.error*). The results of individual rules are represented as a combined area, and the final value of the output is determined by dividing the combined area into two equal parts.

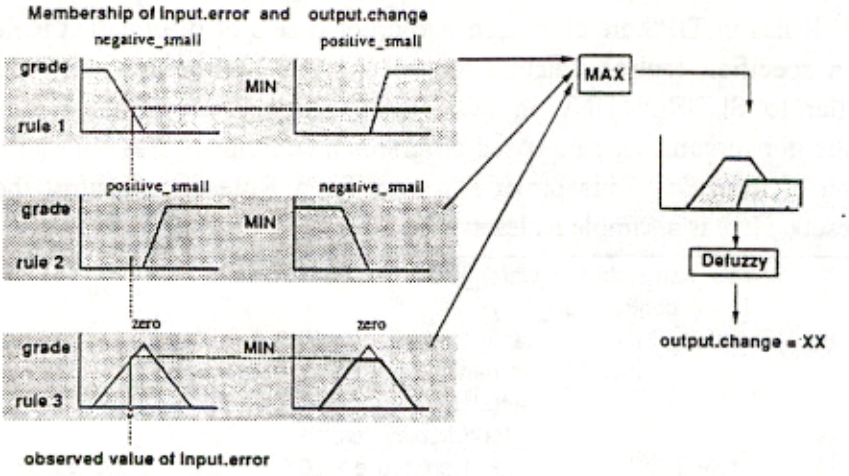


Figure 2. Flow scheme of fuzzy reasoning

In TIPS, there are two ways of using these knowledge expressions. One is an interpretive execution that uses the knowledge definition file sets, and another is direct execution that uses the c++ objects converted from the knowledge definition file by the Ruleset compiler.

Process Data Handling Objects

In an intelligent plant monitoring system, a shared memory mechanism is a typical facility for accessing plant data. We have expanded the functions of UNIX-IPC (shared memory, message, queue, semaphore, remote procedure call, etc.) and implement objects in TIPS.

In the research and development phase a prototype monitoring system often connects with a simulator instead of the actual plant. The simulator is usually written as a FORTRAN program, and it is not easy to communicate with the C++ program on the shared common memory. Therefore we prepared an utility that automatically makes an interface library using FORTRAN compiler outputs. If this interface library is used, the objects for knowledge processing access the variables of the simulator easily.

Graphical User Interface Objects

The objects of the TIPS graphical user interface require the X window system. This class group is composed of two packages. One is a class group that expands graphical parts based on Motif for plant monitoring and the other is a class group based on InterViews[6]. The user can select either package according to their purpose. For instance, the Motif based package is selected when the interactive style is important, and the InterViews package is chosen when the output style to a PostScript printer is important. If the user uses the InterViews package, a special interface design utility (interface builder) is available.

The communication method is very important in the design of human interfaces. The concepts behind multi modal interfaces will be important in the plant monitoring system of the future. TIPS prepares the objects which treat the sound, the still color picture, and animation as a means of achieving a multi modal interface.

TIPS APPLICATIONS

Presently, we are developing the following prototype application systems using TIPS.

- An expert system for the diagnosis of turbine systems in a power plant.
- An advanced process control system.
- An expert system for the diagnosis of circuit breakers in a sub station.

The fault diagnosis system for the turbine is a typical TIPS application. This system monitors the components in the plant (turbine, generator, condenser, etc.), detects failure symptoms, and infers which component has failed. The knowledge on which the diagnosis is based is extracted from technical manuals and dialogue with human experts. Figure 3 shows a part of the causal relationship tree used for a diagnosis. Each variable reflects the conditions of the component. The tree structure corresponds to a Ruleset.
The key parameter (TURB.EFF_DEVIATION) is checked periodically, and TURB.EXHAUST_TEMP, COND.VACCUM, GEN.GAS_PRESS) are also checked, if necessary. Fuzzy reasoning is used to check the status of individual components. Most of the parameters in Figure 3 are monitored, but the underlined parameters are not. When the cause of a failure is identified using monitored parameters (only input parameters of the Process Data Interface), the diagnosis system immediately suggests a countermeasure. If the cause cannot be identified, the system questions the operator about information regarding auxiliary components which are not entered in the PDI.

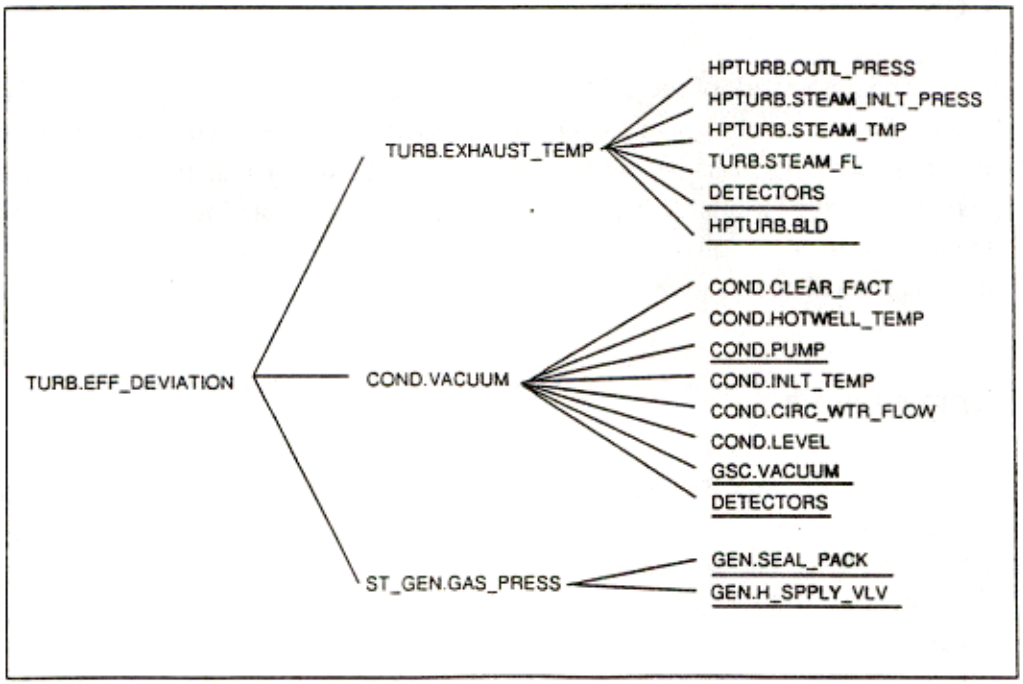


Figure 3 Example of a causal relationship tree for diagnosis

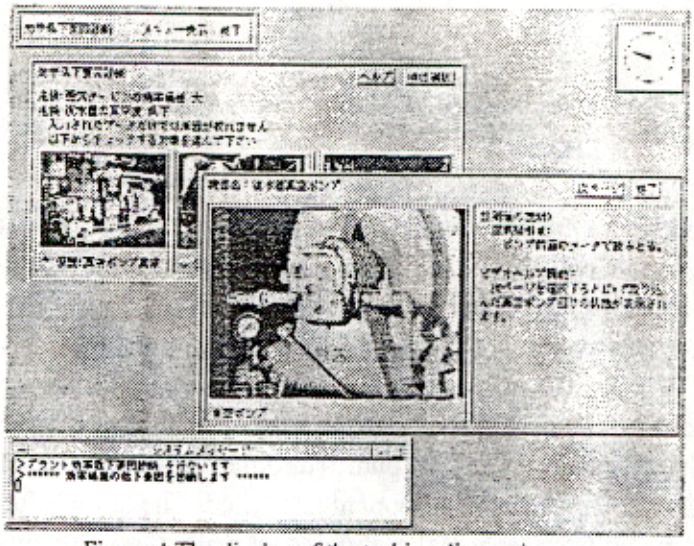


Figure 4 The display of the turbine diagnosis system

The interface between human and computer is an important factor for such interactive systems. Using graphical user interface objects, we can easily apply multi-media data processing to the dialogue interface to facilitate smooth communication. Figure 4 shows the display screen of this diagnostic system. A digital picture of the component is displayed along with questions, and the component's condition can be judged without going to the site using images from an industrial video camera on the display. A prototype system has been developed, and its validity was checked by comparing it to a real case. The diagnostic system is now being improved for practical application.

CONCLUSION

The framework of the TIPS object-oriented toolkit has been presented. TIPS is a set of objects for constructing a intelligent plant monitoring system such as component diagnostic expert system, and can be used for rule-based reasoning and frame-based reasoning. Our experience with TIPS has convinced us of the importance of object-oriented programming for the improvement of software re-usability. In the next step, we will expand TIPS to research into distributed cooperative intelligent agents.

REFERENCES

1. Thomas J.L. et al. "Real-Time Knowledge-Based Systems", AI magazine, Vol. 9, No.1, 27-45, (1988).
2. Margaret A. Ellis et al. "THE ANNOTATED C++ REFERENCE MANUAL",Addison Wesley,(1991)
3. Stefik M. J. et al. "Rule-oriented programming in LOOPS", Knowledge-based VLSI Design Group Technical Memo, (1983)
4. Zadeh, L. A. "Fuzzy Sets", Inf. Control, Vol. 8, 338-353, (1965).
5. Mamdani, E. H. "Applications of Fuzzy Algorithms for Control of a Simple Dynamic Plant", Proc. IEEE, Vol. 121, 1585-1588, (1974).
6. M. A. Linton. "Composing User Interfaces with InterViews", COMPUTER, No. 2, 8-22, (1989)

A COMPUTER AID FOR SAFETY ASSESSMENT AND CONFIGURATION MANAGEMENT OF COMPLEX SYSTEMS BASED ON PSA MODELS

Peter Kafka, Ovid Lupas, Jie Wu and Markus Zimmermann

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH
Forschungsgelände, 85748 Garching, Germany

INTRODUCTION

In many industries there is a great demand to design, build *and* operate the installations on the utmost achievable reliability and safety level. The PSA Technology has matured over the last fifteen years to the point where important assessments and decisions regarding these two challenges can be based on its methods and results. The operation of large and complex installations (e.g. NPP's) is influenced day-to-day by random events on components and planned maintenance and repair work by the personnel. The safety impact and management of these complex event scenarios, which till recently were treated exclusively by engineering judgment and the pre-formulated operating manuals can be better quantified with the aid of on-line advice by intelligent computerized PSA models [1].

The Test Control Room[2] (TCR), which is an engineering simulator with a screen-based control room environment is used at the GRS as a tool for safety analyses of NPPs. The TCR performs classical safety analyses supported by visualization of simulation results and by interactive handling of simulation codes. However, in order to provide extensive support to the analyst, additional information sources, including knowledge on procedures, on diagnostic and explanatory facilities, on PSA as well as the background knowledge on constructive and operational details of the plant are offered by the Analyst Decision Support (ADS) system, which is under development. The analyst is regularly confronted with questions such as which event is the most dangerous or the most probable to occur, what is the safety impact of the failure of specific components for a given state of the plant, or which actions e.g. restoration will minimize risk measures. For answering such questions a Reliability Adviser[3] (RA) which superimposes an on-line probabilistic perspective on the deterministic safety requirements is being implemented in the ADS. The RA is also intended to be used as a stand-alone system to daily advise the plant management on-line as to which current events contribute to an increase of the plant reference risk level and what strategy regarding system configuration, maintenance and repair management is the most

THE RELIABILITY ADVISER

The aim of the RA as part of the ADS system consists in giving the analyst on-line within a simulation session the tools needed for:

- assessing the change of plant risk-level when certain system and reliability parameters are changed (e.g. status of components, failure rates, test intervals),
- evaluating the relative importance of different event sequences (based on associated frequencies) and the impact of failures on them.

The risk-level change is calculated on-line and presented on three levels: loss of system functions, occurrence of event sequences and occurrence of core damage. Fault trees (FT), event trees (ET), reliability data base and minimal cut sets (MCSs) from a plant specific PSA are used as input to the RA. Components in mimic diagrams of subsystems may be chosen interactively, and the failure probabilities for their failure modes may be changed. The failures may be either introduced by the simulator, or by specific mimics of systems and components. The interactive possibilities include hypothetical component failures and restoration to the actual situation. A dialogue system enables the user to look up a description of the most important scenarios in a hypertext data base and to request procedural information on counter measures and corresponding time limits.

Fault Tree Linking and Calculation of Importance Measures (IM)

The evaluation of the risk-level change in the RA is based on the MCSs of the system functions (SF) available from an existing PSA. The MCSs at sequence level are generated with consideration of the success paths. At first the common functional elements (CFE) between SF are identified and then the corresponding cut sets are eliminated or processed according to the individual sequence in the ET. If a MCS of a system function in a failure path (SFF) of a sequence (or a part of a MCS) is the same as a MCS in success paths, it has to be deleted in SFF, as such a (successful) MCS cannot be a failure cause.

Example: Let us assume that in a sequence with 4 system functions with minimal cut sets MCS1,... MCS4, the functions 1 and 2 succeed and 3 and 4 fail. A MCS is the minimal combination of components whose failure leads to the failure of the SF. The MCSs of the SF results from the union of all these independent combinations. The MCSs at sequence level can be written as

$$MCS(SEQ) = \overline{MCS}1 \cap \overline{MCS}2 \cap MCS3 \cap MCS4 \qquad (1)$$

If C1 represents the CFE between all MCS1 to MCS4, and C2 the CFE between failure paths MCS3 and MCS4, MCS(SEQ) can be written as:

$$\overline{C1 \cup MCS1'} \cap \overline{C1 \cup MCS2'} \cap (C1 \cup C2 \cup MCS3') \cap (C1 \cup C2 \cup MCS4')$$

$$= \overline{C1} \cap \overline{MCS1'} \cap \overline{MCS2'} \cup (C1 \cup C2 \cup MCS3') \cap (C1 \cup C2 \cup MCS4')$$

where MCS1',... MCS4' are those MCS of the four SF having no CFE. The Boolean reduction of the "AND" product of MCS3' and MCS4' can be simplified as in (2)

$$MCS(SEQ) = \overline{C1} \cap \overline{MCS1'} \cap \overline{MCS2'} \cap (C2 \cup MCS3' \cap MCS4') \qquad (2)$$

Random events (e.g. component failures) that causes changes of the plant risk level can be modeled by MCS manipulation. The failure probabilities of their basic events in the MCSs are set on 1 if failure is assumed (with re-minimalization of the MCSs, due to the possible apparition of not minimal cut sets) or on 0 respectively if failure is considered impossible (with deletion of the individual MCS containing the basic events).

communicate through the RTworks message server (RTserver). The server receives messages from every module (client) and distributes it to its destination module(s). (Fig. 1).

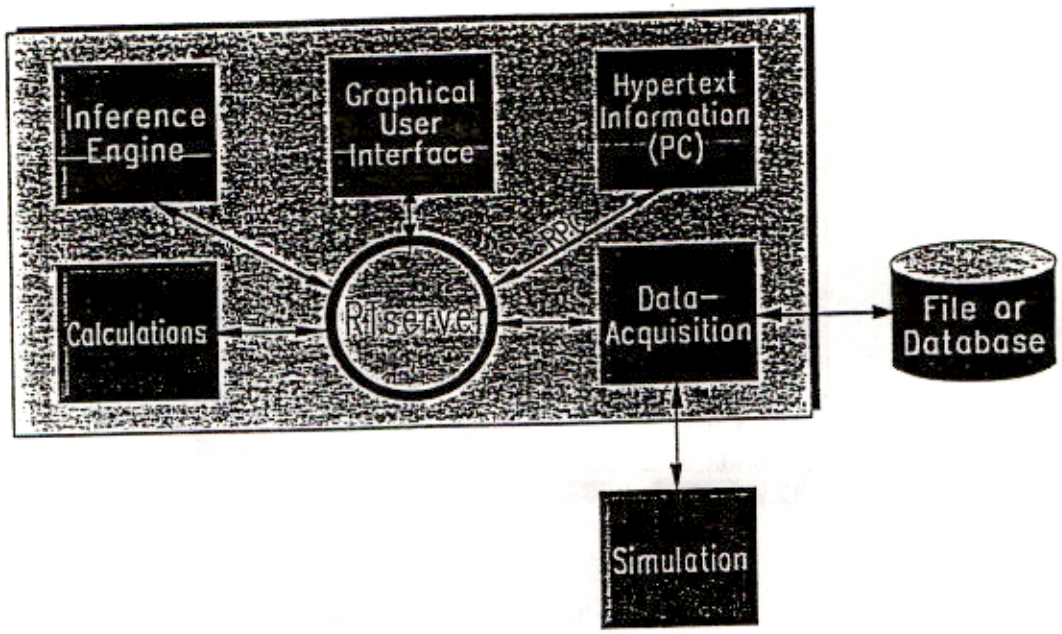


Fig. 1 Reliability Adviser: Client/Server architecture.

The major components of RTworks are:

- An Inference Engine that provides rule-based inferencing, statistical and trending functions to analyze historic and current real-time data and provide information such as alarms, diagnostics or predictions about future events.
- A graphical User Interface based on DataViews with a sophisticated point-and-click environment and the capability to display changing data in real-time. It runs within the X-Window system.
- A Data Acquisition Module to build easily interfaces to external data sources. Therefore the Reliability Adviser can get real-time data from an external process as well as from a simulator, file or database.

The Background Information System running on PC under Windows 3.1 was developed with the Hypertext Software ToolBook, and was designed as a client to the RA, allowing thus a direct communication. The user is supported by text and graphics based information on the CRT of the PC. Thus the RA can provide detailed information on the present plant state automatically or descriptions of components modeled in the system by clicking on them. Modules written in CC+ provide extensive calculations as e.g. the sequence probabilities under consideration of CFE.

An easy navigation through the RA is possible due to the point-and-click facility of the system. A template that surrounds every view contains objects which are to be watched at all times, shows info-, alarm- or warning-messages and allows a direct access to important views from every point in the RA. A zoom facility and a 2-D slider on the template allows the user to zoom and move on every point of the displayed view.

The main modules of the RA are:

1. Event Trees (Fig. 2).The SF and sequence probabilities are displayed and are updated automatically as the system state changes during the simulation in the TCR. The color of each path shows its reachability.

2. Fault Trees. FTs from the PSA can be graphically displayed and be represented through their appertaining MCSs.

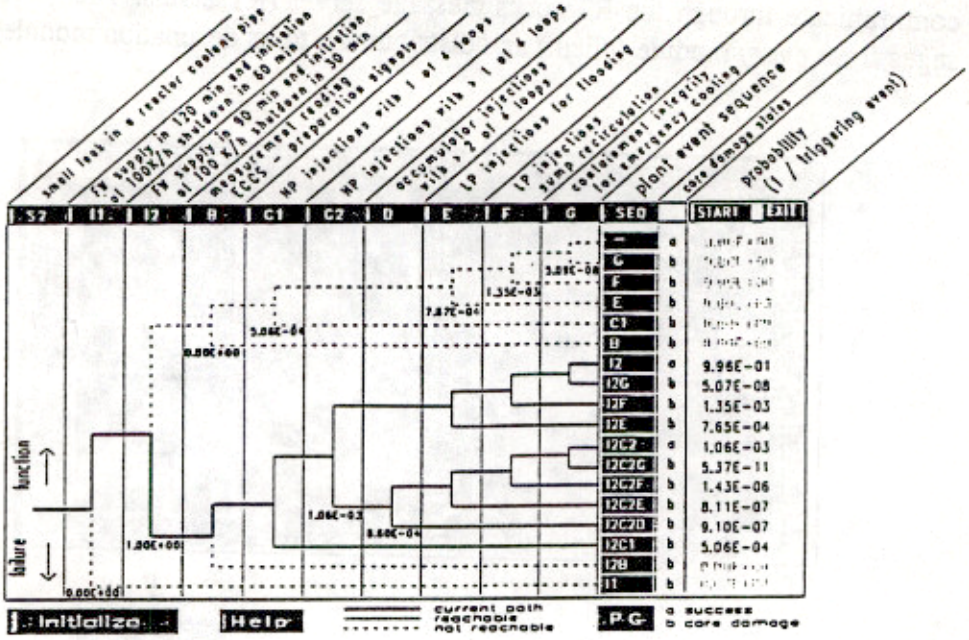


Fig. 2 Event Tree: Small-break LOCA

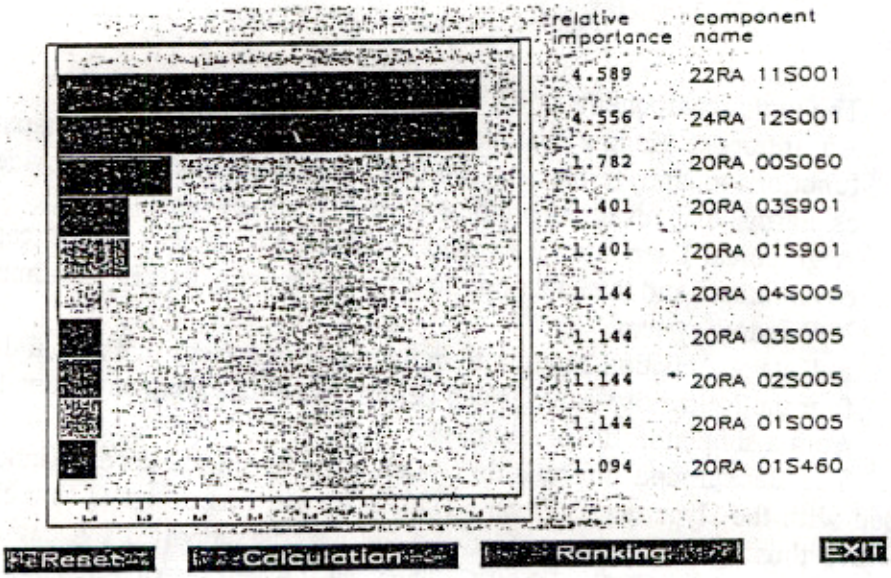


Fig. 3: Components sorted according to their contribution on SF I1

3. Mimic Diagrams. When the user selects a specific mimic diagram all its components (e.g. valves, pumps..) that were considered in the PSA will be displayed in color. When clicking on a component the user can choose whether he wants to have a description about it, or if he wants to declare it as failed. He can also get a list of the according failure models with their present failure probabilities. These values can be edited as well. All components influencing a specific SF can be highlighted on demand.

4. Importance Measures. Are displayed textually as well as graphically (Fig. 3).

5. Data and Specification. The user has access to all the input data of the system, e.g. MCSs, sorted lists of components and a detailed list of function elements with specific data through an editor.

The IM rank the components (basic events) quantitatively according to their contribution to the probability of a top event (e. g. SF-failure) and provide guidance in search of the most efficient way of improving the system reliability by minimum effort. Depending on the top event considered, the computation is done on the three levels mentioned previously (system function, sequence and core damage level). In view of identifying plant vulnerabilities, relative importances, i.e. Birnbaum IM, risk reduction worth and risk achievement worth relative to a component can be computed in the RA by using the rare event approximation for an intact plant as well as for a plant were several components fail.

Repair and Maintenance Management

The RA can be used for supplying guidance on optimum use of resources and minimizing risk-level increase as:

1. Reevaluation of the plant risk level and updating of the component failure probability when the surveilance test intervals, and repair or maintenance frequency are modified. For a repairable, periodically tested component with maintenance action the average unavailability U can be calculated as:

$$U = \tfrac{1}{2}\lambda T_o + f_R \frac{T_R}{T} + f_M \frac{T_M}{T} \qquad (3)$$

where: λ = constant failure rate; T_o = operating time; T = surveilance test interval; T_R, T_M = repair maintenance duration; f_R, f_M = repair, maintenance frequency

Although a repaired component can not be always considered as good as new and the failure rate may not be constant after repair or maintenance, the relative risk-level change can be evaluated and used for optimizing the repair sequence, the maintenance duration, the frequency and test intervals and to check whether the original values of these parameters were appropriately assigned.

2. The RA can be used to advise which component should have the repair priority when several components are to be repaired. This optimization considers which component's restoration mostly reduces the plant risk level. The sequence with the smallest area defined by the risk reduction and the corresponding repair duration should be choosen.

REALIZATION

The main hardware platform consists of a DEC station 5000 with ULTRIX 4.3 as operating system. All modules of the RA are running on this workstation except the Background Information System, which runs as a separate client on an IBM compatible PC 80486 within the same network. In this way the user disposes of an additional display where any information that extends the on-line help facility of the RA can be shown by means of a Hypertext system. The communication mechanism used is RPC (Remote Procedure Calls) in connection with the TCP/IP network protocol.

The RA was realized by means of the real-time expert system shell RTworks,[4] Ver. 2.1. RTworks is a suite of software tools written in the C programming language for the development of time-critical monitoring and control systems. Its open architecture is based on a distributed client-server model. Applications can consist of a server and clients running on a single workstation or the clients can be distributed across multiple processors in a heterogeneous network. As RTworks is available in a variety of real-time operating environments, the RA can be implemented easily on different hardware platforms. As RTworks is an expert system shell all its components are fully integrated in the RA. All processes

6. Background Information. This module allows the control of the Hypertext based Background Information System running on PC. This System is optional and could be replaced by an adequate system on the workstation if no PC is available.

FURTHER IMPROVEMENTS AND PROSPECTS

Based on the experience with the DEMO version, where only a few FTs and ETs have been processed, a full-scope PSA will be implemented with about ten ETs and a hundred FTs representing roughly 2000 function elements of the plant. The modeling of various maintenance strategies (e.g. various fixed intervals; failure dependent flexible intervals; so called reliability centered maintenance) should advise plant personnel about actual risk and burden reduction possibilities. Changes in the system structure require an update of the FTs and the MCSs calculation. For that procedure a tool box with adequate programs will be added and intermeshed to the RA. Short response times of a few minutes are desirable, without giving up the level of detail of the underlying PSA models.

Considering these improvements following observations seem reasonably justified:

- The strength of a RA as stand alone system is the possibility to focus on dominant risk contributors and to advise on-line plant personnel during normal plant operation and abnormal occurrences in minimal-risk decision making. There appear to be no technical obstacles that would prevent converting any available Level 1 PSA into a RA, enabling utilities to be operationally flexible on an optimum safety level[5,6].
- A RA would allow plant personnel to avoid complex plant configurations which reduce the plant safety. Small risk contributions can result in relaxing requirements and significant contributions should be avoided.
- Specific expansions of the ideas of a RA can be used not only regarding minimal- risk decision making but also for more commercial aspects like the identification of the most cost effective repair and maintenance strategy with respect to high plant performance.
- Nowadays there is a preference to recommend the daily use of the RA by the plant management, but safety analysts can use it also for pre-optimizing adequate safety management actions at plants under operation.

Acknowledgement

This on-going research work is funded by the German Federal Minister for Research and Technology (BMFT) under contract RS 758A.

REFERENCES

1. P. Kafka, Risikomanagement des Anlagenbetriebs, *Atomwirtschaft* 36:421 (1991)
2. D. Beraha, H. Jahn, O. Lupas, T. Voggenberger. Extended support for accident analysis in the test control room, *Kerntechnik* 58:115 (1993)
3. IAEA Report, TCM on use of PSA for optimizing NPP operational limits and conditions, Barcelona, Spain, September 1993
4. --, RTworks product family overview, Talarian Comp., Mountain View, CA
5. B.E. Horn, The essential system status monitor for Heysham 2 nuclear power station, TCM, IAEA, Vienna, October 1988
6. M.B. Sattison, H. J. Reilly, From PRISIM to IRRAS/SARA; lessons learned in living PSA, 2nd TÜV-Workshop on living PSA application Hamburg, May 1990

025 PSA for Dynamic Systems: Analysis Techniques

Chair: N.O. Siu, INEL

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

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

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

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

IMPROVING THE EFFICIENCY OF MONTE CARLO METHODS IN PSA BY USING NEURAL NETWORKS

Marzio Marseguerra, Enrico Zio

Dept. of Nuclear Engineering
Polytechnic of Milan
Italy

Abstract - Monte Carlo methods represent an useful approach to PSA investigations, due to their capability of treating in detail different situations, even very complex, with relative ease. However, good statistical estimates of the desired quantities are generally obtained at the expenses of large computational times. Therefore many efforts have been devoted to the development of time–saving techniques. In spite of the improvements introduced, the analysis of real plants still requires exceedingly large running times, and new shortcuts are most welcomed. In the present paper we address this problem with the aid of the Artificial Neural Network methodology.

A first utilization aims at shortening the time required for sampling from complex distributions resorting to a vector quantization. This problem is hereby faced making use of the self–organizing Kohonen's network.

A second application refers to the so called "dynamic" PSA, in which the physical evolution of the plant process variables strongly affects the safety features of the plant itself and, therefore it must be accounted for. This dynamic analysis requires solving the mathematical models which describe the plant's behaviour. The involved equations are generally integrated numerically, with time steps which are much smaller than the time intervals of interest in PSA studies since they are related to the time constants of the process evolution. Due to the exceedingly large computer times, the procedure is still prohibitive for real plants and, at present, the research in the field is concentrated on the development of new methodologies currently tested on simple study cases. In this work, a multi–layered, supervised neural network, trained by the error back–propagation algorithm, has been used to provide the solutions to the mathematical models. The results of a study case have shown that the artificial neural networks are capable of directly arriving at a satisfactorily approximated solution even for times much larger than the time constants of the underlying process. Due to the intrinsic capability of parallel distributed processing of the neural networks, this advantage is expected to be more evident in the future parallel computers.

INTRODUCTION

Monte Carlo simulation methods[1-4] have been extensively used in reliability assessments, in particular within the fault tree and block diagram analyses. In general, one resorts to Monte Carlo simulation for the analysis of systems which are too complex and too large to be managed by analytical methods. In addition to the system complexity, the *rare event* nature of the failures in real plants renders the reliability analysis such that large computer times are required in order to get good statistical estimates of the desired quantities. For these reasons, many time–saving techniques such as the variance reduction methods have been introduced but more, also of different kind, are still welcome.

A first possibility here investigated aims at reducing the time required for sampling from given probability distributions. This is an important issue in the Monte Carlo simulations where a very large number of samplings is usually required. Obviously, the burden is heavier in case of complex distributions. In the reliability field, typical examples are the Weibull or other, more general, inhomogeneous Poisson distributions. Other examples are the multivariate distributions. In these cases, the sampling may be drastically simplified by resorting to a self–organizing Kohonen's map[5] trained to perform a vector quantization.

The other possibility here investigated concerns the so called *dynamic* PSA, which is an approach to reliability problems that is receiving more and more attention. Indeed, the increase in the computational power of today's computers has allowed the researchers to turn their interest to the possibility of including within the probabilistic model a description of the physical processes developing in the plant. This would account for a more realistic and comprehensive risk analysis that pays attention to the evolution of the plant process variables and to their mutual interaction with the hardware. Obviously, this approach requires major efforts in the development and solution of reasonably detailed models of the physical phenomena occurring in the plant. In this framework, the Monte Carlo simulation method seems to provide a suitable technique to treat dynamic aspects in PSA. In the dynamic scenario, a drastic increase of "slowness" is due to the fact that the involved phenomena evolve with time constants that are much smaller than those pertaining to the stochastic transitions so that in general the analysis must be carried out with very short time steps. Therefore, the dynamic approach is almost prohibitive unless suitably simplified models describing the evolution of the physical processes in all the system configurations and efficient algorithms for their solution are developed. Here we investigate the feasibility of solving the equations relating to a simple study case by using a multi–layered, supervised neural network trained by the error back–propagation algorithm.

In Section 2 and 3 we describe the main characteristics of the self–organizing Kohonen's map and present the application of this artificial neural network to the random sampling from a bathtub probability density function; in Section 4 and 5 we describe the multi–layered feedforward neural network and present the results of a simple study case. Eventually, some remarks are given in the concluding Section.

THE SELF–ORGANIZING KOHONEN'S MAP

The self organizing Kohonen's map has the property of creating a spatially–organized internal representation of the features distinguishing various input signals. Typically, the Kohonen's map is a one–dimensional string, or a bidimensional grid.

composed of interrelated nodes, each one containing a reference vector (weight vector) of the same dimension as the input vectors. During the self–organization, the nodes become specifically tuned to various patterns of input, or classes of patterns, through an unsupervised learning process.

Here we shall briefly report only the basic principles underlying the learning process of a Kohonen's map which consists in the determination of all the weight vectors. First of all a matching criterion between the input pattern and the weight vectors of the nodes must be introduced: typical choices are the dot product and the Euclidean metric. In correspondence of a given input vector, this criterion allows to select the winner node, that is the node whose weight vector "best matches" the input. For all incoming inputs, the best matching nodes are selected and the weight vectors are updated so to match even more closely the inputs. A crucial point in the formation of the ordered map is that the nodes be adjusted not independently of each other but rather as topologically related subsets. In other words, not only the weight vector of the best matching node is brought closer to the input pattern vector but also a suitable number (to be decreased during the learning) of its neighbours, so that an area of the map is created which is related to the features of the presented input pattern.

In the course of the learning process, the nodes in the map responding to given inputs tend to become spatially ordered so to perform a sort of cluster analysis: by so doing different areas of the map are devoted to feature–differing families of input signals. Moreover, it can be shown that the weight vectors tend to be located in the input space in such a way that they approximate the probability density function of the input patterns. Once the map is organized, as a new input vector is fed to the network it activates that particular node which most closely encodes its characterizing features.

RANDOM SAMPLING WITH KOHONEN'S MAP

The possible use of the Kohonen's map for accelerating the sampling procedure from complex distributions has been investigated with reference to an inhomogeneous Poisson distribution with a bathtub–like probability density. This distribution typically describes the probability for the failure times of many plant components throughout their life, from the early failures to the aging. Here we considered the following failure time probability density

$$\lambda(t) = 2.8 \cdot 10^{-5} \left(\frac{t}{25000} \right)^{-.3} + 2 \cdot 10^{-5} + 1 \cdot 10^{-3} \left(\frac{t}{5000} \right)^{4}$$

A one–dimensional Kohonen's map composed of 500 nodes has been trained to obtain the vector quantization and the final weights, which represent the failure times, are plotted in Fig. 1 *vs.* the node numbers. Each time sampling with the usual procedures would require three uniform random samplings, three logarithms, three exponentiations and finally a minimum search among three numbers. With the Kohonen's map only one uniform random sampling is sufficient: that of selecting one of the nodes. Then, the associated weight represents the required time value. Fig. 2 reports the histogram of 20,000 such values, together with the analytical probability density plotted for comparison. It appears that the data are in good agreement. Moreover, it turns out that the reduction in computer time is of a factor of ~ 20 so that the

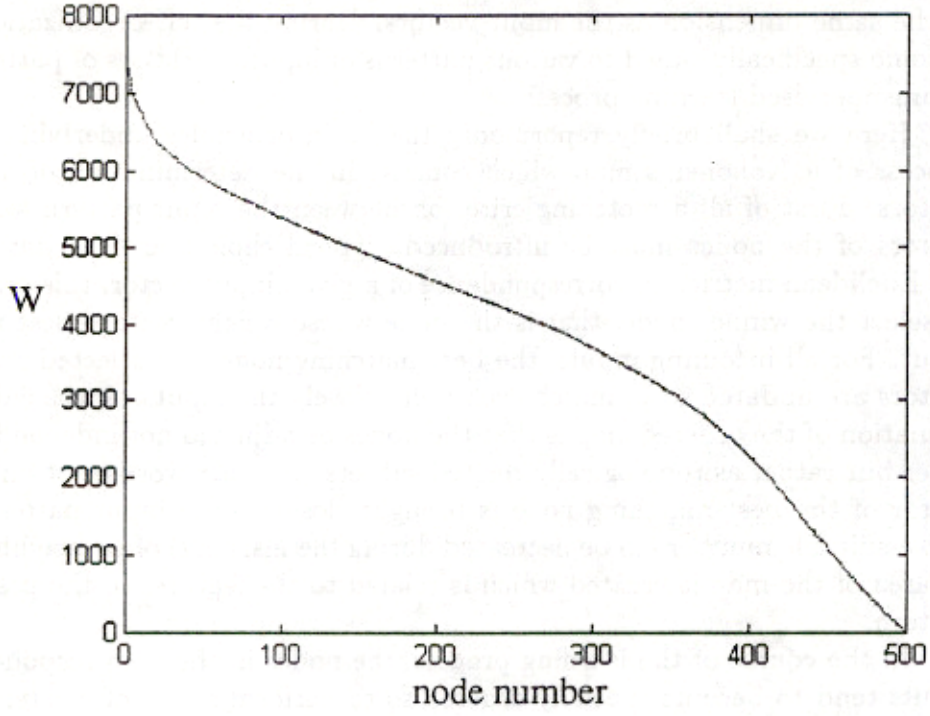


Figure 1. Plot of the weight values W vs. the nodes numbers

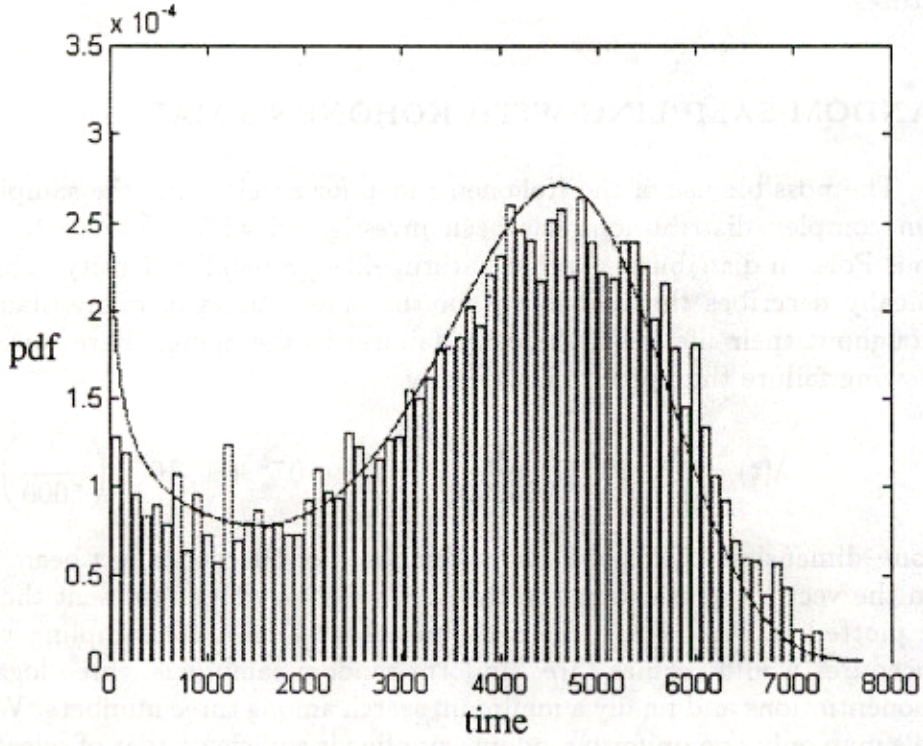


Figure 2. Histogram of the 20,000 values sampled with Kohonen's map and the corresponding analytical probability density function

THE ARTIFICIAL NEURAL NETWORK TRAINED BY THE ERROR BACK PROPAGATION ALGORITHM

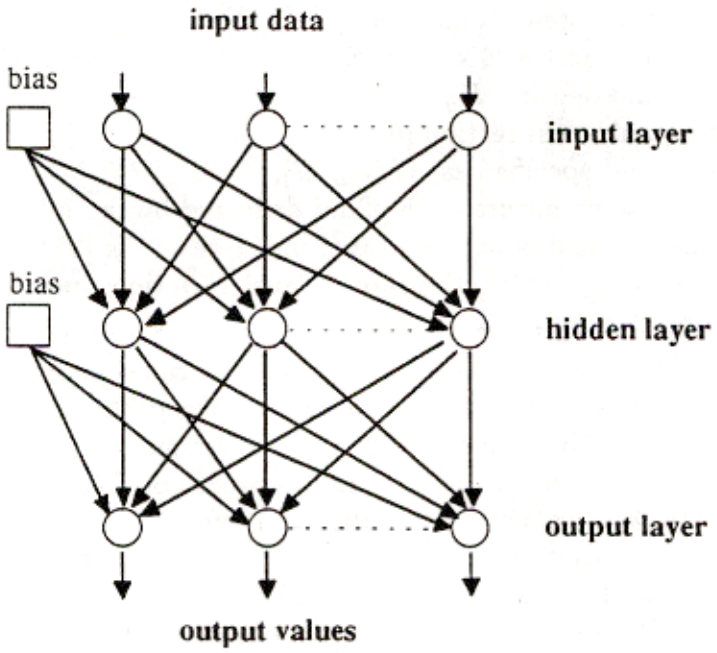
The *supervised, multilayered, feedforward neural network*, in its simplest form, consists of three layers of processing elements: the input, the hidden and the output layers, with n_i, n_h and n_o nodes respectively, linked by weighted connections [6-7]. The signal, which consists of n_i real values feeding the input nodes, is processed forwardly from the input to the output layer (Fig. 3). Each node collects the sum of the output values, weighted by the connection strengths, from all the nodes of the preceding layer, processes this information through a sigmoidal function $f(x) = (1 + e^{-x})^{-1}$ and then delivers the result to all the connections towards the nodes of the successive layer. In the present work both input and hidden layers have the additional bias node which acts as a threshold in the argument of the activation function and whose output always equals unity.

The values of the connection weights are determined through a training procedure. In this case we have adopted the usual error back-propagation algorithm which follows from the general gradient descent method[6-7]. In short, the algorithm consists in repeatedly presenting a set of n_p input and corresponding output patterns, and iteratively adjusting the values of the connection weights so to minimize the *average squared output deviation error function*, or *Energy function*, over all training patterns and all n_o outputs, defined as

$$D = \frac{1}{2n_p n_o} \sum_{p=1}^{n_p} \sum_{l=1}^{n_o} (t_{pl} - o_{pl})^2 \qquad (1)$$

where, t_{pl} and o_{pl} are the true and the network-computed values of the l-th output node, to the p-th pattern presented.

Through this training procedure, the network becomes able to build an internal representation of the input/output mapping of the problem under investigation.



After the training is successfully completed, new input patterns are presented to the network which is capable of recalling the information, stored in the connection weights during training, to produce the corresponding output, coherent with the internal representation of the input/output mapping. Notice that the nonlinearity of the sigmoidal function of the processing elements allows the neural network to learn arbitrary nonlinear mapping. Moreover, the functioning of one node does not depend on the states of those other nodes to which it is not connected. This allows for efficient distributed representation and parallel processing exploitation in the near future.

THE STUDY CASE

The possibile use of the artificial neural network described in Section 4 for the solution of differential equations has been investigated with reference to a simple study case of a dynamic process system[4,8-9] which consists of a tank containing a fluid whose level is controlled by means of three active units. Unit 1 and 2 are two inlet pumps while unit 3 is an outlet valve. All components work independently and each of them is either in an ON, or in an OFF state. A thermal power source heats up the fluid: for simplicity's sake, we assume that this source is uniformly distributed and no heat is transferred outside the tank (adiabatic condition). Moreover the fluid delivered by the inlet components is assumed to mix instantaneously and the outlet flow rate is independent of the fluid head.

The two process variables of interest are the level $H(t)$ and the temperature $\Theta(t)$ of the fluid in the tank at time t. The mass and energy conservation laws applied to the system lead to the following system of differential equations:

$$\begin{aligned} \frac{d}{dt}[\rho A H(t)] &= \alpha_1 q_1 + \alpha_2 q_2 - \alpha_3 q_3 \\ \frac{d}{dt}(\rho A C H(t)\Theta(t)) &= \alpha_1 q_1 C\Theta_{in} + \alpha_2 q_2 C\Theta_{in} - \alpha_3 q_3 C\Theta(t) + W \end{aligned} \qquad (2)$$

where

- q_i is the flow rate of component i $[Kg/h]$;
- $\alpha_i = 1$ if the unit is ON or stuck ON, $= 0$ if the unit is OFF or stuck OFF;
- ρ is the fluid density $[Kg/m^3]$;
- A is the tank cross section $[m^2]$;
- C is the fluid specific heat $[J/Kg°C]$;
- Θ_{in} is the temperature of the fluid delivered by the inlet pumps $[°C]$;
- W is the thermal power generated inside the tank $[J/h]$.

We define $Q_i = \frac{q_i}{\rho A}$ $[m/h]$, the rate of level variation due to the i–th unit, $Q_{net} = \alpha_1 Q_1 + \alpha_2 Q_2 - \alpha_3 Q_3$ the net rate of level variation in the tank and $w = \frac{W}{\rho A C}[\frac{m°C}{h}]$.

In our experience the use of artificial neural networks requires focussing the analyst's attention not only to the mathematical aspects of the problem but also to the underlying physical implications. Here we performed the integration of the differential equation (2) using four artificial neural networks of the type described in Section 4. The four networks are devoted to different physical situations defined in terms of the net rate of level variation in the tank, Q_{net}, and of the temperature value Θ_{in} of the fluid as compared to its asymptotic equilibrium value, Θ_{as}. In particular, the first network, ANN1, predicts the solution to equation (2) for $Q_{net} > 0$ and $\Theta_{in} < \Theta_{as}$, ANN2 for $Q_{net} > 0$ and $\Theta_{in} > \Theta_{as}$. ANN3 for $Q_{net} < 0$ and $\Theta_{in} < \Theta_{as}$. and ANN4

bias node), 9 hidden nodes (plus the additional bias node) and 1 output node. The input quantities are: $Q_{input} = \alpha_1 Q_1 + \alpha_2 Q_2$; $Q_{output} = \alpha_3 Q_3$; Q_{net}; w; $\Theta(t_0)$; Θ_{in}; $H(t_0)$ and t_{fin}, the final time. The output of the network is the temperature $\Theta(t_{fin})$. A large number of different input–output patterns has been generated by means of a procedure consisting in randomly sampling the independent input values within specified ranges and analytically evaluating the corresponding output of eq.(2). In particular, we randomly chose Q_{input} within the range (1,5), Q_{output} within (1,3), w within (10,30), $\Theta(t_0)$ within (10,50), Θ_{in} within (10,80), $H(t_0)$ within (2,10), t_{fin} within (0,50) and (50,500), all in the corresponding units. The subdivision of the range of t_{fin} in two separate intervals has revealed necessary for a better training of the network.

After the training has been completed, each network has been tested on a different set of 100 new patterns randomly generated within the same ranges of the training patterns. In Fig. 4 we report the relative errors made by the four networks in the prediction of the temperature. As it can be seen, in all cases most of the errors are within few percents. These errors can be considered acceptable in view of the magnitude of the uncertainties that typically affect the data used in reliability analyses.

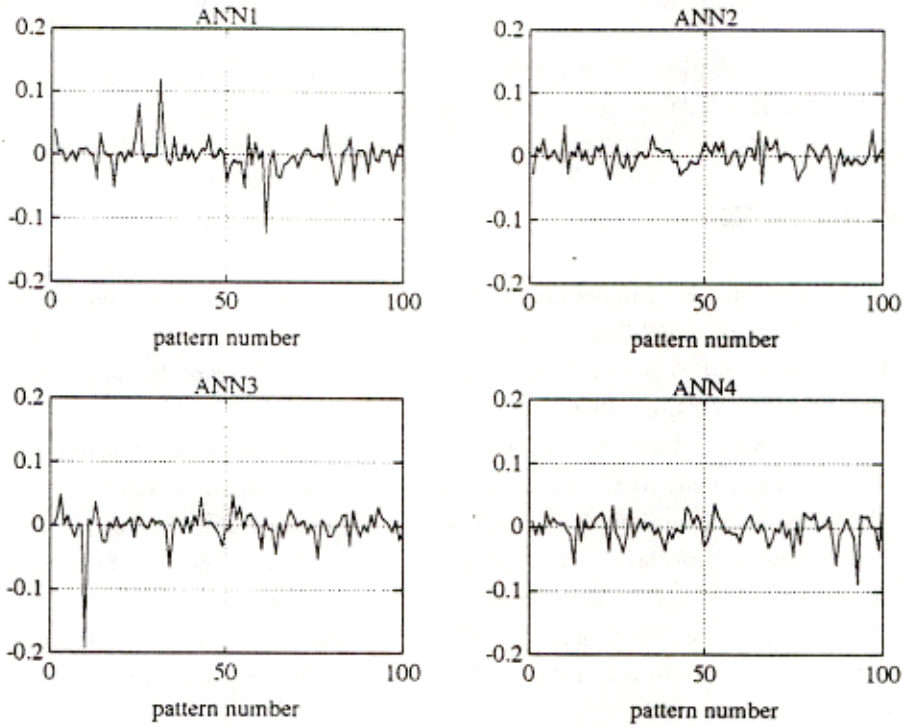


Figure 4. Relative errors made by the four neural networks in the prediction of the temperature $\Theta(t_{fin})$, over 100 patterns of test for each network

CONCLUSIONS

Monte Carlo methods represent an useful approach to PSA, due to the capability of dealing with complex systems with relative ease. However, the large computer times usually required by the analysis render almost mandatory the introduction of time–saving short cuts.

A first point in this paper concerns the possibility of simplifying the sampling from complex distributions by using a self-organizing Kohonen's map which, once trained, is capable of performing a vector quantization. An example of application of this technique has been presented with reference to an inhomogeneous Poisson distribution with a bathtub-like failure probability density function. Instead of the usual and rather intricate sampling procedure, this technique simply consists in a uniform random sampling of a node of the map and thus allows for a nice reduction in the computer time.

Also, in the paper we have faced the problems relating to the so called *dynamic PSA*, for which the Monte Carlo method seems very suitable. In our opinion this dynamic approach may be pursued only if methods of fast solution to the equations describing the evolution of the physical variables involved in the plant's processes are available. To this aim, we have here analyzed the possibility of using artificial neural networks to exploit their capability of delivering the required output almost instantaneously. A simple case study of a dynamic process system has been considered and a set of four multilayered, feed-forward neural networks has been trained to directly arrive at the solution at various final times. This allows to avoid the lengthy procedure of a stepwise integration. In all cases the networks seem to be capable of giving the output with a reasonable approximation, which can be regarded as acceptable when compared to the degree of uncertainty typical of the reliability statistical data.

Acknowledgments: The authors wish to thank P. De Capitani, G. Feldi and M. Lideo for their contribution to the work.

REFERENCES

1. H. Kumamoto. K. Tanaka and K. Inoue, Efficient Evaluation of System Reliability by Monte Carlo Method. IEEE Trans. on Reliability, Vol. R-26, N.5, 1977, pp. 311-315.
2. E. E. Lewis and F. Bohm, Monte Carlo Simulation of Markov Unreliability Models, Nucl. Eng. and Des. 77, 1984, pp.49-62.
3. C. Smidts and J. Devooght, Probabilistic Reactor Dynamics II. A Monte Carlo Study of a Fast Reactor Transient, Nucl. Sci. and Eng. 111, 3, 1992, pp. 241-256.
4. M. Marseguerra and E. Zio, Approaching Dynamic Reliability by Monte Carlo Simulation, Proceedings of the Nato Advanced Research Workshop on the Reliability and Safety Assessment of Dynamic Process Systems, Kusadasi, Turkey, Aug. 24-28, 1992.
5. T. Kohonen, The Self-Organizing Map, Proc. IEEE, Vol. 78, n. 9, 1990, pp. 1464-1480.
6. D.E. Rumelhart and J.L. Eds. McClelland, Parallel Distributed Processing, Vol.1, MIT Press, Cambridge MA., 1986.
7. B. Muller and J. Reinhardt, Neural Networks: An Introduction, Springer Verlag, 1991.
8. W.E. Vesely, A Time Dependent Methodology for Fault Tree Evaluation, Nucl. Eng. and Des. 13, pp. 337, 1970.
9. T. Aldemir, Utilization of the Cell-to-Cell Mapping Technique to Construct Markov Failure Models for Process Control Systems, PSAM Proceedings, Elsevier Publishing Co. Inc, 1991, pp. 1431-1436.

SENSITIVITY ANALYSIS TECHNIQUES IN RELIABILITY STUDIES

A. Dubi[1], A. Gandini[2]

[1]Ben Gurion University, Beer Sheva
[2]ENEA, CRE Casaccia (Rome)

INTRODUCTION

In the probabilistic analysis of systems, by which assessing the degree of confidence, under the point of view of performance and safety which we may associate to a given system during its operation, it is clear that, beside the correct knowledge of the data base, a key point is the identification of the important components. Such identification is in fact used in assisting the analyst in finding weaknesses in design and operation and in suggesting optimal modifications for system upgrade. Starting from the concept of importance introduced by Birnbaum[1] in 1969, a number of methods have been suggested so far to evaluate the relevance of basic components or component-related entities, such as cut sets, on system behaviour. The concept of importance function associated to Markov state probability vector has also been proposed[2], leading to the definition of sensitivity coefficients closely related to the Birnbaum importance. Rather than to component availability, these sensitivity coefficients are related to system parameters. On the other hand, Monte Carlo techniques are strongly emerging as a powerful tool for system life simulation, especially in those case in which interdependence between components, sequence of events not reducible to a markovian chain, multiprofile system evolution and varying levels of performance of systems formed by a large number of components may introduce considerable difficulties to identify an alternative approach. In these cases the use of Monte Carlo techniques appears mandatory (see Appendix).

A method to calculate directly sensitivity coefficients by Monte Carlo techniques have been proposed mutuating techniques well known in particle transport simulation[3]. A different method for calculating component importance has been used in the Monte Carlo simulation codes[4-7] AMIR and SPAR. These codes have been developed for reliability and availability analysis, respectively, mutuating Monte Carlo concepts developed in many years of research on particle transport simulation. Within these codes specific conventional functions and instructions are defined for user utilization. At each system "collision" (i.e., at each state vector change) these functions can give, in particular, a) the state of the system after "collision", b) the time at which it occurred, c) the component that (by failure or repair) triggered the system "collision", d) the state of any component (up, down, active, passive, etc.) at that moment. By proper instructions (i.e., calling special subroutines built in the main code) it is possible, in particular, a) to passivize, or activize specific components at that same moment, b) to force detection of a detectable failure of a particular component (of interest in maintenance studies), c) to rejuvenate a specific component by setting its birth time to current time and its age to zero. These above functions and instructions can be used in special subroutines to be defined by the user. At each system event the code goes to these subroutines before any further action. Non linear, nonmarkovian systems of high complexity can then be modeled through their proper use. They can also be utilized for tallying specific

It is the purpose of the present paper to discuss the sensitivity analysis techniques mentioned above, in particular those adopted in AMIR and SPAR codes. A simple procedure is proposed to obtain the Birnbaum importances related to the system components (and thereafter the sensitivity coefficients relevant to their parameters) without significant increase of calculational time. A number of significant examples are given demonstrating the validity of the method.

COMPONENT IMPORTANCE

In AMIR and SPAR the (normalized) component importance with respect to a given component j, which we shall call I_j^D, is given by the ratio between the times this component has been critical (i.e., making part of a minimal cut set) to system failure and the number of system failures during mission time (predefined in SPAR and up to first system failure in AMIR). Its relationship with the classical Birnbaum importance (I_j^B) will be given in the following. Define

ΔT	= Time interval considered
$\bar{A}_s$	= System unavailability (average in interval ΔT)
$\bar{A}_j$	= Component j unavailability
ΔT_j^{crit}	= Average time system is down when component j is critical
ΔT_j^{res}	= Average time to reset (repair) component j
$\Delta T_{sys/j}^{res}$	= Average time to reset system after failure in which jth component was critical
$N_{f,sys}$	= Average number of system failures in interval ΔT
N_j^{crit}	= Average number of critical failures of component j in interval ΔT
N_j	= Average number of failures of component j in interval ΔT

The average component j unavailability can be defined as

$$\bar{A}_j = \frac{\Delta T_j^{down}}{\Delta T} = \frac{\Delta T_j^{res} N_j}{\Delta T} \qquad (1)$$

The Birnbaum importance (I_j^B) for component j can then be expressed, for unavailability ($\bar{A}_s$) and unreliability ($\bar{R}_s$) analysis, as

$$I_j^B \equiv \frac{\Delta \bar{A}_s}{\bar{A}_j} \equiv \frac{\Delta T_{sys/j}^{res} N_j^{crit}}{\Delta T_j^{res} N_j} = \frac{\Delta T_{sys/j}^{res}}{\Delta T_j^{res}} \frac{N_{f;sys}}{N_j} I_j^D \qquad (2)$$

$$I_j^B \equiv \frac{\Delta \bar{R}_s}{\bar{R}_j} \equiv \frac{N_j^{crit}}{N_j} = \frac{1}{N_j} I_j^D \qquad (3)$$

respectively, where

$$I_j^D = \frac{N_j^{crit}}{N_{f;sys}} \quad \text{and} \quad I_j^D = N_j^{crit} \qquad (4\ a,b)$$

are the importances as calculated by AMIR and SPAR, respectively. Obviously, it is always $I_j^D \leq 1$. Expression (3) has been obtained from Eq.(2) considering $\Delta T^{res}_{sys/j}$ and ΔT^{res}_j equally diverging to infinity and then with their ratio equal to unity. In this case N_{fj}^{crit} may be viewed as the probability of component j being responsible for system failure (i.e., critical). In case a reset time ΔT^{res}_j in expression (2) for component j differs significantly from $\Delta T^{res}_{sys/j}$, importance I_j^B may become significantly different from I_j^D.

Calculating I_j^B as given by Eq.(2) in SPAR codes poses no difficulty since, beside I_j^D, this code gives also the quantities $N_{f,sys}$ (average number of system failures in interval ΔT) and N_j (average number of component j failures in interval ΔT), while quantity ΔT^{res}_j (average time to reset component j) may be assumed an a priori known quantity. Quantity $\Delta T^{res}_{sys/j}$ (average time to reset system after failure in which jth component was critical) can be evaluated with the current version of the code by proper definition of the user defined subroutines mentioned in the Introduction. The implementation of this capability within the main code is foreseen in a future version..

To demonstrate the validity of the above expressions we shall consider two simple examples.

Example 1

Consider a system formed by two components (1 and 2), both simultaneously running in parallel for a mission time of 500 hr. We assume for simplicity exponential distributions for failure and repair events. The system is assumed correctly operating if at least one component is up. The following state probabilities can be defined:

P_1 = Probability of system to be UP with both components 1 and 2 operating
P_2 = Probability of system to be UP with component 1 failed and component 2 operating
P_3 = Probability of system to be UP with component 2 failed and component 1 operating
P_4 = Probability of system to be DOWN with components 1 and 2 failed.

These state probabilities obey the Markov equations

$$\frac{dP_1}{dt} = -(\lambda_1 + \lambda_2)P_1 + \mu_1 P_2 + \mu_2 P_3 \qquad (5)$$

$$\frac{dP_2}{dt} = -(\mu_1 + \lambda_2)P_2 + \lambda_1 P_1 + \mu_2 P_4 \qquad (6)$$

$$\frac{dP_3}{dt} = -(\mu_2 + \lambda_1)P_3 + \lambda_2 P_1 + \mu_1 P_4 \qquad (7)$$

$$\frac{dP_4}{dt} = -(\mu_1 + \mu_2)P_4 + \lambda_2 P_2 + \lambda_1 P_3 \qquad (8)$$

λ_j and μ_j being the instantaneous hazard and repair rates for component j, respectively.

Let us consider first the values $\lambda_1 = 0.001$, $\lambda_2 = 0.001$, $\mu_1 = 0.1$, $\mu_2 = 0.1$. While it is obviously $I_1^D = I_2^D = 1$, by integration of the above equations and recalling that the jth component unavailability $\bar{A}_j = \frac{\lambda_j}{\lambda_j + \mu_j}$, we obtain directly

$$I_1^B = \frac{dP_4}{} = \frac{dP_4}{} \left(\frac{d\bar{A}_1}{}\right)^{-1} = 0.0095 \quad (= I_2^B) \qquad (9)$$

Apart from a normalization coefficient, importances I_j^B and I_j^D coincide. If we change then parameter μ_1 and set $\mu_1=1.0$, while it is always $I_1^D = I_2^D = 1$, we obtain

$$I_1^B = 0.0097 \qquad I_2^B = 0.00096. \qquad (10\ a,b)$$

i.e., importances I_1^B and I_2^B differ by a factor of 10. This discrepancy can be easily explained by the fact that in this case component 1 has a repair time relatively much larger than that of component 2. As a consequence, when component 2 is critical (together with component 1) to system failure, it is the repair of component 1 that will be generally responsible for system recovery.

If we apply expression (2), recalling that

$$N_{f,sys} = \int_0^{500} (\lambda_2 P_2 + \lambda_1 P_3)dt\ , \quad N_1 = \int_0^{500} (P_1+P_3)\lambda_1 dt\ , \quad N_2 = \int_0^{500} (P_1+P_2)\lambda_1 dt\ , \qquad (11)$$

we easily obtain, for these two cases:

for $\mu_1 = 0.1$ $\qquad I_1^B = I_2^B = 0.0096$

for $\mu_1 = 1.0$ $\qquad I_1^B = 0.0097 \qquad I_2^B = 0.00098$,

i.e., values very close to those of Eqs.(9) and (10 a,b).

Example 2

Consider the simple noncoherent system, become a classic, studied first by T. Inagaki and R.J. Henley[7] and considered also in Reff. 2,3. This system consists of the following components subject to failure: 1) a pump supplying liquid to a tank, 2) a level sensor and 3) a level controller (the control valve, the tank and pipes never fail). These components have the following failure modes: the pump supplies too much liquid, the sensor generates a spurious signal indicating that the liquid level is low, the level controller fails to respond to the signal from the level sensor. Correspondingly, the system has the following failure modes (the top-event being flooding):

1. the pump (component 1) supplies too much liquid to the tank and the level sensor (component 2) generates a spurious signal indicating that the liquid level is low,
2. the pump supplies too much liquid to the tank and the level controller (component 3) fails to respond to the signal from the level sensor,
3. the level sensor generates a spurious signal indicating that the liquid in the tank is low and the level controller responds correctly to the signal from the level sensor.

The 2^3 possible Markov states are illustrated in Table 1.

Assume ΔT equal to the mission time (500 hr) and the following parameter values:

$$\lambda_1 = 0.001\ /\text{hr} \qquad \lambda_2 = 0.002\ /\text{hr} \qquad \lambda_3 = 0.003\ /\text{hr} \qquad (12)$$

$$\mu_1 = 0.1\ /\text{hr} \qquad \mu_2 = 0.05\ /\text{hr} \qquad \mu_3 = (1/60)\ /\text{hr} \qquad (13)$$

Consider now as response the average system unavailability ,

$$\bar{A}_s = \frac{1}{\Delta T} \int_0^{\Delta T} [P_5(t) + P_6(t) + P_7(t) + P_8(t)]\ dt \quad . \qquad (14)$$

The unavailability $\bar{A}_s$ results 0.0225. The values of component importances I_j^D (obtained from

Table 2(+). The incoherence of the system is clearly evidenced by the negative value corresponding to the third component. Also for this case the validity of expression (2), and then the possibility to use it within the SPAR Code to calculate the Birnbaum importance, are confirmed.

Table 1. System States

State	Component 1	2	3	System
1	UP	UP	UP	UP
2	DOWN	UP	UP	UP
3	UP	UP	DOWN	UP
4	UP	DOWN	DOWN	UP
5	UP	DOWN	UP	DOWN
6	DOWN	UP	DOWN	DOWN
7	DOWN	DOWN	UP	DOWN
8	DOWN	DOWN	DOWN	DOWN

Table 2. Values of Importances I^D and I^B

	Direct Calculation	Calculation using Eqs.(4a) and (2)	
Comp.	I^B	I^D	I^B
1	.14	.072	.14
2	.83	.88	.83
3	-.030	.039	-.029

APPENDIX

As well known, a Markovian system evolution can be described by the differential equation

$$\frac{d\mathbf{P}}{dt} = A\,\mathbf{P} \qquad (A.1)$$

P being the probability vector and A the transition matrix. A basic assumption for a

(+) In presence of noncoherence, as may be the case with a component 3 failure, the jth indexed quantities appearing in Eq.(1-4) should be viewed as referring to repair events rather than to failure ones. In this case ΔT_j^{crit} would be the average time system is up when component j is critical, ΔT_j^{res} the average time for component j to fail, $\Delta T_{sys/j}^{res}$ the average time to reset system after failure in which jth component was critical (for being up), N_j^{crit} the average number of critical repairs of component j per mission, N_j the average number of repairs of component j per mission and the importances I_j^B defined by Eqs.(2) and (3) would result

Markovian system is that the system evolution after a given time (t) depends on its state at t, not on its past. This is not the case in important instances, for instance when aging components are present (as those characterized by Weibull distributions), or the repair distribution of a component is a Gaussian one. In these situations, we need to associate to each of these aging components, or processes, an individual aging time. Writing a differential equation like (A.1) is impossible. A way out of this this difficulty, if a reference equation over which basing a simulation model is required, is that of introducing a new quantity, the so called "state collision density" $\psi_i(t)$, defined as the number of times the system enters into state i per unit time. This density results governed by the set of integral, Volterra type equation[8]

$$\psi_i(t) = \sum_{\substack{j=1 \\ j\neq i}}^{N} \int_0^t \psi_j(t') \, R_j(t-t') \, \alpha_{ij}(t-t') \, dt' \qquad (A.2)$$

where N is the overall number of possible states, α_{ij} represent the transition probability from state j into state i, while $R_j(t-t')$ is the probability that if the system entered state i at t' it will remain in this state up to time t, i.e.

$$R_j(t-t') = \exp\left[-\int_{t'}^{t} \gamma_j(t-x)dx\right] . \qquad \left(\gamma_j = \sum_{\substack{i=1 \\ i\neq j}}^{N} \alpha_{ji}\right) \qquad (A.3)$$

The state probabilities P_i can be now obtained easily from the expression

$$P_i(t) = \int_0^t \psi_i(t') \, R_i(t-t') \, dt' . \qquad (A.4)$$

The following obvious condition should be associated to Eq.(A.2)

$$\sum_{j=1}^{N} \int_0^t \psi_i(t') \, R_i(t-t') \, dt' = 1 . \qquad (A.5)$$

AMIR and SPAR represent system simulation codes solving above Eq.(A.2) for reliability and availability problems, respectively.

REFERENCES

1. Z.W. Birnbaum, "On the importance of different components in a multi-component system", *Multivariate Analysis II*, P.R. Krishnaiah, ed., Academic Press, 1969.
2. A. Gandini, "Importance & sensitivity analysis in assessing system reliability", IEEE Trans. on Reliability, 39, 61 (1990).
3. Yun-Fu Wu, J.D. Lewins, "Monte Carlo studies of engineering system reliability", J. of Nuclear Energy, 19, 825 (1992).
4. A. Goldfeld, A. Dubi, "Monte Carlo methods in reliability engineering", Quality and Reliability Engineering International, 3th, pp; 83-91 (1987).
5. A. Dubi and A. Goldfeld, "SPAR 1.2 - A multipurpose Monte Carlo based code for logistic analysis of multi-systems fields,"Code Manual,Malchi Sci.-Ben Gurion Univ.Contract MCU-01/1988/9 (1988).
6. A. Dubi, A. Gandini, A. Goldfeld, R. Righini, "A new multipurpose Monte Carlo method for reliability analysis of complex systems. Application to a FBR decay heat removal system", Proceed. Reliability '89 Conference, London, 14-16 June 1989, page 2B/6/1.
7. T. Inagaki and R.J. Henley, "Probabilistic evaluation of prime implicants and top-events for non-coherent systems", IEEE Trans. Reliability, vol R-29, 1980 Dec, pp 361-367.
8. A. Dubi, "Stochastic modeling of realistic systems", Tutorial notes for the annual E&M Symposium. L.A. January (1990)

SOME RESULTS IN SEMI-MARKOV RELIABILITY THEORY

Jeffery D. Lewins[1] and Yun-Fu Wu[2]

[1]Cambridge University Engineering Department,
Trumpington, Street,
Cambridge, CB2 1PZ, England, U.K.

[2] Taiwan Power Company, (Room 1706)
242, Roosevelt Road,
Sec. 3, Taipei, Taiwan, R.O.C.

INTRODUCTION

A study of system reliability involves the fluctuations due to random failure of components which may be accompanied by randomness in repair. Such components having constant age specific decay (and renewal) characteristics can be said to be Markovian and hence subject to fairly straightforward analysis, at least for small systems. When the systems are large and complex, it is found to be efficient to employ stochastic simulation, sometimes called Monte Carlo modelling[(1)]. Of course in the development of this latter approach, solutions to elementary systems by Markov modelling is a useful technique to validate Monte Carlo methods.

We have wished to undertake the extension to semi-Markovian models where the system must be specified over an extended history and not simply at an initial instant. The technique is readily extended in Monte Carlo modelling to incorporate age-specific failure rates that depend on the history of the system[(2)] and we seek therefore independent solutions of non-Markovian sample problems to validate the Monte Carlo generalization. This note provides one such solution developing the work of Malaiya and Su[(3)] to some general and specific cases.

We are concerned with components whose failure and renewal characteristics depend upon their age but not absolute time; the problem is therefore continuous in time, discontinuous in state but involves the history of the system. Nomenclature is not standard. We take the view that this is a semi-Markov system being aware

(i) that for discrete time systems, some authors will speak of a first-order Markov system if the state at only one time requires specification, second-order if two different time states are required, etc. We deal here with a continuous time, discrete state model where this classification is inappropriate, and

(ii) in queuing theory, age dependence is referred to as semi-Markov.

THEORY

Notation

i	state of the system
τ	age of the component
$\lambda(\tau)$	age-specific failure rate
$\mu(\tau)$	age-specific repair rate
$\pi_i(t,\tau)$	probability density defined in text

The theory given in this section is essentially that of Malaiya and Su with some corrections of misprints and a modification of their final equation to integral form.

Consider a component capable of being in two discrete states ('working', 'failed', 1,0 etc.), as shown by the following figure, but where changes of state occurred in time randomly according to some continuous probability distribution. A constant age-specific decay rate is the more well known example, leading to a Markov

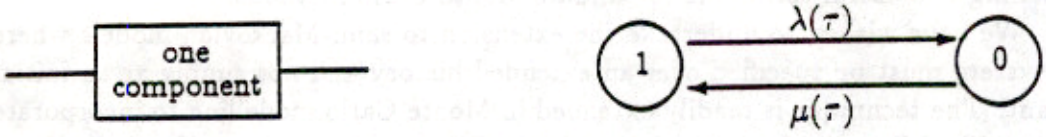


Figure 1: Transition between two states.

system, which we generalize. The failure rate $\lambda(\tau)$ is the mean rate at which the system which has been in state 1 for a period τ will change to state 0 and the repair rate $\mu(\tau)$ is the mean rate at which the system which has been in state 0 for a period τ is repaired to state 1. These mean age-specific rates are to be provided.

Let $\pi_i(t,\tau)$ be a probability density for the system in state $i(i = 1,0)$ such that

$$\pi_i(t,\tau)d\tau = P_\tau\{ \text{(system is in state } i \text{ at time epoch } t\text{)} \cap \text{(system entered state } i \text{ in } d\tau \text{ about a period } \tau \text{ earlier)} \}.$$

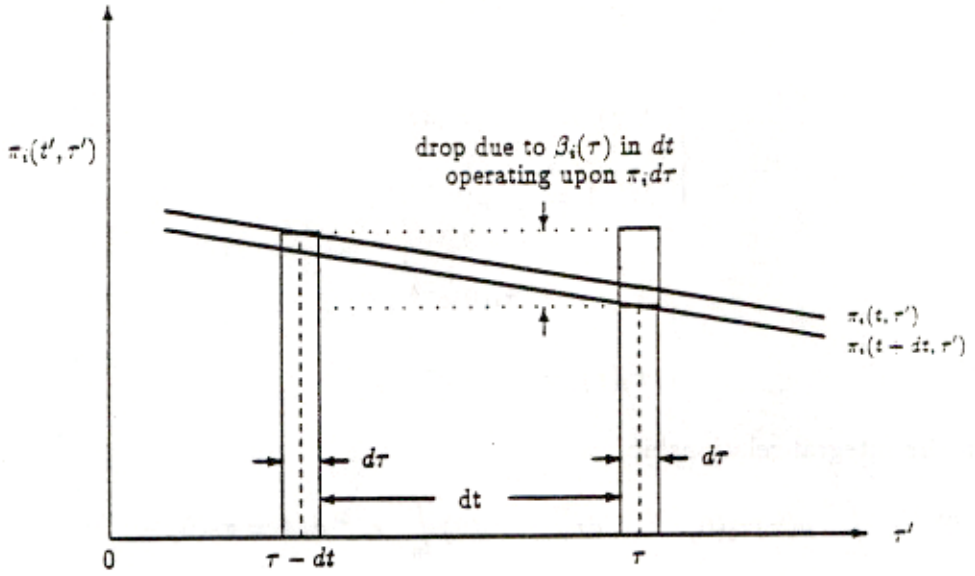


Figure 2: Derivation of equation

Referring to Figure 2, the two areas $d\tau$ wide would describe the same probability except for the opportunity to change from state i in the interval dt. Hence we have

$$\pi_i(t,\tau - dt)d\tau = \pi_i(t + dt,\tau)d\tau + \beta_i\pi_i(t,\tau)d\tau dt\ , \tag{1}$$

where

$$\beta_i = \begin{cases} \lambda, & \text{if } i = 1\ . \\ \mu, & \text{if } i = 0\ . \end{cases}$$

Considering suitable limits,

$$\frac{d\pi_i}{dt} = \frac{\partial\pi_i}{\partial t} + \frac{\partial\pi_i}{\partial\tau} = -\beta_i\pi_i\ . \tag{2}$$

We therefore have the probability $P_i(t)$ of being in state i at t to be

$$P_i(t) = \int_0^\infty \pi_i(t,\tau)d\tau\ . \tag{3}$$

Finally we have the statement that at $\tau = 0$, the pdf π_i is determined by integrating over the pdf for $i' \neq i$ over all τ:

$$\pi_i(t,0) = \int_0^\infty \beta_{i'}(\tau)\pi_{i'}(t,\tau)d\tau \ . \tag{4}$$

Malaiya and Su, having obtained this relationship, chose to differentiate it but we find this unnecessary when solutions of the system are to be obtained.

One special solution, the steady state case ($t \to \infty$) is obtained by Malaiya and Su however. We have, in that limit,

$$\frac{d\pi_i(\tau)}{d\tau} = -\beta_i(\tau)\pi_i \ .$$

Writing

$$\begin{cases} \Lambda(\tau) = \int_0^\tau \lambda(\tau')d\tau' \ , \\ M(\tau) = \int_0^\tau \mu(\tau')d\tau' \ , \end{cases} \tag{5}$$

then

$$\begin{cases} \pi_1(\tau) = \pi_1(0)e^{-\Lambda} \ , \\ \pi_0(\tau) = \pi_0(0)e^{-M} \ , \end{cases} \tag{6}$$

and from the integral relationship,

$$\pi_1(0) = \int_0^\infty \mu(\tau)\pi_0(0)e^{-M(\tau)}d\tau = \pi_0(0)\int_0^\infty e^{-M}dM = \pi_0(0) \equiv \pi(0) \ . \tag{7}$$

Since the steady state probabilities are given by

$$\begin{cases} P_{1_s} = \pi(0)\int_0^\infty e^{-\Lambda}d\tau \equiv \pi(0)\bar{\Lambda} \ , \\ P_{0_s} = \pi(0)\int_0^\infty e^{-M}d\tau \equiv \pi(0)\bar{M} \ ; \end{cases} \tag{8}$$

where

$$\begin{cases} \bar{\Lambda} = \int_0^\infty e^{-\Lambda}d\tau \ , \\ \bar{M} = \int_0^\infty e^{-M}d\tau \ ; \end{cases}$$

where $e^{-\Lambda}$ and e^{-M} are the survivor probability densities and $\bar{\Lambda}$, $\bar{M}$ are the mean times in the respective states. Since $P_1 + P_0 = 1$, we obtain, with Malaiya and Su,

$$\begin{cases} P_1 = \frac{\Lambda}{\Lambda+M} , \\ P_0 = \frac{M}{\Lambda+M} , \end{cases} \tag{9}$$

in steady state.

GENERAL SOLUTION

In view of the first-order partial differential equation statements, Lagrange's method of solution is appropriate. The auxiliary equations are

$$\begin{cases} \frac{\partial \pi_1}{\partial t} + \frac{\partial \pi_1}{\partial \tau} = -\lambda \pi_1 , & \text{giving} \\ dt = d\tau = -\frac{d\pi_1}{\lambda \pi_1} ; \end{cases} \tag{10}$$

$$\begin{cases} \frac{\partial \pi_0}{\partial t} + \frac{\partial \pi_0}{\partial \tau} = -\mu \pi_0 , & \text{giving} \\ dt = d\tau = -\frac{d\pi_0}{\mu \pi_0} ; \end{cases} \tag{11}$$

with solutions

$$\begin{cases} t - \tau = C_1 , \\ \pi_1(t,\tau) = C_2 e^{-\Lambda(\tau)} ; \end{cases} \tag{12}$$

$$\begin{cases} t - \tau = D_1 , \\ \pi_0(t,\tau) = D_2 e^{-M(\tau)} ; \end{cases} \tag{13}$$

so that general solutions are

$$\begin{cases} e^{\Lambda} \pi_1(t,\tau) = \psi(t-\tau) , \\ e^{M} \pi_0(t,\tau) = \phi(t-\tau) . \end{cases} \tag{14}$$

where ψ and ϕ are arbitrary functions. In view of the integral relationship at $\tau = 0$, we obtain convolutions

$$\pi_1(t,0) = \psi(t) = \int_0^\infty \mu(\tau)\pi_0(t,\tau)d\tau = \int_0^\infty \mu(\tau)e^{-M(\tau)}\phi(t-\tau)d\tau . \tag{15}$$

Consider the sufficiently general case that at $t = 0$ the system has just with certainty been repaired so that $\phi(t-\tau) \equiv 0$ for $\tau \geq t$ and $\psi(t-\tau) \equiv 0$ for $\tau > t$ but $\psi(t-\tau)$ contains a Dirac delta distribution at $t = \tau = 0$. The general case can be obtained as a linear combination of such cases. Then

$$\psi(t > 0) = \int_{0+}^{t} \mu(\tau)e^{-M(\tau)}\phi(t-\tau)d\tau , \tag{16}$$

but

$$\phi(t>0) \;=\; \int_{0^+}^{t} \lambda(\tau)e^{-\Lambda(\tau)}\psi(t-\tau)d\tau + \lambda(t)e^{-\Lambda(t)} \;. \tag{17}$$

In view of the convolutions, take one-sided Laplace transforms in parameter s:

$$\begin{cases} \bar{\psi}(s) \;=\; \overline{\mu e^{-M}}\,\bar{\phi}(s) \\ \bar{\phi}(s) \;=\; \overline{\lambda e^{-\Lambda}}\left[\bar{\psi}(s)+1\right] \end{cases} \tag{18}$$

and since

$$P_1(t) \;=\; \int_0^{\infty} \pi_1(t,\tau)d\tau \;=\; \int_0^{t} \pi_1(t,\tau)d\tau \;=\; \int_0^{t} e^{-\Lambda}\psi(t-\tau)d\tau + e^{-\Lambda(t)} \tag{19}$$

allowing again for the Dirac-jump in ψ at $t=0$, we have a further convolution such that

$$\bar{P}_1(s) \;=\; \frac{\overline{e^{-\Lambda}}}{1-\overline{\lambda e^{-\Lambda}}\cdot\overline{\mu e^{-M}}} \tag{20}$$

- **The Markov case**

Put λ and μ constant so that $\Lambda(\tau) \;=\; \lambda\tau, M(\tau)=\mu\tau$ and $\overline{e^{-\Lambda}} \;=\; \frac{1}{\lambda+s}, \overline{e^{-M}} \;=\; \frac{1}{\mu+s}$, and hence

$$\bar{P}_1(s) \;=\; \frac{1}{\lambda+s}\cdot\frac{1}{1-\frac{\lambda}{\lambda+s}\frac{\mu}{\mu+s}} \;=\; \frac{\mu+s}{s\left[s+\lambda+\mu\right]} \;. \tag{21}$$

Note

$$\lim_{s\to 0} s\bar{P}_1(s) \;=\; \frac{\mu}{\lambda+\mu} \;,$$

the established steady state result, and

$$\lim_{s\to\infty} s\bar{P}_1(s) \;=\; 1$$

for $P_1(0)$ as required by the $t=0$ condition. We have

$$\bar{P}_1(s) \;=\; \frac{\mu}{\lambda+\mu}\cdot\frac{1}{s} + \frac{\lambda}{\lambda+\mu}\cdot\frac{1}{s+\lambda+\mu} \;. \tag{22}$$

Therefore, we have

$$P_1(t) \;=\; \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu}e^{-(\lambda+\mu)t} \tag{23}$$

giving the expected exponential fall-off of this well-known Markov result.

- A semi-Markov case

Suppose $\lambda = \lambda_0 \tau$ and $\mu + \mu_0 \tau$, i.e., linear ageing. so that

$$\begin{cases} \Lambda(\tau) &= \frac{1}{2}\lambda_0 \tau^2 \,, \\ M(\tau) &= \frac{1}{2}\mu_0 \tau^2 \,. \end{cases} \tag{24}$$

We have

$$\overline{e^{-\Lambda(t)}} = \int_0^\infty e^{-\frac{1}{2}\lambda_0 \tau^2} e^{-st} dt = \sqrt{\frac{\pi}{2\lambda_0}} e^{\frac{s^2}{2\lambda_0}} \, erfc\left(\frac{s}{\sqrt{2\lambda_0}}\right) , \tag{25}$$

$$\overline{\lambda_0 t e^{-\Lambda(t)}} = 1 - \sqrt{\frac{\pi}{2\lambda_0}} s e^{\frac{s^2}{2\lambda_0}} erfc\left(\frac{s}{\sqrt{s\lambda_0}}\right) , \tag{26}$$

$$\overline{\mu_0 t e^{-M(t)}} = 1 - \sqrt{\frac{\pi}{2\mu_0}} s e^{\frac{s^2}{2\lambda_0}} erfc\left(\frac{s}{\sqrt{2\mu_0}}\right) , \tag{27}$$

so that

$$\bar{P}_1(s) = \frac{\sqrt{\frac{\pi}{2\lambda_0}} e^{\frac{s^2}{2\lambda_0}} erfc\left(\frac{s}{\sqrt{2\lambda_0}}\right)}{1 - \left[1 - s\sqrt{\frac{\pi}{2\lambda_0}} e^{\frac{s^2}{2\lambda_0}} erfc\left(\frac{s}{\sqrt{2\lambda_0}}\right)\right]\left[1 - s\sqrt{\frac{\pi}{2\mu_0}} e^{\frac{s^2}{2\mu_0}} erfc\left(\frac{s}{\sqrt{2\mu_0}}\right)\right]} \tag{28}$$

To see the behaviour more readily, we specialize to $\lambda_0 = \mu_0$ and without loss of generality chose $\lambda_0 = \frac{1}{2}$. Then

$$\bar{P}_1(s) \to \frac{\sqrt{\pi} e^{s^2} erfc(s)}{1 - [1 - s\sqrt{\pi} e^{s^2} erfc(s)]^2} = \frac{1}{s\,[2 - s\sqrt{\pi} e^{s^2} erfc(s)]} . \tag{29}$$

Then

$$\lim_{s \to 0} s\bar{P}_1(s) = \frac{1}{2}$$

as expected for $t \to \infty$ in this symmetric case, and

$$\lim_{s \to \infty} s\bar{P}_1(s) = 1$$

using the asymptotic expansion of $erfc(s)$, i.e.,

$$erfc(s) \to \frac{e^{-s^2}}{s\sqrt{\pi}} \left(1 - \frac{1}{2 \cdot s^2} + \frac{1 \cdot 3}{2^2 \cdot s^4} - \frac{1 \cdot 3 \cdot 5}{2^3 \cdot s^6} + \cdots\right) . \tag{30}$$

We seek a power series expansion in $\left(\frac{1}{s}\right)$ as $s \to \infty$ to invert $\bar{P}_1(s)$ and have

$$\lim_{s\to\infty} \bar{P}_1(s) \to \frac{1}{s}\frac{1}{2 - 1 + \frac{1}{2s^2} - \frac{1\cdot 3}{2^2 s^4} + \frac{1\cdot 3\cdot 5}{2^3 s^6} - \cdots}$$

$$\equiv \frac{1}{s}\frac{1}{1 + \sum_1^\infty \frac{a_n}{s^{2n}}}$$

$$\equiv \frac{1}{s}\left[1 + \sum_1^\infty \frac{b_n}{s^{2n}}\right]$$

where the coefficients a_n are known and we want to find the b_n. Clearly

$$\left[1 + \sum_1^\infty a_n \left(\frac{1}{s}\right)^{2n}\right]\left[1 + \sum_1^\infty b_n \left(\frac{1}{2}\right)^{2n}\right] \equiv 1\,, \tag{31}$$

n	:	0	2	4	6	8	10
a_n	:	1	$+\frac{1}{2}$	$-\frac{3}{4}$	$+\frac{15}{8}$	$-\frac{105}{16}$	$+\frac{945}{32}$
b_n	:	1	$-\frac{1}{2}$	$+1$	$-\frac{11}{4}$	$+\frac{154}{16}$	$-\frac{665}{16}$

Table 1: Series expansion coefficients.

so that coefficients can be matched. Explicitly after $a_0 = b_0 = 1$, we have all odd a_n and hence b_n are zero. Indeed this can be developed to a recurrence relation involving the appropriate coefficients of a multinominal expansion to each term so that we have further first 10 terms as in Table 1. We then have

$$P_1(t) = \sum_0^\infty \frac{b_n t^n}{n!} \tag{32}$$

although this is a slowly converging series. The coefficients, b_n, may readily be computed from Equation (31). We found that 40 non-zero terms ($n = 80$) were necessary to provide convergence before the steady state value was reached.

- **General case $\lambda_0 \neq \mu_0$**

$$\bar{P}_1(s) = \frac{\sqrt{\pi} 2\lambda_0 e^{\frac{s^2}{2\lambda_0}} erfc\left(\frac{s}{\sqrt{2\lambda_0}}\right)}{1 - \left[1 - s\sqrt{\frac{\pi}{2\lambda_0}} erfc\left(\frac{s}{\sqrt{2\lambda_0}}\right)\right]\left[1 - s\sqrt{\frac{\pi}{2\mu_0}} e^{\frac{s^2}{2\mu_0}} erfc\left(\frac{s}{\sqrt{2\mu_0}}\right)\right]}\,. \tag{33}$$

$$\lim_{s\to\infty} \bar{P}_1\left(\frac{1}{s}\right) \to \frac{\frac{1}{s}\left[1 - \frac{1}{2\left(\frac{s^2}{2\lambda_0}\right)} + \frac{1\cdot 3}{2^2\left(\frac{s^2}{2\lambda_0}\right)^2} - \frac{1\cdot 3\cdot 5}{2^3\left(\frac{s^2}{2\lambda_0}\right)^3} + \cdots\right]}{1 - \left[\frac{1}{2\left(\frac{s^2}{2\lambda_0}\right)} - \frac{1\cdot 3}{2^2\left(\frac{s^2}{2\lambda_0}\right)^2} + \frac{1\cdot 3\cdot 5}{2^3\left(\frac{s^2}{2\lambda_0}\right)^3} - \cdots\right]} \times$$

$$\frac{1}{\left[\frac{1}{2\left(\frac{s^2}{2\mu_0}\right)} - \frac{1\cdot 3}{2^2\left(\frac{s^2}{2\mu_0}\right)^2} + \frac{1\cdot 3\cdot 5}{2^3\left(\frac{s^2}{2\mu_0}\right)^3} - \cdots\right]},$$

$$= \frac{\frac{1}{s}\left[1 - \frac{\lambda_0}{s^2} + \frac{1\cdot 3\cdot \lambda_0^2}{s^4} - \frac{1\cdot 3\cdot 5\cdot \lambda_0^3}{s^6} + \cdots\right]}{1 - \left[\frac{\lambda_0}{s^2} - \frac{1\cdot 3\cdot \lambda_0^2}{s^4} + \cdots\right]\left[\frac{\mu_0}{s^2} - \frac{1\cdot 3\cdot \mu_0^2}{s^4} + \cdots\right]} . \tag{34}$$

We seek coefficients d_n where a_n, b_n, c_n are all known, from

$$\sum_0^\infty d_n s^{-n} \equiv \frac{\sum_0^\infty a_n s^{-n}}{1 - \left[\sum_0^\infty b_n s^{-n}\right]\left[\sum_0^\infty b_n s^{-n}\right]} \tag{35}$$

where $a_0 = 1$, $b_0 =)$, and $d_0 = 1$ but all odd coefficients of d_n are zero. Then

$$P_1(t) \;=\; \sum_0^\infty \frac{d_n}{n!} t^n \; . \tag{36}$$

The coefficients, d_n, may again be readily programmed.

MULTIPLE STATES

If the system has more than two states but remains a continuous time system, with the transition from one state to another being dependent upon the time the system has been in that state, the model can be extended.

Let $\lambda_{ij}(\tau)$ be the mean rate of transition from state i to j, $j \neq i$ after a period τ in state i. From the previous discussion for the pdf $\pi_i(t,\tau)$ in state i, we have

$$\frac{\partial \pi_i(t,\tau)}{\partial t} + \frac{\partial \pi_i(t,\tau)}{\partial \tau} \;=\; -\pi_i(t,\tau)\sum_{j\neq i}\lambda_{ij} \;=\; -\lambda_i \pi_i(t,\tau);\;\; \tau > 0 \tag{37}$$

if we define $\lambda_i \;=\; \Sigma_{j\neq i}\lambda_{ij}$. In addition, the transfer into state i at $\tau = 0$ is given by

$$\pi_i(t,0) \;=\; \sum_{j\neq i}\int_0^\infty \lambda_{ji}(\tau)\pi_j(t,\tau)d\tau \; .$$

In steady state

$$\frac{d\pi_i}{d\tau} \;=\; -\lambda_i(\tau)\;;\;\; \pi_i(\tau) = \pi_i(0)e^{-\int_0^\tau \lambda_i(\tau')d\tau'} \equiv \pi_i(0)e^{-\Lambda_i(\tau)} \; , \tag{38}$$

so that we have a set of equations

$$\pi_i(0) = \sum_{j\neq i} \pi_j(0) \int_0^\infty -\lambda_{ji}(\tau) e^{-\int_0^\tau \lambda_j(\tau')d\tau'} d\tau$$

$$\equiv \sum_{j\neq i} \pi_j(0) \int_0^\infty -\lambda_{ji}(\tau) e^{-\Lambda_j(\tau)} d\tau \ , \tag{39}$$

or

$$\pi_i(0) \equiv \sum_{\neq i} \tau_j(0) \bar{\Lambda}_{ji} \ . \tag{40}$$

These are of algebraic form and can be solved for the $\pi_i(0)$ to within a single constant. We then have

$$P_i = \int_0^\infty \pi_i(\tau) d\tau = \pi_i(0) \int_0^\infty e^{-\Lambda_i(\tau)} d\tau \ , \tag{41}$$

together with $\Sigma_i P_i = 1$ to determine the constant.

For the transient problem, we can, as before, assume that the system has just been repaired into state 1 which is thus associated with a Dirac-delta distribution. Then using Lagrange method with $\pi_i(t,\tau) = e^{-\Lambda_i(\tau)}\psi_i(t-\tau)$ as before we have

$$\psi_1(t>0) = \sum_{j\neq 1} \psi_j(t) \int_{0+}^t \lambda_{j1}(\tau) e^{-\Lambda_j} d\tau \ , \tag{42}$$

but for $i \neq 1$

$$\psi_i(t>0) = \sum_{j\neq 1} \psi_j(t) \int_{0+}^t \lambda_{ji}(\tau) e^{-\Lambda_j} d\tau + \lambda_{1i}(t) e^{-\Lambda_1(t)} \ . \tag{43}$$

These convolutions can again be expressed in the Laplace transform space as

$$\begin{cases} \bar{\psi}_1(s) = \sum_{j\neq 1} \bar{\psi}_j(s) \overline{\lambda_{j1} e^{-\Lambda_j}} \ , \ \text{and} \\ \bar{\psi}_{i\neq 1}(s) = \sum_{j\neq 1} \bar{\psi}_j(s) \overline{\lambda_{ji} e^{-\Lambda_j}} + \overline{\lambda_{1i} e^{-\Lambda_1}} \end{cases} \tag{44}$$

from which we can seek inversions by, for example, a series expansion as before. Finally we have

$$\begin{cases} \bar{P}_1(s) = \bar{\psi}_1(s) \overline{e^{-\Lambda_1}} + \overline{e^{-\Lambda_1}} \\ \bar{P}_{i\neq 1}(s) = \bar{\psi}_1(s) \overline{e^{-\Lambda_i}} \end{cases} \tag{45}$$

and the system stochastics can be determined as before.

CONCLUSIONS

Figure 3 shows the computed probability $P_1(t)$ up to $t/\sqrt{2\lambda_0} = 8$ for the special case of the two-state linear aging system having $\lambda_0 = \mu_0$ with the failure of convergence shown as a function of terms taken in the power series. A significant feature of the converged result is the oscillatory approach to the steady state value, notably different from the Markov result with its monotonic approach. In addition, the initial behaviour is flat [corresponding to $\lambda(0) = \mu(0) = 0$].

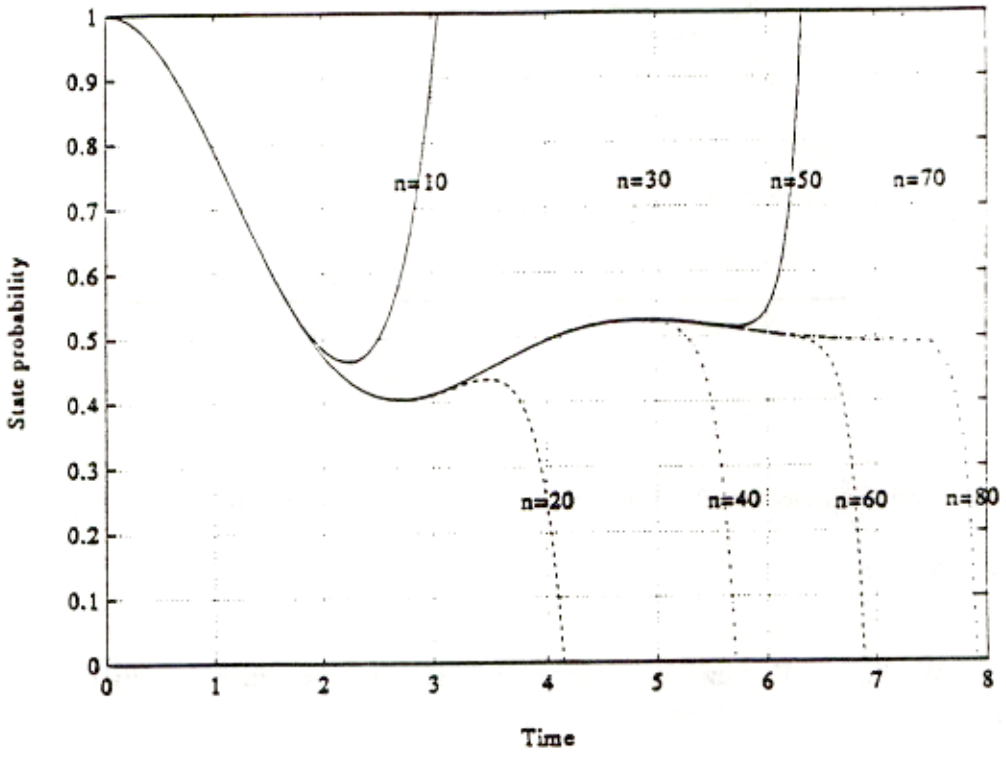


Figure 3: The aging non-Markov results ($\lambda_o = \mu_o$) with 10-80 terms; showing successive failure of convergence of the power series.

We also solve this problem by Monte Carlo. Since the motivation for this work was to validate a stochastic simulation, the results, where the Monte Carlo curve (as shown in Figure 4) is essentially indistinguishable, cannot therefore be offered as a validation of our analytic solution but nevertheless provides a satisfactory conclusion to the project.

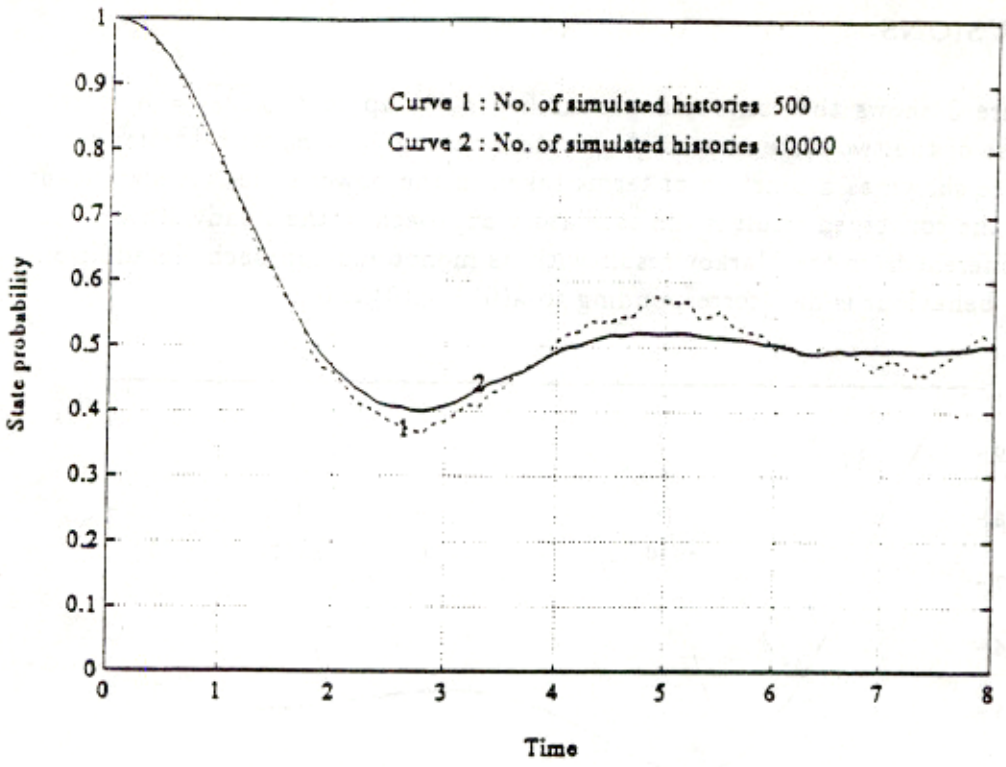


Figure 4: Monte Carlo simulation results under various simulated histories.

REFERENCES

1. Y.-F Wu and J. D. Lewins, "Monte Carlo studies of engineering system reliability", *Annals of Nuclear Energy*, (1992).

2. Y.-F. Wu and J. D. Lewins, "Monte Carlo studies of system reliability in non-Markovian system", *Proceedings of International Reliability Availability Maintainability Quality Conference for the Power Industry*: Philadelphia, Pennsylvania, USA (1992).

3. Y. K. Malaiya and S. Y. H. Su, "Analysis of an important class of non-Markov systems", *IEEE Trans. Reliability*, R-31: 64-67 (1982). *Energy*, 19: 825 (1992).

VARIANCE REDUCTION TECHNIQUES FOR DYNAMIC PROBABILISTIC RISK ASSESSMENT

Nathan O. Siu, Dana L. Kelly, and John A. Schroeder

Idaho National Engineering Laboratory
P.O. Box 1625
Idaho Falls, ID 83415
USA

ABSTRACT

Sensitivity analysis is potentially useful for improving discrete event simulation analyses of dynamic process system reliability because it aids the development of variance reduction techniques that acknowledge process dynamics. This paper discusses strategies for using sensitivity analysis in variance reduction efforts, and presents results obtained from early implementation of these strategies.

INTRODUCTION

Variance reduction techniques (VRTs) are used in a variety of areas to improve the efficiency of Monte Carlo simulation. In neutron transport applications, for example, such techniques as splitting and Russian Roulette are employed to emphasize important regions for sampling while de-emphasizing less important regions. In other applications, such VRTs as antithetic variable sampling, conditional sampling, and stratified sampling all have their uses.[1] One general result from the considerable amount of work done on VRTs to date is that VRTs are quite problem-specific: in extreme cases, a VRT actually can lead to worse results than would be obtained if no VRT were employed at all, that is, if crude Monte Carlo sampling were employed.

The key characteristic that separates risk (and reliability) assessment sampling problems from most other Monte Carlo applications is that a risk assessment is concerned with very rare events. A typical demand failure rate might be on the order of 10^{-3} or less per demand. Without an appropriate VRT, most sampling trials will result in the uninteresting (from the risk analyst's standpoint) result that no failures have occurred. Such techniques as forcing transitions,[2,3] boosting failure rates,[4] and biasing towards failures[2,3,5] have been suggested to combat this problem.

A second risk assessment characteristic that should affect the sampling process is that the accident scenarios with the largest contribution to risk (the "dominant scenarios") often involve multiple, dependent failures of equipment. Typical sources of dependency between equipment include common support systems (e.g., power supplies) and common environments. A particularly important source of dependency is provided by control systems and operators; planned actions by either of those during the course of an accident can, in some situations, lead to undesired plant responses and configurations.

The problem with the specific VRTs mentioned above is that they are focused only on component and system hardware states. Thus, they do not modify the Monte Carlo sampling scheme to account for other parameters that can increase the dependency between failure events (e.g., process variables, control system setpoints, operating procedures) in a dynamic accident scenario. One recent observation is that these VRTs can easily overemphasize (i.e., over-sample) unimportant failures, and effectively mask scenarios of greater interest[4,5]. Additional results indicate that, the masking problem aside, these VRTs need to be more efficient in reducing sampling uncertainty.

This paper explores the extent to which sensitivity analysis techniques can be used to develop improved VRTs for discrete event simulation.* These techniques provide information concerning process dynamics that should be helpful in determining (in the context of the scenario being analyzed) if the sampling scheme employed is likely to obtain interesting results. Strategies for employing sensitivity analysis are described and demonstration results obtained from an early implementation of these strategies is presented.

APPROACH

The general approach for employing sensitivity analysis in developing improved VRTs is a simple one. As shown in Figure 1, the random walk associated with a particular Monte Carlo trial describes a trajectory in phase space. Ordinarily, most trajectories will not intersect with the undesired absorbing region, due to the rarity of failure events. The objective is to bias the sampling process to artificially increase the number of "hits" in the absorbing region; the role of sensitivity analysis is to provide dynamic process information (e.g., time-dependent temperature and pressure) that can be used to affect the biasing. (In other words, sensitivity analysis can be used to develop an improved importance sampling scheme.)

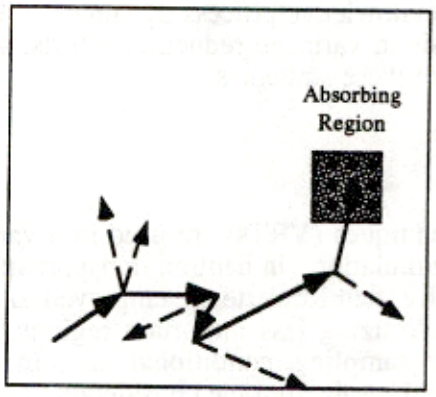


Figure 1. Simulation trajectories in phase space.

Sensitivity Analysis

Given a set of n nonlinear, first-order differential equations,

$$\dot{y} = f(y,t|\alpha) \tag{1}$$

where α is a vector of parameters, sensitivity analysis can be used to compute the sensitivity coefficients

* Discrete event simulation is a particular form of Monte Carlo simulation in which interactions between processes are mediated through the use of a central event calendar.[1] This work employs an object-oriented approach to discrete event simulation. Each system object is modeled separately; the overall system state is defined implicitly by the different object states and the status of any system state variables (e.g., continuous process variables). This object oriented approach allows a relatively direct treatment of complex systems, although it can be less computationally efficient than more system-based simulation approaches (e.g., as described by Lewis and Bohm[2]).

$$z_{j,k}^{(i)} \equiv \frac{\partial^{(i)} y_k}{\partial \alpha_j^{(i)}} \qquad (2)$$

of the dependent variables with respect to the parameters α.

Various methods can be used to obtain the sensitivity coefficients, with most methods focusing on the linear (i.e., first-order) coefficients. Some methods, commonly applied to simpler systems, directly attack the governing system of equations. Examples in this class are the direct method, which differentiates the given system with respect to the input parameters to generate an augmented set of $2n$ equations which can then be solved for $\mathbf{y}$ and $\mathbf{z}_\alpha$; the adjoint method, which solves the adjoint system of equations; and integral methods (e.g., Green's function method) which transform the set of n differential equations into an integral equation which is then solved. For larger, more complex problems, subjective screening ("expert opinion") and subsequent numerical analysis is a commonly employed method, as are regression-based techniques. Both methods are useful for systems in which a description in terms of a set of differential equations is difficult or practically impossible. Methods that deal directly with the governing equations have advantages over subjective screening in that expert bias does not affect the results, but they can be computationally intensive, especially when used in an iterative mode. Further, they do require an explicit formulation of the governing set of equations. Regression-based methods may be impractical if there are many parameters that can affect the system. Thus, in many realistically complex cases, subjective screening is unavoidable.

The coefficients derived from sensitivity analysis are useful in two ways. First, they indicate the relative importance of model parameters generally not considered in VRTs for risk assessment simulations. Second, they can be used to project system trajectories in phase space. These projections can then be used to determine which of a number of different possible trajectories will most closely approach the absorbing region, and the sampling scheme can be biased to favor that trajectory, as discussed below.

Strategies for Employing Sensitivity Analysis in VRT Development

In discrete event simulation, sampling is performed to decide: a) which of a set of alternative paths should be followed, and b) when the next event should be scheduled in the event calendar. Sampling can be performed when an event is being executed (it has been "triggered"). Event triggering can occur because the event was scheduled or because the system state satisfies user-specified criteria (opportunistic triggering).

It can be seen that these two types of decisions provide us with a means to influence the development of a scenario. We would like to exercise these controls to "steer" the simulation towards the undesired region (see Figure 1). (Of course, the weight associated with a given trial will be modified to reflect any biasing that we introduce into the sampling process.) Using the notion that sensitivity analysis will allow projection of potential phase space trajectories, different strategies for employing simulation analysis can be defined. These strategies are distinguished by their measure of distance (used to determine how close a given trajectory will approach the undesired region) and by the number of possible trajectory changes (due to triggered events) they will accommodate in the projection.

Distance from the undesired region can be measured in two ways: "Euclidean distance" and "probabilistic distance." The former is defined as the root-mean-square distance in phase space from the current position to the closest point of the undesired region. The latter is defined as the likelihood that the simulation trajectory will eventually end in an absorbing region. Naturally, the probabilistic distance will not be known in most cases (else the simulation analysis is not needed). However, heuristic methods to estimate probabilistic distance can be developed. (Note that a formalization of these heuristics can lead to the identification of key variables that can then be incorporated explicitly into the definition of phase space. This would allow the incorporation of probabilistic distance measures in the Euclidean framework.)

Sensitivity analysis, by itself, can be used to project the current trajectory of the simulation in phase space. However, more accurate projections of the eventual outcome of a trial may be possible if knowledge concerning the possibility of future potential trajectory changes (events) is incorporated into the analysis. For example, if the system is heading

towards a particular setpoint, knowledge of actions that can be triggered upon reaching the setpoint (and the trajectories resulting from those actions) might be useful in steering the simulation. Thus, steering strategies can be distinguished by the number of potential future events included in the projection. "Zero branching" strategies base steering decisions only on the trajectories provided by sensitivity analysis; the possibility of future branchings and their effect on progress towards absorbing regions is not treated. "Single branching" strategies allow for one branching (after the branching currently being considered). "N-branching" includes the effects of N branches in the steering scheme.

Note that Smidts and Devooght[2] employ limited process variable information in their forced transition scheme; the reference time window (in which the failure event must occur) is based on the estimated time for the simulation to reach an absorbing region (either success or failure). The strategies described above represent generalizations of this approach.

TEST PROBLEM

To provide a simple demonstration of how the preceding ideas can be implemented, we work on the storage tank problem ("Case A") introduced by Aldemir[6] and modified by Deoss and Siu[7]. Two pumps (each with flow rate ℓ) provide input to the tank; outflow is through a single valve (with flow rate of ℓ). The tank control laws are given in Table 1. Tank overflow occurs when the tank level is higher than setpoint b ($b \geq \alpha_2$); tank dryout occurs when the tank level is lower than setpoint a ($a \leq \alpha_1$). Unlike Deoss and Siu[7], demand failures are treated in addition to runtime failures; the failure rates used (the values are chosen somewhat arbitrarily) are listed in Table 2. Repairs of failed equipment are not considered.

Table 1. Control laws for sample tank problem.

Tank Level	Pump 1	Pump 2	Valve
$L \leq \alpha_1$	On	On	Closed
$\alpha_1 < L < \alpha_2$	On	Off	Open
$L \geq \alpha_2$	Off	Off	Open

Table 2. Component failure rates for sample tank problem.

Component	Demand (/d)	Runtime (/hr)
Pump 1	1.0E-2	5.0E-4
Pump 2	1.0E-2	5.0E-4
Valve	1.0E-2	5.0E-4

In this problem, all trajectories will lead to failure (either overflow or dryout). We arbitrarily focus on estimating the likelihood of overflow, in order to test the ability of any VRTs developed to emphasize one path over another. We also focus on the very early portion of the scenario (from 0 to 100 hours) to reduce the likelihood of system failure (and thereby increase the potential benefit of the VRT).

The VRT used is a simple, intuitive one that can be seen to fall in the (Euclidean distance, zero branching) category. This VRT boosts demand failure rates (by a factor of 10) in order to favor rising level trajectories. For example, if the tank level reaches the upper level of the control region (α_2) from below, any running pumps are supposed to stop. Biasing for positive dL/dt means biasing for failures to stop (by boosting the pump demand failure rates). To compensate for the biasing, the trial weight is modified to account for the degree of boosting and the sampling outcome (component success or failure)[2-4].

To investigate the success of the variance reduction scheme for the test problem, two sets of calculations are performed. Each set involves 10 runs with 1000 sampling trials per run. Denoting the run-specific estimated probability of overflow at 100 hours by P_o, the sample means and standard deviations for P_o are given in Table 3. Histograms for P_o are shown in Figure 2.

Table 3. Summary statistics for base case and variance reduction case.

	Base Case	WIth Variance Reduction
Number of runs	10	10
Trials per run	1000	1000
$E[P_O]$	5.5E-3	5.0E-3
$SD[P_O]$	3.1E-3	1.4E-3

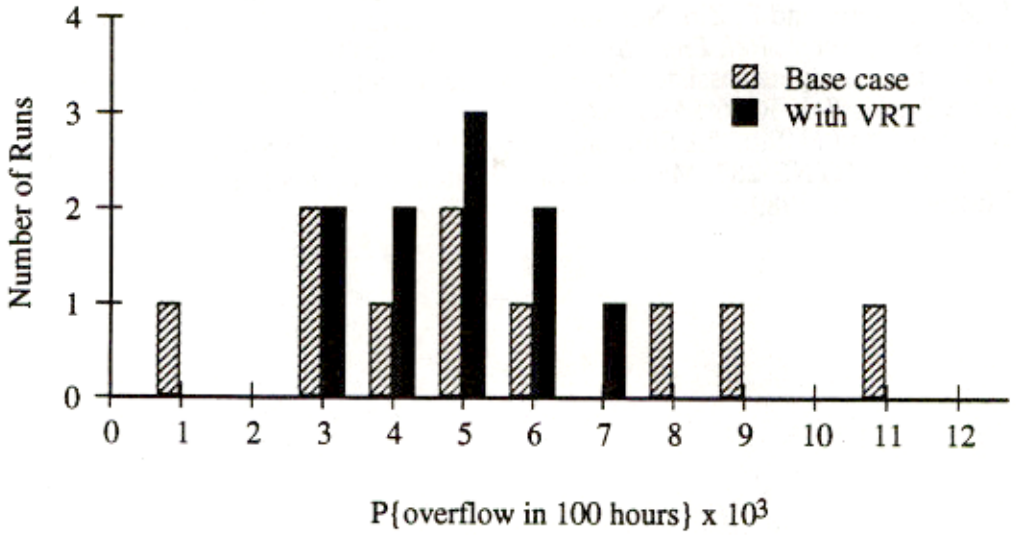


Figure 2. Empirical histogram for probability of overflow at 100 hours.

Although the number of runs is limited for both cases, both Table 3 and Figure 2 appear to indicate that the VRT is successful for the given problem. Additional runs should be useful to confirm this result, and to identify the conditions for which this VRT is of greatest usefulness.

CONCLUDING REMARKS

The simple sensitivity-based variance reduction technique (VRT) appears to useful for improving the computational efficiency of the dynamic process system simulation investigated. The efficiency of the VRT, of course, depends on the characteristics of the problem being simulated. In the test problem, lower demand failure rates or higher runtime failure rates will tend to de-emphasize the importance of demand failures, thereby reducing the usefulness of the VRT. More work is needed to more formally characterize problems for which the VRT will be beneficial.

More importantly, additional work is needed to: a) implement the general strategies for using sensitivity analysis discussed earlier in this paper, and b) to broaden the investigation to treat more realistic systems (e.g., including complex controllers). Current efforts are aimed at achieving these two objectives.

ACKNOWLEDGMENTS

Work supported through the EG&G Idaho Laboratory Directed Research and Development Program under DOE Idaho Field Office Contract DE-AC07-76ID01570. The assistance of V. Dang in developing and supporting the simulation software used in the test problem is gratefully acknowledged.

REFERENCES

1. P. Bratley, B.L. Fox, and L.E. Schrage. "A Guide to Simulation," Wiley, New York (1981).
2. E.E. Lewis and F. Böhm, Monte Carlo simulation of Markov unreliability models, *Nuc. Engr. Des.* 77:49(1984).
3. C. Smidts and J. Devooght, Probabilistic reactor dynamics - II: a Monte Carlo study of a fast reactor transient," *Nuc. Sci. Engr.* 111:241(1992)
4. V. Dang. "Improved Methods for Simulation-Based Risk Assessment," S.M. Thesis, Massachusetts Institute of Technology, Cambridge, Massachusetts, 1991.
5. M. Marseguerra and E. Zio, Non-linear Monte Carlo reliability analysis with biasing towards top event, *Rel. Engr. Sys. Safety*, 40:31(1993).
6. T. Aldemir, Computer-assisted Markov failure modeling of process control systems, *IEEE Trans. Rel.*, R-36:133(1987).
7. D.L. Deoss and N. Siu. "A Simulation Model for Dynamic System Availability Analysis," MITNE-287, Massachusetts Institute of Technology, Cambridge, Massachusetts, 1989.

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

Chair: O. Svenson, Stockholm U.

Self-Reported Human Errors in Control Room Work

L. Jacobsson, O. Svenson (Stockholm U., Sweden)

Development of an Orientation Based Approach to Evaluation of Process Operators' Expertise

L. Norros, K. Hukki (Technical Res. Ctr. Finland)

Decision Making under Uncertainty: A Pilot Study on Exemption from Technical Specifications

K. Porn (Studsvik Eco & Safety, Sweden)

SELF-REPORTED HUMAN ERRORS IN CONTROL ROOM WORK

Lena Jacobsson* and Ola Svenson

Nuclear Safety, Risk Analysis and Decision Research Unit, Department of Psychology, Stockholm University, S-106 91 STOCKHOLM, SWEDEN
* and PTM Vattenfall AB, Safety and Technology, S-162 87 VALLINGBY, SWEDEN

INTRODUCTION

Human errors occur in everyday life and have recently been given considerable attention within psychological research (e.g. Reason & Mycielska, 1982; Reason, 1990; Broadbent, Cooper, FitzGerald and Parkes, 1982; Harris & Morris, 1984). Most everyday errors are associated with little or no negative consequences since people are able to compensate for them. However, when humans control complex technological systems such as an aeroplane or a nuclear power plant the consequences of human errors can be disastrous. In industrial accidents human errors have been identified as an important contributing factor (e.g. Perrow, 1984; INPO, 1985; Miller & Swain, 1987). This is one of the reasons why researchers have paid increasing attention to human errors in technical systems (e.g. NUREG-1154, 1985). Another reason for a focus on human errors is that errors provide information important for basic research about fundamental psychological processes (Harris & Morris, 1984; Reason et. al., 1982; Reason, 1990; Woods, 1982).

Self-report questionnaires and diaries have been used frequently in studies of human error in applied settings (Harris & Morris, 1984; Reason et. al., 1982; Reason, 1990). Most of the recent studies have been either carried out in everyday life situations or have been performed in laboratories. Some single case studies have been performed on accident reports (Reason et. al., 1982; Reason, 1990; Woods,1982). The databases for accidents is restricted, although some attemps have been made to identify causes of accidents using epidemiological data of occupational accidents (Feyer & Williamson, 1991). Some recent studies adressing human error in nuclear power plants have studied errors in simulator training (e.g. Norros & Sammatti, 1986; EPRI NP-6937). Few published studies have adressed human error and working conditions in nuclear power systems in real work situations (e.g. Jacobsson & Svenson, 1991).

Different ways of classifying errors

A widely used system for categorization of errors uses the three categories of slips, mistakes (Norman, 1981) and violations (Reason, 1990). Slips are actions not in accordance with the actors' intention, the result of an adequate plan but poor execution. Mistakes are planning failures, when an action follows what is planned but the plan is inadequate. Violations are the breaking of rules or regulations such as not following procedures. Svenson (1992) also introduced a fourth category; judgment, problem solving and decision errors. Such errors are embedded in an adequate plan and lead to errors in the implementation of the plan.

Self-report error questionnaires

Several reliable self-report questionnaires on memory performance in everyday-life situations have been developed (e.g. Herrman, 1983). Memory failures over a six month period were investigated by Broadbent et. al. (1982) in the CFQ questionnaire. CFQ measures a general liability to failure and two types of failures can be distinguished, social failures and cognitive failures. A high rate of cognitive failures could be related to higher ratings of psychosomatic symptoms. The error proneness questionnnaire developed by Reason et. al. (1982) adresses slips and lapses in everyday life. A high occurrence of slips was identified in the execution of highly automatized tasks in familiar surroundings and subjects were frequently distracted when the slip occurred.

PURPOSE

Most human errors in a process industry are minor errors and do not lead to serious consequences. However, serious errors can be related to the population of everyday errors of different categories that everybody makes - including operators in a process industry. For example, British civil aircraft accidents were investigated by Reason (1982) and he revealed a number of instances of major pilot errors involving minor errors such as slips of action. An analysis of all errors made in the interaction with a technical system will thus be important in identification of risk situations in nuclear power plants. The goals of the present study was to explore the extent to which self-reported errors in a process industry setting could be (1) collected in a meaningful way and (2) classified in categories used in contemporary psychological research (Norman, 1981; Reason, 1990). Furthermore the goal was to investigate (3) the distribution over categories of errors related to method (retrospective questionnaire and diary reports) and (4) the distribution of errors over categories related to operational states of the industry (normal production and annual outage in a nuclear power plant).

METHOD

Subjects

A total of 127 control room operators from two nuclear units participated in the study (122 men, 5 women). The average age was 34 years (SD=9.0). The participants had worked for an average of 6.6 years (SD=5.1) at the plant. A large majority (72%) had a college exam or more theoretical education. The participants were asked to report about working conditions and their own errors using two different instruments (a questionnaire and a diary) during two different work periods in a nuclear power plant (annual outage and normal, steady-state operation). The annual outage was expected to be a work period with high workload and normal operation a period with lower workload.

The questionnaire

Two questionnaires were distributed to the operators containing questions about work organization, working conditions, workload and frequency of errors. One questionnaire adressed annual outage and was distributed to the operators at the end of the annual outage work period. The other questionnaire concerned normal operation and was distributed to the operators during normal operation after the annual outage. There were four questions specifically devoted to errors attributed to the operators themselves. The questions were (1) "I misinterpreted a situation and therefore I made an error", (mistake); (2) "I was not attentive enough and therefore I missed some important information", (slip); (3) "I could not remember essential information when performing an operation and therefore I had to ask for the information again", (slip); (4) "I had to deviate from the procedure in order to be able to perform an operation", (violation). Each question was answered on a scale ranging from 1= "never" through 2="at rare occasions", 3="sometimes", 4="at several occasions" to

The risk of making serious errors at work

Two questions concerned the risk of making serious errors at work during annual outage as well as normal operation. These questions were answered for both operational conditions at the same occasion, after the annual outage. The questions was answered on a scale ranging from 1="hardly no risk at all", through 2="small risk", 3=" great risk" to 4="very great risk".

The diary

In contrast to the questionnaire asking questions about a longer time period, the diary questions concerned only one day at a time. Questions were asked about working conditions, workload, mood and frequency of errors during one work shift. The diary questions were answered by the operators before the annual outage and at 1-4 times during the outage period (depending on the number of shifts each operator worked during the annual outage) and at one shift after the outage period. The diary was answered at the end of the days work shift. In all there were 4 questions referring to errors attributed to the operators themselves. They were the following (1) "forgot to change the indicator of component status in the process chart", (2) "promised to return to someone with information but forgot to do so", (3) "was unable to remember something which I knew I am familiar with and (4) "forgot to perform an operation in a sequence of operations that I planned to carry through". In addition, two questions specifically attributed the error to someone else; (5) "forgot what to do because someone disturbed me" and (6) "was forced to interrupt a surveillance operation or control task because I was disturbed by someone and forgot to return to what I was busy doing". Each of the diary questions was answered on a scale, 1="never", 2="infrequently" (one time), 3="sometimes" (2-3 times), 4="frequently" (3-4 times) and 5="very often, more than 4 times". Relating this to the questionnaire the slips are in focus in the diary while they only represents half of the questions in the questionnaire.

RESULTS

The questionnaire

Table 1 provides response frequencies and means for the 4 questions. The left two columns report the number of operators who have indicated some error (steps 2-5 on the scale). First, in accordance with previous research operators make errors just as people in general do (Reason et. al., 1982). Second, the number of operators who report some kind of error varies between 30 and 65% depending on the type of error.

In the next two columns the mean responses across operators in each condition indicates rather small differences across the conditions. A significant difference ($p<0.02$) was found for question (1) concerning how often the operators had misinterpreted a situation and therefore made an error. In the normal condition this was reported to occur more often than in the outage condition. There was also a difference (non-significant, $p<0.10$) on question (3) concerning how often the operators forgot and had to ask again, where this error was more frequent in outage as compared to normal operation. It is interesting to note that as many as about 60% of the operators reported deviations from procedures. When responses to the same questions for the two work conditions were correlated across subjects the highest correlation was $r=0.62$ for question 4 in table 1, "I had to deviate from the procedure in order to be able to perform an operation" .

TABLE 1. Error percentages and scale values for questionnaire items. Standard deviations in parentheses. Pairwise t-tests were used for each error type and only significant t-values are reported.

	Percentage operators reporting at least one error		Mean scale values across all operators		
Error type	Normal	Outage	Normal	Outage	
1. MISTAKE- I misinterpreted a situation and therefore I made an error	42	30	1.43 (0.52) n=90	1.31 (0.48) n=123	p<0.02 t=-2.3 n=85
2. SLIP- I was not attentive enough and therefore I missed important information	44	44	1.46 (0.52) n=90	1.48 (0.58) n=124	ns
3. SLIP- I could not remember essential information when performing an operation and therefore I had to ask for information again	54	63	1.55 (0.52) n=92	1.70 (0.61) n=125	p<0.10 t=1.6 n=88
4. VIOLATION- I had to deviate from the procedure in order to be able to perform an operation	65	58	1.74 (0.66) n=92	1.75 (0.76) n=125	ns
Mean	51	49	1.55 (0.51)	1.55 (0.43)	ns

The risk of making serious errors at work

The results showed that in normal operation 4% of the operators judged the risk of making serious errors at work to be great or very great (levels 3 and 4 on the scale), while in the outage state 23% responded in this way. This difference was significant ($Chi2=15.46$, $p<0.001$, $df=1$). The answers to this question in normal operation and annual outage was significantly correlated across subjects ($r=0.35$, $p<0.01$, $df=124$). The results indicate a consistent individual level of rating across different working situations.

The risk of making serious errors at work was significantly correlated at the 5 percent level with the questionnaire items in Table 1(correlation range 0.17-0.46). This was true for all questions concerning both annual outage and normal operation except for question (4) "I had to deviate from the procedure in order to be able to perform an operation" in annual outage condition.

The diary

In the diary the operators were asked to report how often during an eight-hour shift they had made the specific error presented in table 2. The data were collected directly after each individual work shift.

TABLE 2. Error percentages (of total number of responses) for diary questions across different phases of the outage period. Participants indicating occurrence of the error at least once during the work shift. Due to the design different sets of crews generated different columns in the table.

Error type	Before outage n=90	Outage phase 1 n=57	2 n=57	3 n=63	4 n=58	After outage n=118
1. "Forgot to change the indicator of component status in the process chart"	13	14	33	30	26	7
2. "Promised to return to someone with information but forgot to do so"	8	25	30	17	17	10
3. "Was unable to remember something which I knew I am familiar with"	24	46	33	35	45	19
4. "Forgot to perform an operation in a sequence of operations that I planned to carry through"	11	11	18	13	16	4
5. "Forgot what to do because someone disturbed me"	18	38	42	30	47	19
6. "Was forced to interrupt a surveillance and control task because I was disturbed by someone and forgot to return to what I was busy doing"	14	18	18	20	33	12
Mean	14.7	25.3	29.0	24.2	30.7	11.8

Table 2 exhibits the proportion of operators indicating their own errors. The table shows the frequency of operators reporting each specific error at least once during the work shift (indicating level 2-5 on the scale). First, the results indicate that across error types between 11 and 47 percent of the operators report errors during outage (median=28%). In the measurements during normal operation (before/after outage) the corresponding numbers range from 4 to 24 (median=12.5%). Correspondingly the average percentage of errors across types and outage phases was 27.3 while the corresponding number was only 13.3 percent for the before/after condition ($Chi2=6.06$, $p<0.001$, $df=1$). Last, as could be expected, across all conditions, operators report more type (3) and (5) errors representing the less specific, wider categories of memory failure errors.

Subgroup analysis of diary questions

An analysis of variance was performed for the diary questions for operators participating before and after the annual outage during normal operation as well as at least at one occasion during annual outage. Pairwise comparisons were performed using a Scheffé test. The results are presented in Table 3.

TABLE 3. Analysis of variance for diary error ratings in a subgroup of 58 operators participating before, after and during the annual outage. (Means, standard deviations in parentheses). One way analysis of variance was applied to each error type and the resulting F values are shown. Differences between occasions that were significant are indicated below each error type.

Error type	Normal operation before outage (N1)	Annual outage (A)	Normal operation after outage (N2)	F	p (df=114/2)
1. "Forgot to change the indicator of component status in the process chart" (pairwise; A-N2, p<0.05, F=7.66)	1.14 (0.40)	1.31 (0.54)	1.03 (0.18)	7.8	0.001
2. "Promised to return to someone with information but forgot to do so" (pairwise; A-N1, p<0.05, F=6.55; A-N2, p<0.05, F=8.55)	1.10 (0.36)	1.34 (0.55)	1.07 (0.26)	10.2	0.001
3. "Was unable to remember something which I knew I am familiar with" (pairwise; A-N1, p<0.05, F=12.60; A-N2, p<0.05, F=15.44)	1.26 (0.48)	1.74 (0.85)	1.21 (0.49)	18.8	0.001
4. "Forgot to perform an operation in a sequence of operations that I planned to carry through" (pairwise; A-N2, p<0.05, F=5.10)	1.34 (0.66)	1.48 (0.60)	1.17 (0.38)	5.1	0.007
5. "Forgot what to do because someone disturbed me"	1.10 (0.31)	1.17 (0.42)	1.05 (0.22)	2.9	0.06
6. "Was forced to interrupt a surveillance and control task because I was disturbed by someone and forgot to return to what I was busy doing"	1.21 (0.52)	1.43 (0.90)	1.24 (0.54)	2.2	ns
Mean	1.19 (0.46)	1.42 (0.64)	1.13 (0.34)	-	-

All error types except (6) " was forced to interrupt a surveillance and control task because I was disturbed by someone and forgot to return to what I was busy doing" was rated as significantly more frequent during annual outage than during normal operation.

The results emphasize, as previously stated, that more errors are reported in the annual outage condition than during normal operation. The diary questions for this subgroup were significantly correlated between operational conditions across subjects (N1, mean correlation=0.44; A, mean correlation=0.44; N2, mean correlation=0.51). These correlations may have became inflated due to personal tendencies of high or low ratings but may also reflect other interindividual differences such as performing slightly different work tasks.

In summary, the results have indicated the usefullness of the questionnaire and diary method for collecting error data and indicates that errors could be categorized and compared

Covariance questionnaire and diary error reports

Because of different questions in the questionnaire and the diary it was not meaningful to compare them on a specific questions level. However it is possible to compare, for each operator, his answer to both the questionnaire and the diary through registering if there was (1) no error at all reported or (2) one or more errors reported. In this way it is possible to illustrate the responses elicited from the same sample of operators through the diary and the questionnaire. Table 4 illustrates this.

TABLE 4. Number of operators who reported at least one error in response to questionnaire and/or diary.

		Questionnaire		
		Operators reporting at least one error	Operators reporting no error	Sum
Diary	Operators reporting at least one error	75	29	104
	Operators reporting no error	15	5	20
Sum		90	34	124

It is clear that a great majority (119 out of 124) reported at least some kind of error in response to either the diary or the questionnaire. A total of 75 of the 124 operators report errors in response to both the diary and the questionnaire and only five operators reported no error at all. In general, the more concurrent diary method elicited more reports of one or more error (104 of 124) than the questionnaire (90/124). This seems to indicate that slightly more errors were reported using the diary method as compared to the questionnaire. However, we do not know whether the methods differ in sensitivity across the categories of errors.

The results indicate that self-reported errors can be collected in the Swedish nuclear power industry with a majority of the operators reporting errors. The results also show a consistent reporting of errors in a diary as well as in a questionnaire.

CONCLUDING COMMENTS

The present study has demonstrated that it is possible to collect self-reported errors from operators in a nuclear power process industry using either a questionnaire or a diary. Furthermore, the response frequencies were large enough to enable meaningful classifications of the errors into the categories of slips, mistakes and violations. The slight overrepresentation of slips during the outage period found in the questionnaires proved strong and significant when the diary data were analysed. In contrast, more mistakes were reported during normal operation than during the outage condition. Also the high proportions of violations indicates the importance of studying human errors and that an increased knowledge on human errors can result in technical design and procedural improvements.

It should be remarked that all incident investigations put the investigator at risk of making unwarranted, intuitive causal inferences (Dawes, in press). The fact that the sampling is performed on the dependent variable (errors) and uses human memory implies that the results can only illustrate errors (not e.g. indicate their relative frequencies). In addition human encoding, memory storage and retrieval of events are biased in many ways (e.g. Tversky & Kahneman, 1974). In the present study, the operators both encoded, memorized and reported their errors. Another problem is the lack of studies investigating the relationship between self-reported errors and "objective" error data. Therefore the validity of the self-reported errors as compared to objective measurements is difficult to assess and should be

in annual outage as compared to normal operation is interesting and suggests an important area for further research. The annual outage in nuclear power plants is an operational state with increased risk of errors and high workload, hectic work and time pressure and has recently attracted much attention (e.g. NSAC-174, 1992). A higher frequency of errors could therefore be expected for this operational state. Advantages of the self-report methods used in this study are ease of administration and low costs which make the methods attractive in field research. The memory bias may be greater for the questionnaire as compared to the diary method since errors reported in a questionnaire must be memorized over a longer time period.

The present study also illustrates a proactive approach to the control of human errors where minor errors are regarded as important in the sequence of a chain of events leading to a major accident. In other words, a proactive approach collecting reports of minor errors, with use of real life data from industrial settings as presented in this study as well as in-depth studies of severe incidents (e.g. Svenson, 1991), can be used to enhance our knowledge about human errors and thus enhance industrial safety.

REFERENCES

Broadbent, D.E., Cooper, P.F., FitzGerald, P. and Parkes, K.R. The cognitive failures questionnaire (CFQ) and its correlates. British Journal of Clinical Psychology, 21, 1-16, 1982.

Dawes, R. M. (in press). The prediction of the future versus an understanding of the past: A basic assymetry. American Journal of Psychology.

EPRI NP-6937. Operator reliability experiments using power plant simulators. Electrical Power Research Institute, Palo Alto, CALIF, 1990.

Feyer, A.M. and Williamson, A.M. A classification system for causes of occupational accidents for use in preventive strategies. Scandinavian Journal of Work, Environment and Health,1991;17:302-311.

J. E. Harris and P.E. Morris (ed.). Everyday memory, actions and absent-mindedness. Academic Press, London, 1984.

Herrman, D.J. Questionnaires about memory. In J. E. Harris and P.E. Morris (ed.). Everyday memory, actions and absent-mindedness. Academic Press, London, 1984.

INPO, 1985. An analysis of root causes in 1983 and 1984 significant event reports. INPO-85027. Atlanta, Ga: Institute of nuclear power operations.

Jacobsson, L. and Svenson, O. Psychosocial work strain of maintenance personnel during annual outage and normal operation in a nuclear power plant. Proceedings of the Human factors society 35th Annual meeting, San Francisco, CALIF, 1991.

Miller, D. P. and Swain, A.D. Human error and human reliability. In Handbook of human factors, G. Salvendy (Ed.). John Wiley, New York, 1987.

Norman, D.A. Categorization of action slips. Psychological review, 88, 1-15, 1981.

Norros, L. and Sammatti, P. Nuclear power plant operator errors during simulator training. Technical Research Center of Finland, research reports 446, Espoo, 1986.

NSAC-174. Survey of PWR plant personnel on shutdown safety practices and risk managment needs. EPRI Outage Risk Assessment and Managment (ORAM) program. Nuclear Safety Analysis Center, Electrical Power Research Institute, Palo Alto, CALIF, 1992.

NUREG-1154. Loss of main and auxiliary feedwater event at the Davis-Besse plant on June 9, 1985. Washington, D.C.: U.S. Nuclear Regulatory Comission, 1985.

Perrow, C. Normal accidents: Living with high-risk technologies. New York, Basic Books, 1984.

Reason, J. and Mycielska, K. Absent-minded? The psychology of mental lapses and everyday errors. Prentice-Hall, Englewood Cliffs, N.J. , 1982.

Reason, J. Human error. Cambridge University Press, Cambridge, 1990.

Svenson, O. The accident evolution and barrier function (AEB) model applied to incident analysis in the process industries. Risk Analysis, 11, 499-507, 1991.

Svenson, O. Safety barrier function analysis in AEB modeling of incidents and accidents. Reports to the Swedish Nuclear Power Inspectorate, MTO-unit, No. 20, 1992.

Tversky, A. and Kahnemann, D. Judgment under uncertainty: heuristics and biases. Science, 185, 1124-1131, 1974.

Woods, D.D. Operator decision behavior during the steam generator tube rupture at the Ginna nuclear power station. Research report 82-1C57-CONRM-R2. Pittsburgh, Penn.: Westinghouse R&D center, 1982.

DEVELOPMENT OF AN ORIENTATION BASED APPROACH TO EVALUATION OF PROCESS OPERATORS' EXPERTISE

Leena Norros and Kristiina Hukki

Technical Research Centre of Finland (VTT)
FIN-02150 Espoo
Finland

INTRODUCTION

Increasing reliability in the implementation of automation seems to imply the existence of two discrete operating states in production, the normal operation and the rare disturbance or accident situation. This fact has commonly been considered to create a polarized cognitive demand structure in the process control activity, characterized by the daily routines and the highly demanding novel problem solving, sometimes in an actual crisis. The question, how operators are in the daily routine able to learn those skills that are necessary in an accident situation, challenges the idea of polarized demands and calls for an elaboration of the connections between them.

In our research we have attempted to define the general common problems of expertise that must underlie the specific demands in routine and crises situations. It has been assumed that through tackling these common problems it would be possible to find a coherent approach to expertise in this work. The problem of interpretation of information in a complex situation has been considered the key problem through which expertise in process control activities could be studied. The concept of **orientation**, utilized originally by Galperin (1979), which refers to a person's way to frame a problem situation, is central in our approach. It is used to define the operators' way to cope with the problems of interpretation of information. We utilize this concept as a means to relate routine work and critical decision making in rare situations with each other and to conceive the roles of these seemingly polarized demands in the formation of expertise. In this paper, two simulator experiments on nuclear power plant operators' diagnostic activity are described. In the presentation of the results of these two experiments we want to draw particular attention to the methodological development of the experiments. This development indicates changes in our conceptions of the nature of process operators' expertise.

FIRST STUDY: AN ERROR APPROACH TO PROCESS OPERATORS' DIAGNOSTIC ACTIVITY

In an acute problem situation the difficulty of interpretation of information becomes manifest in the demand on the operators to interfere in the dynamics of the process by taking operative actions. In order to manage this the operators must meet the requirement to interpret the process information in the situation on the basis of their previous experiences

and verbal knowledge of the process. Operating experience and research results indicate that in such a situation the operators do not always succeed in their diagnostic and operative interpretations adequately. Typical problems are either unoptimal utilization of process information or unability to operationalize former knowledge of the system.

Above problems could be identified also in our own study on nuclear power plant operators' errors in simulated disturbance situations (Norros and Sammatti 1986). In the study a s.c. pathological method to study cognitive functions was adopted. Thus, deficiencies in activity control were analyzed with the goal of acquisition of information of the important control functions of activity in general. This approach has been widely used in studies of cognitive demands of different activities, and a comprehensive presentation of it can be found in the recent book by James Reason (1990). In our study, 12 NPP crews each performed two accident control situations of different complexity in full scale simulator experiments. A method developed in Risö National Laboratory to identify and classify operator errors was used (Hollnagel 1981). In this method deviations of the ideal operation scheme are classified according to the failing decision function and error category. These comprised of different task features which could be thought to contribute to errors.

No significant differencies in the distribution of errors along the decision function could be found as the task complexity increased. In both experiments errors concentrated equally in the decision and execution functions. Differencies were, however, found in regard with the contributing task characteristics. Thus, it was found that, with growing complexity, deficiencies in the knowledge of process interdependencies tended to increase, and this became evident in deficient and delayed decisions. According to the instructor it seemed that a classificatory diagnosis of the problem and choice of corresponding event based instruction was an efficient strategy in the less complex situation, but in the more complex situation this would not be sufficient. Further, on the basis of the fact that the number of errors in communication and cooperation was larger in the more complex transient, in the critical sequencies of the transient, and among the high error crews, it was concluded that possibly the strategies used by the crews were not optimally taking advantage of cooperative resources.

On the basis of the results we concluded that possibly there is a need to develop a disturbance handling praxis that would rely on cooperatively developed and used strategic plans within which process knowledge could be made operative. Our conclusion seemed reasonable and it was in accordance with other results indicating problems that operators may have in making use of process knowledge. As the used method did not, however, allow direct analysis of the crews' performance, a further study was considered necessary in order to verify this conclusion.

SECOND STUDY: AN ORIENTATION BASED APPROACH TO OPERATORS' DIAGNOSTIC ACTIVITY

This became possible on the basis of data from an earlier study within the OECD Halden project cooperation. This study was designed to validate particular operative aids. The data included comprehensive log outs and verbal protocols of 12 NPP operator crews in three different simulated disturbance situations. Parts of the data had been analyzed and published from the tool validation and tool development point of view (Hollnagel et al. 1983, Kautto 1984). No detailed psychological analysis of the crews' strategies in disturbance handling had been carried out.

When considering the methodology of analysis of the data, a critical evaluation of the

foregoing study (Norros and Sammatti 1986) turned out fruitful. In the earlier study operators' task was described as an ideal sequence of actions in the predefined disturbance situation. This ideal sequence was then used to define errors and evaluate the adequacy of operators' performance. This implies a traditional interpretation of expertise as an ability to reproduce actions that have been defined to represent excellency.

This definition of expertise is not explicit but it is embedded in the used experimental technique and the model of human cognition behind it. This widely accepted model implicitly assumes that human actions are governed by plans because they retrospectively can be described as following plans (Collins 1990,p. 43). This planning metaphor of action has been been criticized by Suchman (1987) who sees action as situated. "The fact that we can always perform a post hoc analysis of situated action that will make it appear to have followed a rational plan says more about the nature of our analyses than it does about the situated actions (Suchman 1987,p.53).

Adoption of the notion of situated action would offer a possibility to orientate to the constructive aspect of activity and expertise, which can be claimed to be relevant features of expertise (Engeström 1989). Instead of analyzing from above the fulfillment of the predefined sequence of acts it would be necessary to scrutinize, from moment to moment, how the operating crew navigates in the genuinely uncertain situation and gradually succeeds in structuring the situation. This new view to crews' activity replaced our earlier assumption of a cooperative strategic plan. In order to be able to analyze operators peformance, two kinds of tools were needed and developed.

First, as we had withdrawn from using an ideal action sequence as the reference of the crews performance a new type of reference had to be created. This was needed in order to relate the crews' actions to the process and to evaluate the adequacy of the crews' performances. Two reference models were defined. The first one was a tabel relating information of the process state to the principle options of the location of the disturbance i.e. the leak. This table provides the researchers with the possibility to define which process information, and at what point of time, is principally available and could be used as evidence in the definition and localization of the leak, i.e. it indicates the role of different process information in reducing uncertainty in the situation. Besides this, another reference model was created in order to evaluate the operative actions of the crews. This model indicates the operative methods that are available in maintaining the critical safety functions, such as primary circuit mass inventory or reactor core subcriticality. In other words, instead of referring to an optimal operative sequence, performance can be evaluated in regard with critical safety in stabilizing the process during which different methods are available. Both of these models allow a context dependent evaluation of the crews' actions without supposing any predefined course of activity.

The second tool needed in the analysis was a model of the psychological processes of constructing performance in disturbance handling. Based on the concept of orientation, the model of the interpretation of a disturbance situation was created. The focus in the model was the role of orientation in the control of actual disturbance handling, and the purpose of it was to guide analysis of the complicated data of the plant events and the crew's performance. The model that represents the assumed basic relationships is depicted in figure 1. It was constructed during the evaluation of six process operator crews' activity during a simulated difficult distrubance situation (Hukki and Norros 1993 a,b).

As indicated in the model (figure 1), task performance is supposed to consist of intertwined diagnostic activities (i.e. selection of information and definition of the problem situation) and prognostic activities (anticipation of the development of the situation in relation

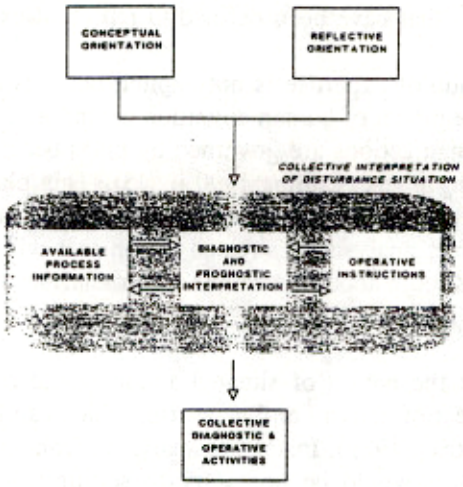


Figure 1. Model of interpretation of a disturbance situation.

to possible action alternatives) leading to operations. Carrying out these activities requires an interpretation of the meaning of the whole situation both from the diagnostic and prognostic point of view. The interpretation is thought to be based on the utilization of available information (dynamic process information and operating instructions, especially emergency procedures). These interactions between interpretations and information (indicated by the horizontal arrows in figure 1) are directed by the crew's orientation towards the task performance.

Orientation is naturally dependent on the operators' knowledge of process dynamics. The coherence of the representation manifests the conceptual aspect of orientation. The other aspect of orientation, the actors' reflective attitude towards their activity, i.e. their critical evaluation of their own activity is also important for the interpretation of the situation. These two aspects of orientation contribute to the construction of the interpretation of the meaning of the situation.

Because of the collaborative nature of the process control activity, the operators' activity has to be considered as group activity, as collective decision making. The construction of the interpretation is collective and therefore the operators' orientation towards the task performance effects their interpretation of the disturbance situation through collaboration.

By using this model, the construction of the interpretation of the disturbance situation and, inferred on the basis of it, the orientation of the crews, can be evaluated by analysing the way the operators use available information. The possibility to make inferences on conceptual orientation is based on the idea that the informating power, i.e. **informativity** of available information, may differ. The better information reflects the dynamically essential functions of the process, i.e. the better it can be used as evidence of the functional state of the process on a global level, the higher the informativity was considered to be. The orientation is supposed to be reflected in the degree of utlization of this informativity. The functionality of conceptual orientation can be evaluated on this basis.

The results of the analysis indicated that there were differences between the crews utilization of informativity of available process information. Those crews whose conceptual orientation was evaluated to be functional seemed to be more efficient in their diagnostic activity. Thus, as figure 2 indicates, the crews H and I, whose orientation was evaluated to be clearly non-functional, made the correct localization of the leak significantly later than other crews. Also the size of the leak was first underestimated by these crews, which was connected to some deficiencies in operative actions.

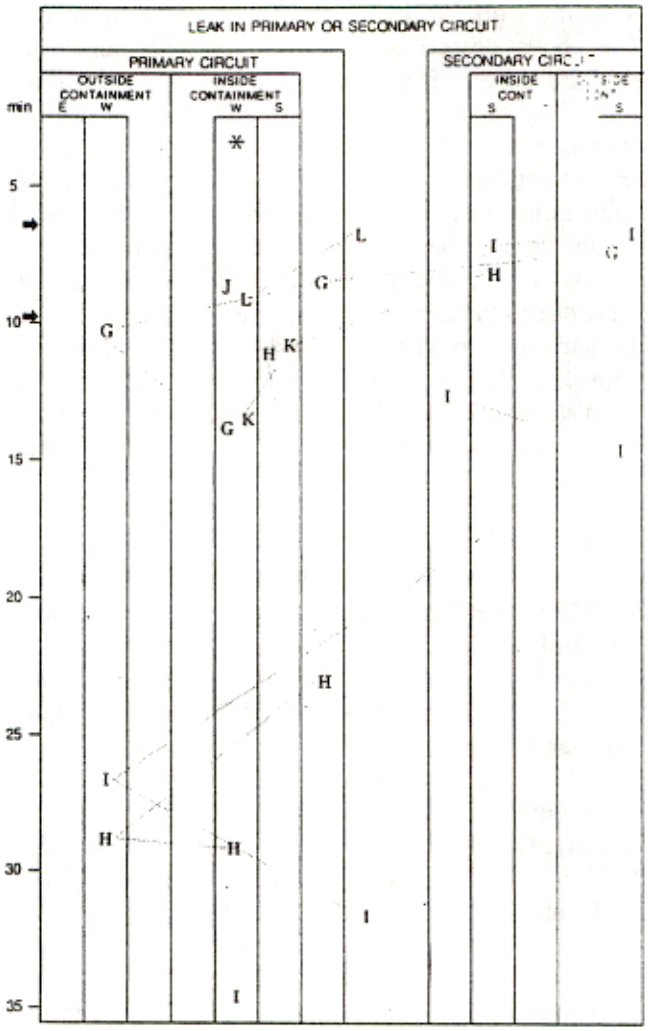


Figure 2. The crews' successive diagnostic hypotheses in the localization of the leak. * = the location of the leak; two small arrows = time span within which all symptoms of the leak had appeared. Type of leak: E=eneregy, W =water, S=steam.

The efficiency of those crews manifesting a functional orientation was interpreted to result from a more coherent reference for diagnostic and prognostic interpretation of the situation. The results concerning the reflective orientation were not equally confirmative, but clear indications of lack of reflectivity by the less functionally oriented crews could be found. This was associated with signs of subjective uncertainty which could be seen as a reflection of incoherency between diagnostic and operative interpretations of the situation among these less functionally oriented crews.

The results of the application of our model were interpreted to indicate the efficiency of the model in the analysis of crews' performance in a dynamic situation. With this model it seemed to be possible to conceive the crews' activity as it was constructed in the situation. In relation to that, instead of primarily emphasizing situatedness of activity (Suchman 1987), we would on the basis of this analysis stress the contextuality of activity. Orientation can be seen to serve this contextualization both through conceptual and reflective control processes.

CONCLUSION

In our ongoing work we have extended the problem to cover also the development of expertise. The above desscribed results support the conclusion that the functionality of orientation explains the expert's capability to interpret a concrete situation in a coherent way, in its relations. This capability to contextualize the particular situation seems to be very much the same as what is often meant by the expert's intuitive problem solving, typical to which is operative efficiency based on immediate insight of the problem situation. Emphasis on contextuality rather than intuitivity of problem solving would have the benefit that the former needs not only to be restricted to characterize experts' thinking but could as well appear at least by some novices. Our further assumption is that these novices would learn more effectively due to the fact that the coherent frame, that allows an effective interpretation of a particular situation, could also serve as a frame for the accumulation of experiences. A bridge between disturbance situation and routine could also be created, as the functional conception of disturbedness of the system would offer a frame to anticipate evolution of disturbances and interpret the role of small changes of the system from this point of view.

REFERENCES

Collins, H.M.,1990, "Artificial experts. Social Knowledge and Intelligent Machines", The MIT Press Cambirdge, Mass.

Engeström, Y.,1989, Developing thinking at the changing workplace: Toward a redefinition of expertise, Report of the Laboratory of Comparative Human Cognition, University of California, San Diego.

Galperin, P.J.,1979, "Introduction to psychology" (in Finnish), Kansankulttuuri, Helsinki. (original Vvedenije v pshihologiju, Moskva 1976).

Hollnagel, E.,1981, Guidelines for observations of operator decision making, Internal projekt report NKA/Lit-3(81)101, Risõ national laboratories, Denmark.

Hollnagel, E., Hunt, G. & Marshal, E.,1983, The experimental validation of the critical function monitoring system. Preliminary results of analysis, OECD Halden Reactor Project, HWR-111.

Hukki, K. & Norros, L., 1993a, An orientation based approach to evaluation of process operators' diagnostic activity. Fourth European Meeting on Cognitive Science Approaches to Process Control, August 25-27, Copenhagen, Denmark.

Hukki, K. & Norros, L.,1993b, Diagnostic orientation in control of disturbance situations. *Ergonomics, 0, 00* (to appear in November 1993)

Kautto, A., 1984, Information presentation in power plant control rooms, Research reports No 320, Technical Research Centre of Finland.

Norros, L. & Sammatti, P.,1986, Nuclear power plant operator errors during simulator training, Research Reports No 446, Technical Research Centre of Finland.

Reason, J.,1990, "Human Error", Cambridge University Press, Cambridge.

Suchman, L.,1987, "Plans and situated action. The problem of human-machine communication", Cambridge University Press, Cambridge.

DECISION MAKING UNDER UNCERTAINTY: A PILOT STUDY ON EXEMPTION FROM TECHNICAL SPECIFICATIONS

Kurt Pörn

Studsvik Eco & Safety
S-611 82 NYKÖPING
SWEDEN

INTRODUCTION

The various analyses with respect to the safety of an industrial complex, e g a nuclear power plant, are very important for the safe operation of such a plant. Many of these analyses are carried out under the banner of Probabilistic Safety Assessment (PSA). In addition to such PSA studies many specific aspects can be considered, for instance testing strategies, dependencies, human interactions, uncertainty issues etc. The purpose of all these studies is to provide various kinds of information based on which hopefully optimal decisions can be made.

In the context of nuclear power plant operation it is most desirable, from the authorities' as well as the power companies' point of view, that their decision making processes could be made in an easier and more reliable way concerning the risks and performance of the nuclear power plants. Within the scope of a Nordic cooperation project, NKS/SIK-1 (Use of living PSA for safety evaluation and management) a specific task was defined in order to study whether and how decision theory could be applied in practice to facilitate and support the decision making process.

Therefore the specific aim of the task was to structure a given decision situation with respect to its objectives, necessary limitations, decision alternatives and a reasonable preference model, following the procedures provided by existing decision theoretic models. Further, based on the gained experiences, we should identify the most obvious drawbacks in the models and data sources. To reach these goals, a concrete decision making problem, concerning an application for exemption from the Technical Specifications, was chosen in consultation with the Swedish Nuclear Power Inspectorate. The task was performed as a pilot benchmark study, carried out by Studsvik AB, Sweden[1] and Technical Research Centre of Finland[2]. This report is focussed mainly on the approach used by Studsvik, but of course, based also on the common experiences gained by cooperation in the benchmark study.

The paper presents results and experiences gained in a pilot study concerning decision making under uncertainty. The objective of the study was an attempt to apply decision theoretic models in order to develop procedures which will facilitate the decision-making

process in practice. The specific case considered is a decision making situation faced by the Swedish Nuclear Power Inspectorate, which had to reply on a NPP-operator's application for an exemption from the Safety Technical Specifications. During periodic tests of isolation valves in the main feedwater system of a Swedish BWR, indication of closed inner check valve was not obtained. Confronted with such a situation decision makers at the power company and at the authorities in particular had to make a rather prompt decision concerning the subsequent operating mode.

After this introduction we give a brief description of the theoretical background of decision making, mainly based on Lindley [3], where the essential concepts are introduced and the framework of decision making is clarified. Then we present the carrying-out and some specific results of the pilot study. Finally, the main conclusions are drawn and some major topics in the decision analysis situation are discussed.

SOME DECISION THEORY

A decision making situation is generally characterized by choosing a specific course of action among a set of decision alternatives, such that some predefined objective is achieved in some optimal way. The difficulty of the decision making lies in the uncertain events that may occur after the decision has been made. The objective of the decision analysis is to support decision making by systematically applying mathematical models and structures. The methods of decision analysis vary from simple methods such as decision tables to very advanced application of stochastic optimization. In spite of this variety of methods there is a common structure in the decision analysis procedures.

Here we concentrate on some fundamental decision theoretic concepts and models[3,4], which have been used in this study. Generally, a decision problem is to choose one specific course of action among a set of mutually exclusive decision alternatives $\{d_i\}$ such that some quantity of interest is maximized or minimized. The difficulty of the choice lies in the uncertain events $\{E_{j_i}|d_i\}$ after each decision d_i is chosen. One decision would be preferred to another one depending on the occurrence or non-occurrence of such event(s). The decision-maker, not knowing what events will in fact occur, must somehow balance one course of action against another to reach an unequivocal decision.

Assume that we have decision alternatives d_1, d_2,...,d_m with subsequent uncertain events $\{E_{j_i}|d_i\}$ conditioned on the decision alternative chosen. The events $\{E_j\}$ must be defined such that they become mutually exclusive and collectively echaustive. The set of all possible events is then

$$E = \bigcup_{i=1}^{m} \{E_{j_i}|d_i\}$$

Now we must be able to compare the decision alternatives in some manner if we want to reach a rational choice of the course of action. Conceivably, we need to assign some, preferably numerical, value to each of the decision alternatives by which the comparison can be made. A naturally arising question is how to take into account the fact that the uncertain events, after each possible course of action is taken, occur with different likelihoods and the consequences of each combination of action and event vary. Hence, after the objective of the decision making situation has been defined and the decision alternatives and the uncertain events have been identified, the process of decision analysis can be divided into following steps: 1) to assign each event E_j a numerical value expressing the probability of occurrence, 2) to assign each couple of action and event (d_i,E_j) a numerical value by evaluating the consequence and 3) to assign each decision alternative a numerical value expressing the merit of the decision alternative. Thus the decision problem is decomposed into elements, each of

which is subjected to analysis and evaluation by the analyst and the decision maker. In step 3) the individual elements are integrated to provide overall insights and preferences with regard to the original problem.

If a particular decision d_i is taken and the uncertain event E_j occurs then no uncertainty is involved and this combination of d_i and E_j, (d_i, E_j) results in a foreseeable consequence C_{ij}. This can be illustrated by the decision table, Table 1.

Table 1. A decision table.

	E_1	...	E_n
d_1	C_{11}	...	C_{1n}
...	...	...	...
d_m	C_{m1}	...	C_{mn}

A qualitative ranking of these consequences may be relatively easy. Such a ranking, however, without a numerical value attached may not be very useful.

Suppose that any pair of consequences can be compared such that one is either preferred to the other or they are equally preferred. Such a comparison is said to be coherent if, whenever consequence C_1 is preferred to C_2 and C_2 to C_3, then C_1 is preferred to C_3. Further, let C and c be the "most favourable" and the "least favourable" consequence respectively in the decision problem. Any consequence C_{ij} is no less favourable than c and no more favourable than C. Using these two consequences as our reference, it can be shown that associated with any consequence C_{ij} is a unique number u lying between 0 and 1 such that C_{ij} is just as desirable as a chance u of getting C and 1-u of getting c. In other words, there must be a value u such that we are indifferent between "getting C with chance u" and the consequence C_{ij} with certainty.

This number which is attached to C_{ij}, denoted by $u(C_{ij})$, is called the **utility** of C_{ij}. It should be noted that this utility is a probability since u is equalized to the probability of obtaining the most desirable consequence C in the game-oriented thinking experiment above. When the concept of utility has been introduced we may now modify the decision table as in Table 2, which in addition to utility values also includes the probabilities of the mutually exclusive events $\{E_j\}$, conditioned by the each of the decision alternatives $\{d_i\}$.

Table 2. A decision table with utilities and probabilities.

	E_1	...	E_n
d_1	$u(C_{11}), Pr(E_1\|d_1)$	...	$u(C_{1n}), Pr(E_n\|d_1)$
...	...	...	...
d_m	$u(C_{m1}), Pr(E_1\|d_m)$	...	$u(C_{mn}), Pr(E_n\|d_m)$

Based on the exclusive and exhaustive feature of the events $\{E_j\}$ we can by simple probability calculus derive the expected utility of decision alternative d_i, $E[u(d_i)]$.

$$E[u(d_i)] = \sum_{j=1}^{n} u(d_i, E_j) \cdot Pr(E_j|d_i)$$

where the expectation is taken over the uncertain events $\{E_j\}$. This expected utility is a measure of the merit of d_i. Therefore, the decision alternative d_i to be chosen should be such that it maximizes the expected utility.

From the above it is readily seen that the most essential task in decision analysis is to estimate the probability values $Pr(E_j|d_i)$ and to assign the utility values $u(d_i, E_j)$. The difficulties of the former task depends on the extent of available information. All adequate operating experiences and expert knowledge should be used. The uncertainties of all model parameters are to be integrated into unique probabilities $Pr(E_j|d_i)$. The assigning of the utility values involves the decision maker's subjective knowledge, available information and not least his/her personal attitude (aversion to risk). The procedure described above presupposes that the consequences of all events considered can be assigned utility values on a single scale (a single-attribute utility function). If this is not possible one has to go to more complex, multi-attribute models which, on the other hand, requires weighting functions for the different attributes. Such a model was applied by the Technical Research Centre of Finland in this pilot study[2].

THE PILOT STUDY

The object of the pilot study is the following. At a Swedish boiling water reactor, in the main feedwater system, one of the inner isolation valves of the containment gave no indication of closed valve in a periodical valve closing test. In accordance with the Safety Technical Specifications (STS), the isolation valve in question was declared to be inoperable. The situation violates the tightness requirements of the containment, and either the plant must be shut down or the power must be reduced to 65 % through keeping the pipe line closed by the outer isolation valve.

The experience of indication failures in other test situations of the same type made the power company suspect that the failure was in the indication, and not in the operation of the check valve. To avoid the requirement stated by the STS, the power company decided to apply for an exemption from the rules to continue the full power operation during the remaining seven weeks until the the next annual refuelling outage.

It is readily seen that the situation poses three different alternatives

- d_1: Continue operation with full effect
- d_2: Continue operation with 65 % effect (the feedwater train of concern is closed)
- d_3: Shutdown

Conditioned on each alternative taken, a sequence of events may occur with consequences varying from no damage, through degradation, to core damage. A failing isolation valve may lead, if not to core damage, to somewhat less severe consequences such as limited discharge of reactor water outside containment or contamination of the feedwater system by radioactive discharge from the containment.

In traditional probabilistic safety assessments (PSA) the main interest is focussed on the probability of core damage (CD). Therefore, it was close at hand to start this case study with considerations from that perspective. By thinking through the decision model with the alternatives mentioned above and with only two groups of uncertain events, *core damage* or *no core damage*, it was readily seen that the study should require comprehensive analyses,

similar to those of PSA level 1, to calculate the probability of core damage, Pr(CD|di), for each decision alternative taking into account the specific situation with no indication of a closed feedwater check valve. Analyses of this kind were not deemed to be practicable in the given situation when a relatively prompt decision was to be made. In addition, it is not relevant to consider consequences only on the level of core damage.

Risk of degraded safety function

The safety function of the inner check valves is to isolate the containment in case of pipe break inside or outside the containment, in order to minimize the release of radioactivity or reactor water respectively. This safety function is regulated by the STS. Therefore, from the authorities' point of view and also with regard to practical decision making aspects, it would be desirable to analyze the decision making problem merely considering the aforenamed safety function. Then the key question is with what probability the indication is correct, that is, the isolation valve is indeed inoperable. The possible consequences with respect to the safety of the whole plant of a failing safety function have to be considered in the choice of utility values, which will be discussed below. These utility values may be determined "once for all", e.g. on the basis of the plant specific PSA and associated analyses.

Hence, the utility table may look like Table 3, where the decision alternatives d_a and d_r mean that the use of the isolation valve is either accepted (d_1 in previous section) or rejected (d_2 or d_3 in previous section). We notice that the function or malfunction of the component itself is listed as uncertain events. Which one of these primary events will occur will be seen only at a real demand or at the annual revision.

Table 3. System specific decision table.

	Events	
Decisions	Check valve can close	Check valve cannot close
d_a (accept)	1	0
d_r (reject)	R_0	R_0
Prob.	Pr("can close"|"no ind.")	1-Pr("can close"|"no ind.")

The most and the least favoured consequence is assigned utility 1 and 0 respectively, as can be seen in Table 3. The operation of the isolation valves (alternative d_a) brings some economic benefits, but at the same time such an operation can introduce an accident risk. It is the safety authorities' task to balance benefits against risk by stating a utility value, denoted by R_0, of "not taking the system into operation" (alternative d_r), which means the safety benefits of "no use and no failure" [5]. Therefore, R_0 is a decision criterion, implicitly determined by the safety authorities saying that the function probability of the check valve must exceed R_0. The criterion value R_0 (system reliability requirement) for the system considered could be determined "once for all", as a function of the system demand frequency and the whole spectrum of consequences that can be caused by a system malfunction. It is also quite obvious that the criterion level R_0 may vary from plant to plant, and from society to society, depending on the overall benefits of the plant in question.

From Table 3 the expected utility of each decision alternative is easy to derive, resulting in

$$E[u(d_a)] = Pr(\text{"valve can close"} | \text{"no ind."})$$

and

$$E[u(d_r)] = R_0$$

Thus the function probability of the check valve, conditioned by the existing knowledge and experience in the specific situation, becomes the quantity to be compared with the predetermined criterion value R_0.

In our case study, the function probability above was assessed through a comprehensive use of generic Swedish data[8] as well as plant and component specific experiences concerning failures of both check valves and closing indication. The so called $q+\lambda t$-model[9] was used to calculate the component unavailability. Some interesting probabilities may be noticed, e.g. Pr("valve fails to close") = 0.0016, Pr("no ind."|"valve can close") = 0.041 and Pr("valve cannot close"|"no ind.") = 0.036.

CONCLUSIONS

In this pilot study we were lucky to have a good deal of information in forms of operational data for the components concerned. Thus we were able to estimate e.g. the probability of "no closing indication" when the check valve succeeds to close. A value as high as 0.041 indicates the need for technical improvement of the indicator equipment. Further, the probability 0.036 of " check valve cannot close", conditioned by "no closing indication" is too high to be considered as negligible.

In this pilot study a relatively simple and practicable approach to decision analysis and decision making has been demonstrated. It would be quite useful for the safety authorities to have, a priori, determined criterion R_0-values for each safety related system, based on the estimated frequency of system demand and the overall consequences when the system fails. With such a predefined set of R_0-values, many decision making situations could be supported by a relatively simple analysis of the kind presented in this study. The required information concerns only the component or system in question, once R_0 is predetermined.

In the pilot study referred to in this paper also other, more complex approaches were used [10], based on multi-attribute utility functions. Such decision analysis methods could be applied to long-term decision situations, when more time is available for analysis. Irrespective of level of decision model, the pilot study has created interest among the Swedish and Finnish nuclear power authorities to go further with the decision anlysis framework.

Acknowledgements

The author is indepted to the Swedish Nuclear Power Inspectorate for the financial support both of the study described in this paper, within the framework of the joint Nordic project NKS/SIK-1, and of the work required for the preparation of this paper.

REFERENCES

1. K. Pörn and K .Shen, Decision Making under Uncertainty - A Pilot Study on Exemption from Technical Specifications. Report STUDSVIK/NS-91/90, NKS/SIK-1(91)29, Studsvik AB, Nyköping (1992).
2. J. Holmberg and U. Pulkkinen, Decision Analysis on an Exemption from the Technical Specifications. Report VTT/SÄH 4/92, RISKI(92)1, NKS/SIK-1(92)8, Technical Research Centre of Finland, Espoo (1992).
3. D.V. Lindley, "Making Decisions", 2nd ed. John Wiley, London, (1985).

4. E. A. Robinson, "Statistical Reasoning and Decision Making", Goose Pond Press, Houston, Texas, (1981).
5. C.A. Clarotti, PSA, Subjective Probability and Decision Making, in: Proc ANS/ENS International Topical Meeting, Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania. (1989).
6. K. Pörn, On Empirical Bayesian Inference Applied to Poisson Probability Models, PhD Thesis, *Dissertations No. 234*, Linköping University, Sweden, (1990).
7. K. Pörn and K. Shen, On the Integrated Uncertainty Analysis in Probabilistic Safety Assessment, in: Safety and Relability '92, ed. K.E. Petersen and B. Rasmussen, ESRA Conference Series, Elsevier Applied Science, (1992).
8. T-book. Relaibility Data of Components in Nordic Nuclear Power Plants. 3rd ed.. Prepared by the ATV-Office and Studsvik AB. The ATV Office, Vattenfall AB, Vällingby, (1992).
9. K. Pörn, Statistical Treatment of Time- and Demand-related Failures in the Nordic Reliability Data Book, in: PSAM-II, An International Conference Devoted to the Advancement of System-based Methods for the Design and Operation of Technological Systems and Processes, Plenum Publishing Corporation, New York, (1993).
10. J. Holmberg, U. Pulkkinen, K. Pörn and K. Shen, Risk Decision Making in Operational Safety Management - Experience from the Nordic Benchmark Study, Report NKS/SIK-1(92)17, RISKI(93)1, Studsvik EcoSafe, Nyköping, (1993).

027 Hazard Analysis in the Process Industries

Chair: T. Aldemir, Ohio State U.

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

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

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

HAZARD ANALYSIS FOR COMPLIANCE WITH PROCESS SAFETY REGULATIONS

Mardy Kazarians

Kazarians & Associates
220 South Kenwood Street, Suite 305
Glendale, California 91205

INTRODUCTION

Process safety management (PSM) is the focus of several regulatory agencies and industry affiliated institutions. Many of these agencies and institutions have promulgated or are in the process of finalizing regulations that require the owners and operators of facilities that handle or store highly hazardous materials to establish a process safety management program. These regulations and suggested practices by industry institutions identify the elements of process safety management which include clauses on hazard analysis.

This article explores the hazard analysis requirements, the various methodologies that can be used to achieve compliance, the current industry practices, and the strengths and weaknesses of the different methods. It addresses such issues as:

- What is meant by hazard analysis?
- Scope of hazard analysis
- Cascading events
- Pitfalls of risk matrices for decision making
- Uses of quantitative risk assessment

REGULATORY REQUIREMENTS

In the United States, regulations that address process safety have been promulgated at the Federal and at state levels, and industry affiliated institutions have issued recommended practices[1 to 8]. At the Federal level Occupational Health and Safety

Administration (OSHA) has adopted 29 CFR Part1910.119[1], and Environmental Protection Agency (EPA) is in the final stages of adopting the Risk Management Programs rule (40 CFR Part 67[2]). Before OSHA and EPA started considering process safety regulations, several states had already passed and implemented laws that effectively addressed process safety management issues[3,4]. In addition to the government bodies, industry affiliated institutions have issued reports and recommended practices[5,6,7,8].

In all cases, an analysis is required of the hazards of the processes and the regulations also provide additional statements about the methodology and scope of the process hazard analysis. For example, OSHA 1910.119 states that "the employer shall perform a process hazard analysis" and lists a series of methodologies accepted for analyzing hazards.

WHY HAZARD ANALYSIS?

The purpose of hazard analysis is to gain an understanding of the hazards in a facility so that decisions can be made to enhance safety. Many of the referenced regulations or recommended practices have provided some clarification on what is meant by hazard analysis and have suggested methodologies for this purpose. In practice, there has been a wide variation in the scope and depth of the analyses conducted by various facilities in different industries.

To properly define the scope of the hazard analysis and to comply with the requirements of the regulations, we should have a better understanding of what is meant by hazard (so that there can be an analysis of it), what is meant by understanding, and how can one use hazard analysis to enhance safety?

Hazard is defined as the source of harm[9]. If this definition is followed narrowly, hazard analysis would solely be focused on the sources of harm, and the analyst may chose to ignore the effects of the safeguards. Clearly this is not the intention of neither the regulations nor the business owners and operators. The term risk, which is defined as the possibility and magnitude of receiving harm, does account for the effects of safeguards (and several other safety related parameters), and therefore is the accurate term for our purposes. Thus, the regulation and recommended practices require us to do a risk analysis and not an analysis of hazards.

The referenced regulations and industry suggested practices do not generally clarify this point and in some cases (e.g., California's RMPP[3]) the interpretation of the term hazard varies among the different paragraphs in the same regulation.

SCOPE OF "HAZARD" ANALYSIS

The guidance provided by the regulations and recommended practices is not specific on the scope of hazard analysis. The accepted scope is still evolving as different industries and regulatory bodies are gaining experience in conducting and using such studies. For example, in the case of the California RMPP law[3], since the early days of its implementation, the scope of hazard analysis has undergone many changes and an accepted scope has evolved.

A risk analysis should provide the answer to three questions -- what can go wrong?, how likely is it? and what are the consequences? These three elements should be addressed regardless of the level of detail or scope of the analysis. How they are addressed and in what level of detail distinguishes among different methodologies and scope of the analysis.

Event characterization includes identification of sources of hazards and chain of events that lead to the occurrence of hazardous situations. A crucial aspect of this part of risk analysis is the completeness of the list of hazards and chain of events. Completeness is necessary to assure that risk acceptance and risk reduction decisions are done on a rational basis.

The chain of events start with an event which is referred to as the initiating event. Often many safeguards are provided in the design of a system to mitigate the effects of an initiating event. A chain of events, therefore, includes an initiating event and the events that follow and specify either failure of the safeguards or occurrence of conditions that affect the magnitude of the release.

The majority of the regulations or recommended practices provide some guidance on the methodology that can be used for event characterization. Many facilities have elected to use methods that identify the hazards, and provide some information about the possible chain of events.

Likelihood evaluation can be a complex process and may require special event modelling, statistical analysis of failure data and manipulation of event frequencies and probabilities. A few of the regulations specifically require that the likelihood of events be estimated (e.g., New Jersey[4]), thus some owners and operators have elected to include likelihood evaluation within the scope of the analysis.

Consequence and damage evaluation addresses worker safety, public exposure, ecological impact, economic impact or a combination of these distinctly different damage attributes. It is generally clear which damage attribute is the focus of a specific regulation. For example, OSHA 1910.119[1] is focused on worker safety and EPA's RMP Rule[2] is focused on public exposure.

HAZARD ANALYSIS METHODOLOGIES

There are a variety of methods available for hazard identification. Several books have been written on the subject; the most famous of which is Reference 10 that provides a catalog of methods with worked examples. The following is a list of methods that have had more usage than others:

- Hazard and Operability (HAZOP) Study
- Failure Modes, Effects and Criticality Analysis (FMECA)
- Fault Tree Analysis (FTA)
- Event Tree Analysis (ETA)

The main requirement of all methods is to identify the complete set of events that may occur and lead to adverse consequences. To achieve this the method should be rigorous, systematic, and structured. HAZOP is perhaps best suited for a facility that processes highly hazardous chemicals, because it addresses all those areas of the process where the

hazardous materials may exist and it focuses on the ways by which an adverse condition may occur.

FMECA is an excellent tool for identifying the ways a complex component or equipment item may fail. It identifies the failure modes of every component in a system (complex component or equipment item) and the impact of those failures on the entire system.

Fault tree analysis is best suited for analyzing safety systems, for a system with many built-in redundancies, for a system where the source of harm, the hazard, is concentrated in one area, or for analyzing a sub-system or equipment item that has been identified in a HAZOP as extremely important to safety.

An event tree is an excellent tool for analyzing a system with several layers of safeguards that require multiple failures to occur for a release to manifest itself.

CASCADING EVENTS

It is often claimed that HAZOP and FMECA (or FMEA) methods address single failures and are incapable of identifying "double-jeopardy" type scenarios. Actually, this is not the case. For an adverse consequence to manifest itself, an initiating event should occur. This is an event that would perturb the balance of the plant and may lead to an adverse consequence if automatic systems or operators fail to intervene. Thus, if there are any safety features incorporated into a system, the initiating event (a single event) would not lead to a release by itself. To properly identify the consequences of a deviation in a HAZOP or the effects of a failure mode in an FMEA, the analysts should consider the influence of the safety features on the chain of events. Many businesses, for estimating the level of the consequences, have adopted the procedure of assuming that all safeguards are rendered ineffective. In such cases, the analysts list the safeguards that could influence the consequences or the likelihood of occurrence. This list represents the additional failures (in addition to the initiating event) of the multiple failure chain of events.

The assumption of loss of safeguards is the same as considering multiple failures. The simultaneous occurrence of two initiating events is very small. Therefore, if the list of initiating events is complete, it can be claimed that the HAZOP or FMECA have properly addressed a complete list of "worst" case scenarios. They are worst case because, in some cases the safeguard limits the damage level. The consequence level is small if the safeguard functions properly, and the level may be severe if the safeguard fail. Clearly, in the case where the safeguard functions, the likelihood of occurrence of the scenario is greater that the scenario that assumes safeguards failure. Thus, the adopted methods would only address the high consequence and low likelihood events.

USING RISK MATRICES

To facilitate the decision whether the risk of a scenario is unacceptable and whether a scenario is more risky than another, an index of criticality levels (a risk ranking scheme) is used. It is based on the two elements of risk -- likelihood and consequences of an event.

A pre-specified set of likelihood and consequence (severity) levels are used to establish the criticality index. The levels can be defined in many different ways and in different levels of detail. The specific conditions and needs of the facility or system should dictate how the categories are defined. Based on the likelihood and consequence (severity) categories, a matrix of criticality (risk) levels can be established. The criticality levels can then be used to establish a decision rule for proposing recommendations.

The estimation of the likelihood and consequence severity is generally done during a brain-storming session (e.g., HAZOP session) where a team of experts who are intimately familiar with the process under study, and often are not necessarily familiar with hazard analysis methods, provide the estimates. This can lead to large uncertainties in the way likelihood and consequences are estimated, and may be influenced by group's hidden agenda. This shortcoming of the methodology can be remedied by third party expert's review of the analysis and the estimates, and management review of the recommendations and their basis.

Another pitfall of the risk matrix approach is that it can be manipulated by the users to justify risk acceptance of a scenario without violating any of the rules of the methodology. Each scenario (chain of events) that leads to adverse consequences, can be redefined in terms of several more narrowly defined scenarios that are individually less likely to occur, but collectively are the same as the original scenario. To circumvent this pitfall, the decisions should be based on the total frequency of the class of scenarios that lead to the same level of consequences. This often is not simple to do because the analysis team uses qualitative terms to define the likelihoods.

WHEN TO USE QRA?

The risk matrix approach is an approximation of a QRA approach using rough definitions for likelihood and severity of consequences. QRA is hazard analysis in its complete form. It encompasses all the necessary elements to produce risk estimates that are defensible and rational. One way to view the hazard analyses, that are conducted today for complying with safety regulations, is that a QRA is conducted with several of its major elements missing. If the applied method yields the information that is sufficient for the decision maker, the conduct of any further analysis, more detailed than that undertaken will be fruitless and ineffective for the plant. However, there are situations where QRA level of detail should be considered for hazard analysis.

Detailed QRA should be the method of choice when faced with an emotionally charged opposition. A detailed study will contain the scenarios that could be the focus of the opposition. QRA will provide the medium for a rational dialog. Any study less detailed than a QRA has to include simplifying assumptions. A simplifying assumption that may not be conservative can be used by the opposition to assert that the risk levels of the facility is unacceptable.

CONCLUSION

Hazard analysis is a central element of all process safety regulations and industry suggested practices. Hazard analysis is actually the analysis of risks (the possibility and

magnitude of receiving harm). The scope of the risk analysis (or hazard analysis as it is used in the regulations) is a different issue. Depending on the specific characteristics of the hazardous materials and operations and the political climate within and outside the plant, a wide spectrum of options are available to the management and the analysts for defining the scope of the analysis.

Risk ranking can afford sufficient detail and the most economical approach, when the alternatives are somewhat expensive or the risk level is rather high. It is important for the users (i.e., the management and hazard analysis team) to understand the pitfalls of risk ranking. If an expensive recommendation is considered, a detailed analysis (a mini-QRA) may be necessary to strengthen the basis of the decision. Also, a detailed analysis of specific issues may be necessary to verify the estimates provided by the analysis team and disputed by the technical reviewer.

"Worst case" analysis can be adopted only when it is suspected that the worst possible release scenario leads to an acceptable consequence level. For this approach to be acceptable, the analysts should assure that there are no scenarios, no matter how unlikely, worse than the so called "worst scenario". Otherwise, the analysts should adopt the risk ranking method.

REFERENCES

1. "Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents; Final Rule", U. S. Federal Register, Part II Department of Labor, Occupational Safety and Health Administration, 29 CFR Part 1910, (February 24, 1992).

2. "Risk Management Programs for Chemical Accidental Release Prevention", U. S. Environmental Protection Agency, 40 CFR Part 67, to be issued.

3. "Hazardous Materials Management", Article 2, of Chapter 6.95 of the California Health and Safety Code, West's Annotated California Codes, Health and Safety Code Sections 18200 to 25699, Volume 40B, (1992).

4. "Toxic Catastrophe Prevention Act", New Jersey Department of Environmental Prevention, Division of Environmental Quality, (June 1988).

5. "Management of Process Hazards" API Recommended Practice 750, First Edition, American Petroleum Institute, Washington D.C., (1990).

6. "Recommended Practice for Development of a Safety and Environmental Management Program for Outer Continental Shelf (OCS) Operations and Facilities" API Recommended Practice 75, First Edition, American Petroleum Institute, Washington D.C., (May 1993).

7. "Guidelines for Technical Management of Chemical Process Safety" Center for Chemical Process Safety, the American Institute of Chemical Engineers, New York, New York (1989).

8. "Plant Guidelines for Technical Management of Chemical Process Safety" Center for Chemical Process Safety, the American Institute of Chemical Engineers, New York, New York (1992).

9. Kaplan, S. and B. J. Garrick "On the Quantitative Definition of Risk." *Risk Analysis* 1(1):11, (1981).

RISTOX, A TOXIC GAS RISK ANALYSIS PROGRAM

James M. Hudson and Alex See

ACTA Inc.
23430 Hawthorne Blvd
Torrance, CA 90505

INTRODUCTION

Recently, the Federal Government issued a draft set of regulations that go beyond hazard evaluations. These regulations are expected to be similar in intent to those embodied in the California Risk Management and Prevention Program (RMPP). The Federal Risk Management Program (RMP) will require many facility operators to determine the effects of worst case accident events. For example, the potentially worst case events identified in a hazard evaluation may require analytical study to define their impact to offsite populations. As is required in the California RMPP, gas dispersion models may be used to determine the extent of a release of toxic materials resulting from a worst case scenario. Contours of toxic concentrations may be overlaid on surrounding populations to show the potential impact of a release.

This method of presentation has some utility in terms of emergency response needs. Unfortunately, however, it paints a bleaker picture than reality, since the likelihood of the event is not included. In other words, a risk framework is a more realistic and probably more useful presentation. A risk presentation does require more effort on the part of the analyst and additional experience on the part of the regulatory body. However, the pay back is likely to be well worth the effort.

The collection of the many elements of data needed to perform a facility risk analysis generally yields much insight into potential problem areas. The presentation of risk in terms of, say, risk profiles provides a yardstick whereby an operator may specify the most suitable mitigation measures should they be deemed necessary.

Presenting the potential impact to a population from a hazardous facility in the form of toxic hazard contours is likely to make all facilities, even relatively safe units, look "risky". The work embodied in this paper offers a different approach, which can be used to complement the worst case hazard presentation. The risk based approach presented here is the basis for a toxic gas risk analysis computer program called RISTOX.

The many elements of computing the risk from toxic gas releases are included in RISTOX, which is currently being programmed to operate in a WINDOWS(tm) environment. The authors have spent many man-months developing RISTOX's subroutines to yield a user friendly program that will handle any type of cold-spill gas release to the atmosphere. The program performs all of the necessary complex calculations and outputs

the results in the form of risk profiles ready for presentation. In addition, the user can perform what-if type computations to determine the impact of mitigations.

RISTOX DESCRIPTION

RISTOX provides the unique ability to define risk profiles associated with the toxic materials released after accidental spills from storage vessels or other equipment. RISTOX thus enables the evaluation of toxic hazards not merely in terms of whether worst-case, deterministic, dose levels may be exceeded in some populated area, but rather in terms of the probability that the number of people who suffer some health effect will exceed some value (risk profile). The computations implemented by RISTOX are as follows:

1. The Main Menu provides options to create or modify input data, execute the program and specify the manner of presenting results.
2. RISTOX computes a release rate from an accident scenario defined by the user.
3. A spill scenario is initiated. The computed release rates are entered to a cold gas dispersion model to determine the toxic concentrations at each receptor. RISTOX generates a correlated random sample of relevant meteorological conditions, which is derived from the weather covariance matrix. The parameters sampled are wind speed and direction, and temperature.
4. For each Monte Carlo cycle, RISTOX enters the sampled meteorological conditions, release rates, exposed populations and their locations, to the selected cold spill model. The concentrations of toxic material that impact each receptor are then computed.
5. RISTOX now computes the probability of a specified health effect severity level (HESL) (mild, significant or fatal) at each receptor. The binomial mean NP_{eff} and variance $NP_{eff}(1-P_{eff})$ are computed, for each receptor, for each HESL. P_{eff} is determined from each relevant exposure-response function. The mean and variance of the number of individuals suffering at least each HESL is then computed for the total population.
6. RISTOX now generates a histogram for each HESL using one of the methods: normal approximation, binomial distribution or Poisson approximation. These histograms have an associated weighting equal to the product of the wind direction frequency and the probability of the hazardous event.

This ends RISTOX's first Monte Carlo cycle. The process is repeated for the number of Monte Carlo cycles selected and the histograms stored with their associated weightings.

7. The discretized histograms are summed to obtain an aggregated histogram for the total set of accident scenarios.
8. Finally, RISTOX derives a risk profile for the facility, for each HESL, from the corresponding histograms. RISTOX interacts with a graphics routine to plot the risk profiles to the screen or to a printer.

RISTOX Menu Screens

The current version of RISTOX provides menu driven capabilities. It provides a user friendly tool to enter input data, to execute the program and output results. The program is structured such that each desired action can be selected from a pull down menu. All RISTOX operations are accessed through its main menu.

RISTOX SUBROUTINES

AFTOX Subroutine

RISTOX currently incorporates the AFTOX [1] cold spill dispersion model that accepts spill scenario data and predicts toxic concentrations at receptor locations. AFTOX Version 4.0 was modified to be an interface program to meet RISTOX needs. AFTOX predicts the time-mean concentration at the center of each receptor.

AFTOX calculates toxic concentrations using an instantaneous puff Gaussian model or a continuous plume Gaussian model, depending on the type and time of release of toxic materials. AFTOX was designed to handle continuous and instantaneous, liquid and gas, surface and elevated releases from a point or area source. It currently contains a library of more than 129 chemicals.

Source-Term Subroutine

This subroutine determines the discharge rate of a specific toxic material for a given hazardous event. RISTOX currently uses the ARCHIE [2] program to compute the necessary source terms for input to AFTOX. ARCHIE (Version 1.0) is a chemical hazard incident evaluation program, which is incorporated into RISTOX. The user specifies hazardous events (accident scenarios) and enters data through the RISTOX main menu.

Exposure-Response Functions

To define exposure-response functions (probability of effect versus exposure, ceiling or TWA concentration) for exposed individuals, given only the single lower limit for each material, a linear function through the limit (used as a 1st percentile) and through the origin, is assumed. As illustrated in Figure 1, this line is conservative; i.e. yields higher values of probability of effect versus response for concentrations in a range of practical interest relative to the probit and other likely exposure-response functions with the same 1st percentile, for non-cancer effects. If not cut off, but continued to the origin, it would be a generally accepted model for cancer effects. While such a line could be non-conservative relative to some exposure-response functions that might ultimately be of concern, at present conservatism is believed much more likely. Linear functions may not be conservative for high exposures. Studies are continuing to develop exposure-response functions that incorporate the best available toxicological data.

Histogram Subroutine

The relevant exposure-response function is applied for each scenario,at each receptor, to each population group, for each health effect severity level. Given the dose predicted by the dispersion model, the probability that an individual will be affected, to the severity level or higher, results. This probability is the parameter of the binomial distribution of the number of such individuals in the group, with the mean and variance defined as follows:

$$\mu = NP_{eff}, \qquad \sigma^2 = NP_{eff}(1-P_{eff}) \tag{1}$$

where, P_{eff} = Probability of effect, and N = Number of people in each receptor, susceptibility group, and health effect severity level

Thus, a binomial distribution is defined for (1) each receptor, (2) each susceptibility subpopulation at the receptor, and (3) each level of severity of health effect. For each scenario there are R×G×S such binomials, where R is the number of receptors, G is the number of susceptibility groups, and S is the number of severity levels. The direct convolution of so many binomials to derive the distribution for the total number of affected individuals may be time consuming. A normal approximation may be made to each binomial and the convolution distribution is then obtained simply as a normal with mean equal to the sum of the binomials' means and variance equal to the sum of the binomials' variances. For each scenario a normal is derived in this way for the total number of affected individuals (1) suffering each level of severity or higher, and (2) suffering any level of severity.

Each of these normals is discretized into a histogram, such as is shown in Figure 2, to facilitate aggregation over the scenarios and the final development of the aggregated histograms' associated risk profiles. As illustrated in the figure, the aggregation over the scenarios is carried out by adding, for each discrete interval of values of the number of affected individuals, the probabilities of occurrence of the interval in all the scenarios, weighted by the probabilities of occurrence of the scenarios. An aggregated histogram of each of the three kinds noted above then results. Its evolution to a corresponding risk profile is described in the next section. In Figure 2, the scenario occurrence probabilities are assumed to be .7 and .3. The aggregation of their two histograms is the histogram defined by the dashed curve.

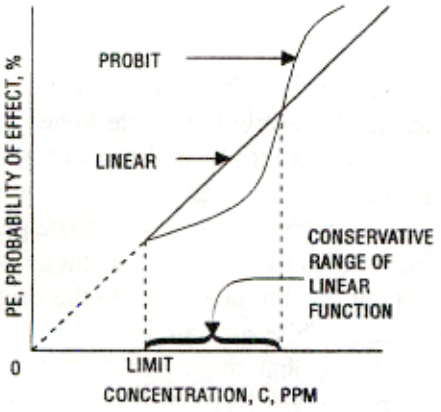


Figure 1. Illustration of Relation of Linear and Probit Exposure-Response Functions

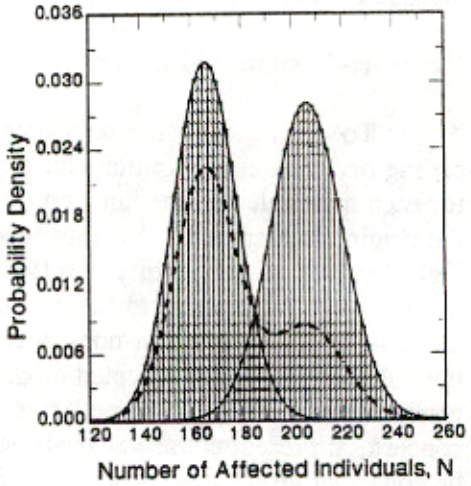


Figure 2. Example of Two Scenarios' Number of Affected Individuals Histograms and Their Aggregation

The convolution of all the binomial distributions to derive the distribution for the total number of affected individuals is completed by adding randomly drawn binomial deviates from all of the binomial distributions. The binomial distribution is integer valued, with j in Equation 2 taking possible values from 0 to n. It depends on two parameters, n and q. The expression for the binomial distribution is,

$$P(j) = \binom{j}{n} q^j (1-q)^{n-j} \qquad (2)$$

If the mean number of the variates is almost equal to the variance, then their distribution may reasonably be defined by the Poisson distribution. Poisson probabilities

are given by the following:

$$P(j) = \frac{\lambda^j e^{-\lambda}}{j!} \quad (3)$$

The mean of the Poisson distribution is $\mu=\lambda$. For each scenario, the total number of affected individuals, for each susceptibility group and health severity effect level, is the sum of the means over all receptors.

For each method used, each final distribution is discretized into a histogram to facilitate aggregation over the scenarios and the final development of the aggregated histograms' associated risk profiles.

Risk Profile Subroutine

A risk profile is the curve that delineates the probability of meeting or exceeding any given level of loss. A risk profile is developed from each aggregated histogram. Risk profile development begins with the maximum histogram interval N_m, with non-zero probability Q_m, and computes the sums, S_j, of the probabilities of all intervals greater or equal to each interval N_j in decreasing order. For each histogram interval, N_j (j=1 to m),

$$S_j = \sum_{i=j}^{m} Q_i \quad (4)$$

The monotonically non-increasing step function resulting from the above equation is plotted to form the risk profile. The risk profile for each HESL (mild, significant, and fatal) is computed and plotted for each population group and for the overall population.

DATA REQUIREMENTS

The user must specify the quantities and types of toxic materials (from a list of 129 chemicals) in each vessel in the facility under study. Other chemicals may be added.

Site specific meteorological data must be entered into RISTOX. This data should consist of observations over at least a one year period, and include wind direction, speed and associated Pasquill-Gifford stability class. Representative values for σ_θ (standard deviation of azimuth angle), and temperature, T, are also required. These observations are condensed into a suitable number of discrete weather conditions specified by wind direction, stability class and associated frequency of occurrence.

Population data should specify the number of people in the "sensitive" and "healthy adults" categories, who are subsequently distributed over four structures and in the open at each population center. The structural types are: (1) closed homes of modern construction, good insulation; (2) closed homes of older construction, poor insulation; (3) offices; and (4) warehouses/schools/hospitals. Each structure provides a dose reduction to the people inside the building. The sheltering effects model was developed from the information contained in References [3 and 4]. The model is defined as:

$$DRF = 1 - \frac{1}{Rt}(1-e^{-Rt}) \quad (5)$$

where, DRF = dose reduction factor, R = R (ΔT, γ, type structure), t = time of passage of cloud, minutes, Δ = inside temp. - outside temp., °F, γ = wind speed,mph.

RESULTS AND CONCLUSIONS

Figure 3 is an example of the type of results provided by RISTOX. Clearly, more information is provided to a risk manager than is available from a presentation of worst cast hazards. Once the data files have been generated, it is easy to determine the effect of various mitigations. For example, if a dehydration system is suggested to dry a gas, and therefore make it more buoyant, this mitigating effect can be considered by changing the parameters supplied to the gas dispersion model in RISTOX. The resulting risk profiles can then be quickly produced to assess the affect of the mitigation measure.

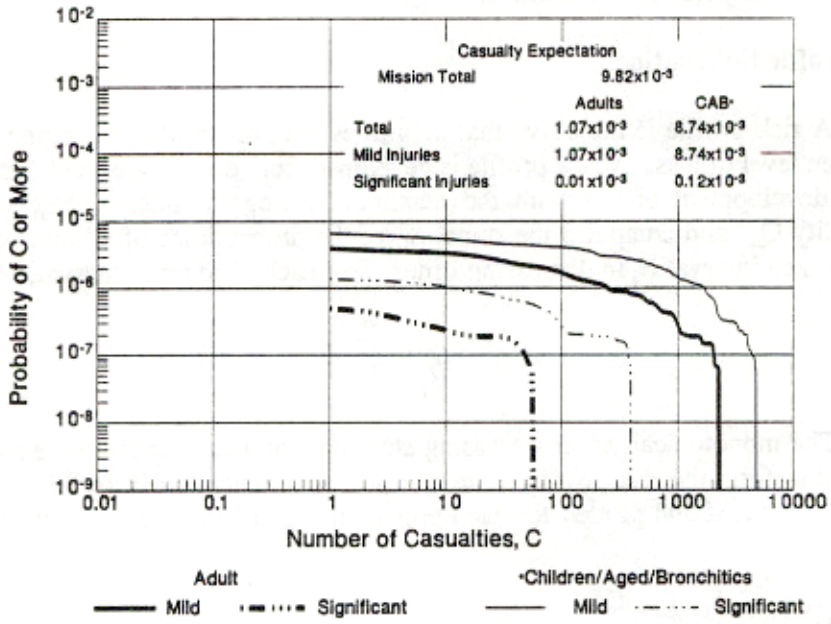


Figure 3. Representative RISTOX Risk Profile

Currently RISTOX is being modified to operate in a WINDOWS(tm) environment. In addition, several other gas dispersion models will be added to enable better computation of toxic concentrations close to the release site and to handle heavier than air gases.

REFERENCES

[1] Kunkel, B.A., AFTOX40 - The Air Force Toxic Chemical Dispersion Model - A User's Guide, Doc. No. PL-TR-91-2119, Phillips Lab. Directorate of Geophysics, Hanscom AFB, MA, 8 May 1991.

[2] Hagopian, John H., ARCHIE (Version 1.0) Program: Automated Resource for Chemical Hazard Incident Evaluation, Prepared for the FEMA, D.O.T., E.P.A., Arthur D. Little, Inc., 1989.

[3] Engleman, R.J., Effectiveness of Sheltering in Building and Vehicles for Plutonium, Rept. No. DOE/EH -0159T, Prep. for D.O.E., Asst. Sec., Envir., Safety & Health, Battelle, Pac. NW Lab., J, 1990.

[4] American Society of Heating, Refrigerating and Air Conditioning Engineers (ASHREA), Inc., Chapter 23, "Infiltration and Ventilation Modeling", Handbook of Fundamentals New York, 1989.

[5] See, A., J. Hudson, R. Nyman, and L. Philipson, LATRA - Launch Area Toxic Risk Analysis Prgrm., Rept. No. 93-282/36.3-01, Prep. for USAF/30&45SPW, ACTA, Inc., Torrance, CA, Sept. 1993.

[6] Nyman, R., Vandenberg Air Force Base Toxic Dispersion Models Support Activities, Report No. 92-265/18-01, Prep. for USAF/30&45SPW, ACTA, Inc., Torrance, CA, Sept. 1992.

[7] Hudson, J., et al., Risk to Prop. Bixby Ranch Project from Chevron Point Arguello Sour Gas Pipeline, Rept. No. 90-213/2, Prep. for Bixby Ranch Co., S. Barbara, CA; ACTA, Torr., CA, Oct. 1990.

CASE STUDY OF A QUANTITATIVE RISK ANALYSIS TO COMPARE PROCESS ALTERNATIVES

J. T. Cranefield[1], D. M. Karydas[1], P. A. Stavrianidis[1], V. Ley [2]

[1] Factory Mutual Research Corporation
1151 Boston-Providence Turnpike
Norwood, Massachusetts 02062

[2] Texas Instruments, Inc.
2623 National Circle
Garland, Texas 75041

ABSTRACT

A case study of a quantitative risk analysis to compare process alternatives is presented to demonstrate the utility of risk analysis for management decision support. The approach and results are presented and opportunities to increase the efficiency of the approach are discussed.

INTRODUCTION

The purpose of this paper is to illustrate, with a case study, the utility of risk analysis in supporting decision-making, to discuss constraints of risk analysis in terms of efficiency and resources, and to discuss potential improvements that will increase efficiency and reduce resource requirements.

Risk assessments are conducted in the process industries to assess risks associated with current process operations, to assess risks associated with new processes or proposed process modifications, and to provide engineering design input for new processes or proposed process modifications. Risk assessment techniques include qualitative, semi-quantitative and quantitative methods.

All techniques review processes systematically to determine potential accidents and assess the potential consequences of an accident. Engineered safeguards, designed to reduce the likelihood of an event or to mitigate accident consequences, are evaluated and improvements are recommended when appropriate.

Studies conducted with qualitative methods evaluate accident frequency and consequences subjectively based upon available data and experience[1]. This provides a

qualitative understanding of potential accidents and an awareness of existing safeguards. Studies conducted with semi-quantitative methods estimate and rank accident frequencies and consequences according to a ranking system. This method identifies process areas that represent significant or unacceptable risk, develops recommendations for reducing risk and identifies processes that require a more detailed study[2].

A quantitative method systematically identifies the likelihood and consequences of various accidents. This provides a vehicle to support decision making with respect to risk acceptability criteria, comparing process or safeguard alternatives, and developing alternatives for reducing risks[3].

Resource requirements increase significantly with increasing analysis complexity. It is desired to use risk evaluation resources efficiently and effectively to meet the project objective. This case study examines a quantitative risk analysis (QRA) conducted to compare the risks associated with two proposed process alternatives. The case study will discuss the methodology employed, conclusions, and additional information and resources that would improve the efficiency of future studies.

CASE STUDY

The management of a facility processing a highly toxic gaseous material desired to compare the risks associated with two alternative methods of supplying the material: 100% material at low pressure and 15% material in a carrier gas at high pressure. A quantitative risk analysis (QRA) was selected as the method that would most efficiently and effectively meet the project objective[4].

Facility Description

Gallium arsenide wafers are manufactured and processed by depositing thin layers of materials in epitaxial metallic-organic chemical vapor deposition (MOCVD) reactors. Process materials include arsine, hydrogen and metallic-organic sources. Hydrogen is stored in tube cylinders located outside the toxic gas room separated by a concrete block wall. Arsine is stored and supplied from cylinders located in the toxic gas room. Arsine is supplied as pure arsine or as a mixture with hydrogen. The mixture is 15% by volume arsine and 85% by volume hydrogen. The pure arsine is supplied in cylinders at 215 psi and the mixture is supplied at 1100 psi. The cylinders are received with 0.010 inch restricting flow orifices.

Process gases are distributed to the reactor via coaxial stainless steel tubing. The annular space is sealed and the pressure is monitored to reveal the presence of any leaks. Three epitaxial reactors operate under vacuum and elevated temperature. Reactor mass flow controllers and any other valves are located in the reactor cabinet. Vacuum is provided by vacuum pumps located adjacent to the epitaxial reactor cabinets. The exhaust line and the vacuum pump of each reactor are enclosed and exhausted separately.

The air handling system for the clean room is a recirculating system. Under emergency conditions, the system converts to 100% exhaust with a rate of 1 air change every 3 minutes. Air treatment prior to atmospheric discharge includes a controlled combustion, decomposition and oxidation (CDO) unit and a carbon bed adsorber to remove any unreacted arsine, silane or hydrogen.

Safety systems provided at this facility include coaxial tubing for arsine process gas lines, arsine monitoring and detection system, automatic gas shutoff valves, restricting flow orifice in arsine cylinders, excess flow valves on gas manifold in gas cabinet, emergency

exhaust system, controlled combustion, decomposition and oxidation unit (CDO) and a carbon bed adsorber.

Approach

The integrated risk analysis approach adopted for this study consists of hazard identification, evaluation of the likelihood of initiating events, modelling of accident scenarios and consequence analysis.

A hazard and operability (HAZOP) study was conducted to identify initiating events with the potential to release arsine at this facility. The HAZOP technique is a formalized, systematic method of evaluating process hazards. The technique systematically reviews a process and determines the consequences associated with deviations from normal operating parameters.

A key aspect of the hazard identification process is to reveal those events which could lead to an accident. For example, a leak from an arsine line is an initiating event in a series of accident scenarios that may or may not lead to a release of arsine to the environment. Initiating events identified in the HAZOP study include: release of arsine from a line, release of arsine from the arsine bottle, release of arsine from the bell jar reactor, and release of arsine from the stack. The probability of occurrence of each initiating event has been determined using fault tree analysis. Many input parameters are necessary for the models employed in this study, e.g., the probability of valve leakage, the probability of arsine line rupture, etc. The probabilities considered in this analysis were taken from failure rate data resources in the chemical, petroleum, utility and nuclear industries.

The effect of engineered safety systems (such as pressure relief valves, the controlled combustion, decomposition and oxidation system [CDO], etc.), the process state, and the location of process piping must also be considered regarding their influence of the rate, phase and duration of an arsine release. What emerges from this analysis is a comprehensive and representative spectrum of potential accident scenarios which can occur in the plant. The probability of occurrence of specific accident scenarios was determined using event tree analysis. This analysis considered the availability of applicable safety systems. This availability was determined by fault tree analysis of each specific safety system.

The consequences of various release scenarios were analyzed to determine the indoor and atmospheric dispersion of arsine. Each scenario results in different consequences and the consequences of releasing 100% arsine are compared to the consequences of releasing the 15% arsine and 85% hydrogen mixture.

Results

The risk profile for the use of 100% or 15% arsine was determined for potential arsine release points and the state of the process when the arsine release occurs. The two process states, "process on" and "process off", determine the amount of arsine available for release given the occurrence of an accident, . The "process on" state refers to a state that has the automatic shut-off valve on the manifold open, the valve on the gas bottle open and the arsine line either pressurized (mass flow controller closed) or arsine flowing through the line (MOCVD reactor operating). A release during this state may allow the release of arsine until the bottle contents are exhausted or the detection and isolation systems operate. The "process off" state refers to a state that has the automatic shut-off valve on the manifold closed, the valve on the gas bottle closed and the mass flow controller upstream of the MOCVD reactor closed. A release under this process state will allow only the arsine

trapped in the line to be released.

A total of 33 cases were identified. Each case accounts for the type of release (leak or rupture), location of the release point and the process state. Every case corresponds to an initiating event that may lead to potential accident scenarios. For example, a leak on the arsine line in the gas room is the initiating event. It may transition to several accident scenarios depending on the availability of the safety systems. Each accident scenario is identified by the probability of its occurrence and the consequences in terms of potential arsine concentration levels in the room of origin or to the atmosphere.

Results of the significant accident scenarios were evaluated for various initiating events. Consider for example, a leak of arsine in the gas room. Table 1 provides a result summary for this initiating event, including the probability of occurrence within one year, the probability of occurrence of each accident scenario within one year, the contribution of each accident scenario to the total probability of having an accident given the specific initiating event and the maximum arsine concentration in the room of origin.

Table 1. Results for Leak from an Arsine Line in Gas Room

Initiating Event: Leak from an Arsine Line in Gas Room (Process is "On")			
Description	Probability	% Arsine	Maximum Arsine Concentration in room [ppm]
No Release to Atmosphere	2.5×10^{-6}	100	56
		15	92
Small Release in Gas Room	3.9×10^{-8}	100	67
		15	110
Small Release to atmosphere	7.2×10^{-9}	100	56
		15	92

Figure 1 provides a risk profile for indoor releases of arsine that summarizes the likelihood and consequences for all releases. This figure shows the cumulative likelihood of occurrence in a year to have a specified arsine concentration indoors. Figure 2 provides a similar risk profile for the portion of the year when the process is operating. The risk associated with the use of 100% arsine, in terms of arsine concentration, is lower than with the use of 15% arsine when the plant is operating. A similar analysis shows that the risk associated with the use of 100% arsine is higher than with the use of 15% arsine when the plant is not operating .

CONCLUSIONS

Prior to this analysis, safety considerations for the process focused on either reducing the likelihood of an accident or minimizing potential consequences from a release but did not consider the integral risk from the release of hazardous material. The quantitative risk analysis provided a systematic, objective method for comparing two process alternatives, i.e., the use of 100% vs 15% arsine, and supported an objective decision-making process by risk management personnel.

This study was significantly impacted by the resources necessary to quantify the availability of the engineered safeguards, such as process control systems, emergency ventilation systems and toxic material detection systems, present at this facility. In addition, the analysis accuracy is influenced by the availability of reliability information for engineered safeguards. Reliability certification of safeguard systems would increase the objectivity and efficiency of the study by eliminating the need to quantify the safeguard system reliability by individual analysts constrained by limited data. In this case, the accuracy is considered sufficient because of the comparative nature of the study. The availability of safety systems are independent of the arsine supply and therefore, uncertainty in this portion of the analysis should not influence the comparison.

REFERENCES

1. Center for Chemical Process Safety of the American Institute of Chemical Engineers. "Guidelines for Hazard Evaluation, Second Edition with Worked Examples". 1992

2. M. L. Casada, J. Q. Kirkman and H. M. Paula, Facility risk review as an approach to prioritizing loss prevention efforts, *Plant/Operations Progress* Vol. 9, No. 4 (1990)

3. Center for Chemical Process Safety of the American Institute of Chemical Engineers. "Guidelines for Chemical Process Quantitative Risk Analysis", 1989.

4. J. T. Cranefield, D. M. Karydas, and P. A. Stavrianidis, Proprietary Report, Factory Mutual Research Corporation, May 1993.

Figure 1. Risk Curve for 15% and 100% Arsine

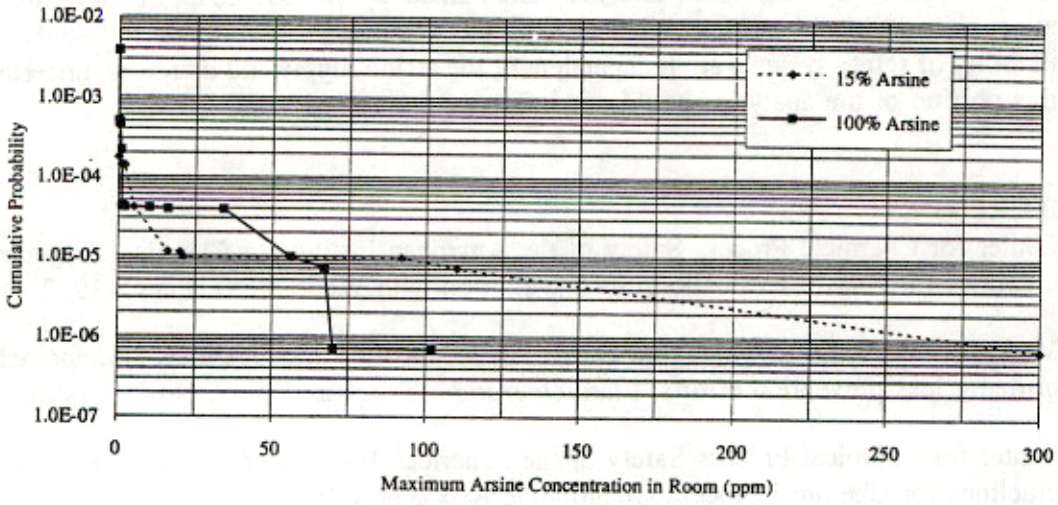
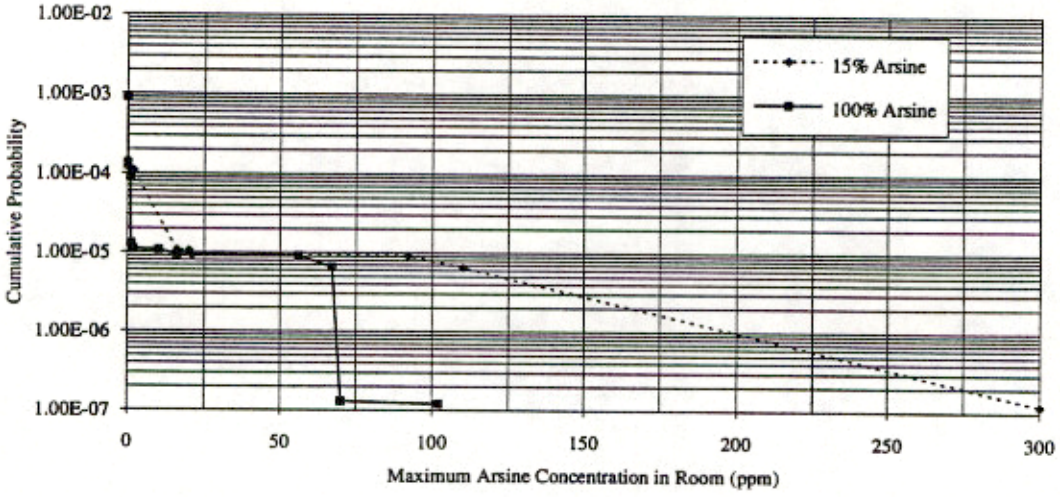


Figure 2. Risk Curves for 15% and 100% Arsine; Process ON



028 Risk Management in Operations

Chair: M. Stamatelatos, Scientech

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

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

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

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

ASSESSING THE RISK IMPACT OF INTEGRATING SURVEILLANCE TESTING AND MAINTENANCE

Curtis L. Smith, Phillip G. Ellison, John A. Schroeder

Idaho National Engineering Laboratory
EG&G Idaho, Inc.
Idaho Falls, Idaho 83415

INTRODUCTION

This paper describes research investigating the integration of surveillance testing with maintenance activities which may be used to achieve an overall risk reduction, reduce component and system unavailabilities, and improve risk-based plant technical specifications. The integration of surveillances research is being supported by the Department of Energy's Idaho National Engineering Laboratory. Additional detail may be found in the report *An Assessment of the Risk Impact of Integrating Surveillance Testing and Maintenance at Nuclear Power Plants*.[1] This research consists of three separate areas: (1) Identifying existing practices regarding the integration of surveillances and maintenance, (2) Identifying integration approaches that may reduce core damage risk or system unavailability, and (3) Identifying effective integration methods.

The integrated surveillance research activities have identified existing integration practices. A brief overview of these practices is presented in below. The integration of surveillances research has also investigated four integration methods. These four methods are covered by two general categories: (1) Concurrency of testing and maintenance and (2) Testing and maintenance interval manipulations.

The first category, concurrency of testing and maintenance, represents the situation where testing and maintenance are performed concurrently. This action will minimize component, train, or system outages. The second category, testing and maintenance interval modifications, represents the situation where testing or maintenance intervals are modified in order to minimize component, train, or system unavailability.

While the research project originally intended to investigate just the potential of concurrency in testing and maintenance, the issue of concurrency cannot be the sole focus for reducing plant risk. This is shown when performing concurrent testing and

maintenance. Concurrently scheduling tests and maintenance will lead to modifying the test or maintenance intervals for particular components. Consequently, this modification of the test or maintenance intervals then moves the analysis into the second category (i.e., interval modifications) discussed above.

FOUR SURVEILLANCE AND TESTING INTEGRATION METHODS

Four integration methods were investigated for the two categories discussed above. For testing and maintenance concurrency, two integration methods are:

1. Perform a historical analysis to identify improvements that influence test or maintenance concurrency.

   This method attempts to provide concurrent testing and maintenance by reviewing historical plant operational data. The historical data review may show scheduled tests or maintenance that could be moved to coincide with other scheduled test or maintenance procedures. This method allows for scheduled tests or maintenance to be moved to coincide with unscheduled maintenance.

2. Perform a predictive analysis to identify improvements that influence test or maintenance concurrency.

   This method attempts to provide concurrent testing and maintenance by predicting a schedule that includes concurrent scheduled tests and maintenance. An integrated schedule is predicted by evaluating current test and maintenance schedules to identify potential concurrency. This method allows tests or maintenance to be moved to coincide with unscheduled maintenance.

For testing and maintenance interval manipulations, two integration methods are:

3. Stagger testing and maintenance intervals to reduce overall system unavailability.

   This method attempts to stagger scheduled test and maintenance intervals. Staggering test or maintenance intervals can reduce overall system unavailability by two methods: (a) reducing the system fault-window (i.e., the length of time between tests during which the system could possibly be failed) and (b) reducing the probability of test-caused common-cause failures.

4. Modify (increase or decrease) testing and maintenance intervals to reduce overall system unavailability.

   This method attempts to modify (increase or decrease) test or maintenance intervals for components. A component's unavailability varies with the length of its test and maintenance interval, with a minimum unavailability somewhere between a very short interval and a very long interval.

OVERVIEW OF THE ANALYSIS

An example two-train auxiliary feedwater (AFW) system was used to assess the overall worth of the four integration methods. The overall worth of a particular integration

method could involve a reduction in system unavailability and may include the potential for (a) an increase in testing or maintenance efficiency, (b) an overall reduction in the frequency of testing or maintenance, (c) a reduction in the number of test- or maintenance-caused plant trips, and (d) an effective testing or maintenance schedule.

The analyses that were performed to determine the worth of the first two methods investigated several concurrency issues, including:

- The overall time during the year that scheduled testing and maintenance results in component outages
- The fraction of the system unavailability resulting from scheduled testing and maintenance compared to unavailability due to random failures and repair times
- The possible effect that concurrency may have on the probability of having test- or maintenance-caused errors
- The effect from increasing the tests and maintenance duration.

The analyses that were performed to determine the worth of the third and fourth methods investigated several issues, including:

- The variability of component and system unavailability when test and maintenance intervals are modified or staggered
- The possible effect that interval manipulations may have on the probability of having test- or maintenance-caused errors
- The fraction of the system unavailability resulting from scheduled testing and maintenance compared to unavailability due to random failures and repair times
- The effect from either over- or under-testing components
- The risk reduction from staggering while modifying test or maintenance intervals versus staggering or modifying intervals alone.

ANALYSIS RESULTS

Methods 3 and 4 provided measurable reductions in system unavailability and plant risk for the example plant. However, Methods 1 and 2 did not show either the potential to significantly reduce system unavailability or show the potential to be effectively implemented at the example plant. In general, the following statements are applicable for the example plant's AFW system:

- Methods 1 and 2 provided few benefits and did not prove practical to implement
- Methods 3 and 4 could provide significant benefits, especially when implemented in conjunction with each other.

Given the current restrictive, nonrisk-based technical specifications, few of the potential integration methods could effectively be implemented. The one method that could

possibly be applied under the current nonrisk-based technical specifications would be staggering of tests or maintenance (i.e., Method 3).

In general, Method 1 and Method 2 provided little benefit for the example plant's AFW system. Several reasons for the lack of benefit for these two methods have been identified.

- The actual overall time the example plant AFW components are out of service due to scheduled testing and maintenance is small. This outage is the time a component is out, and consequently, the system outage time due to testing and maintenance is even less than the component outage times (since no single component can fail the overall system).

- For the example AFW system, the portion of the overall system unavailability directly caused by test and preventive maintenance outages is on the order of 0.2%. This small portion of the system unavailability implies that test and preventive maintenance durations are not as important as the other unavailability contributors. Consequently, effort spent attempting to integrate surveillances using Methods 1 or 2 may not be worthwhile.

- Many of the tests require that the component be operable for the test, resulting in little or no downtime for the test.

- Some component surveillance testing may require that the component's associated train be operable. Consequently, if a component is found to be failed, causing its train to be disabled, the other components in the same train could not be tested since the train is inoperable.

- The example AFW system unavailability is somewhat insensitive to the average duration of a scheduled test or maintenance when the test or maintenance can be readily finished and the system returned to normal standby condition (i.e., the probability of overriding a test or maintenance is close to 1.0).

- If a surveillance test is performed early (for example, integrated with a corrective maintenance), the plant technical specifications may not allow for stretching the test interval until the next scheduled test. Thus, the test may be performed again on the next regularly scheduled test time, thereby possibly overtesting and *increasing* the system unavailability.

- Methods 1 and 2 could increase the potential for test- or maintenance-caused common-cause failures between components which are tested together, especially if the maintenance or testing personnel are in a high-stress situation due to an allowable outage time. The example AFW system model is sensitive to changes in the probability of test-caused failures; consequently, the time saved by performing tests while a train or system is down may be negated by the potential for increasing the chance of test- or maintenance-caused failures.

For the example AFW system model, Method 3 and Method 4 show some benefit in three primary areas: (a) a reduction in system risk and unavailability, (b) a reduction in the probability of having test- or maintenance-caused common-cause failures, and (c) a reduction in the frequency of test- or maintenance-caused plant trips. Several reasons exist for these benefits.

- Staggered testing reduces the system fault window (i.e., the time interval between tests for one of the redundant trains) and also has the potential to reduce the component test- or maintenance-caused common-cause failure probability since the tests or maintenance are not performed consecutively.

- Staggered testing alone does not generally provide the best integration strategy, but when coupled with modification of intervals (i.e., Method 4), the resulting test and maintenance schedule could provide a reduction in the system unavailability.

- A combination of Methods 3 and 4 may keep the system unavailability constant while reducing the testing frequency (since test intervals can usually be increased if a component is currently overtested or if staggered testing is not currently used).

- The plant risk at shutdown could potentially be reduced by combining Methods 3 and 4 if the methods allowed shutdown tests or maintenance to be moved to full power operation. This movement of tests and maintenance could reduce the system unavailability during shutdown (since fewer test and maintenance outage times will occur during shutdown), thereby potentially reducing the plant shutdown risk. The shutdown tests and maintenance that are moved to full power may be scheduled, using Methods 3 and 4, such that the change in system unavailability is negligible.

- A secondary issue to moving testing and maintenance out of the shutdown mode via Methods 3 and 4 has also been identified. This issue is that the test and maintenance may be performed under less stress while at power, thereby possibly reducing the probability of test- or maintenance-caused failures.

- Implementation of Method 4, by itself, has the potential for significantly changing system unavailability. Testing components too often or not often enough can result in a high system unavailability. But current technical specifications do not allow much leverage in moving surveillance test intervals.

CONCLUSIONS

Of the four potential integration methods, only Method 3 (staggering tests or maintenance) and Method 4 (modifying tests or maintenance intervals) demonstrated a potential benefit for integrating surveillances with maintenance. This benefit was best demonstrated when Method 3 and Method 4 were used in conjunction with each other. When the two methods are used together, they could yield benefits from three separate areas, namely:

- A reduction in system risk and unavailability

- A reduction in the probability of having test- or maintenance-caused common-cause failures

- A reduction in the frequency of test- or maintenance-caused plant trips.

Not included above is the possibility that reduced testing and maintenance will conserve plant resources that may be used to further increase plant safety by other means. But evaluating the potential safety increase through conserving plant resources is beyond the scope of the analysis and no attempt was made to quantify the potential benefits.

028 - 6

Method 1 (historical concurrency analysis) and Method 2 (predictive concurrency analysis) did not show either the potential to significantly reduce system unavailability or show the potential to be effectively implemented as a pilot program at the example plant.

Given the current restrictive, nonrisk-based technical specifications, few of the potential integration methods could be effectively implemented in practice (although staggered testing could be applied). Changes to technical specifications or implementation of risk-based technical specifications could present the opportunity for implementing one or more of the four potential integration methods.

Significant changes to surveillance testing may entail obtaining an amendment to the plant's operating license. While scheduled preventive maintenance is not directly addressed by 10 CFR 50.36, preventive maintenance schedules may be tied to surveillance testing intervals for a particular plant. Consequently, significant changes in preventive maintenance schedules may involve similar issues related to changes in surveillance testing. Also, since the technical specification requirements are proposed during the licensing phase of the plant, detailed risk-based considerations may not be incorporated into the requirements. In general, if changes to technical specification-controlled test or maintenance intervals are to be made, the technical specifications should be modified to allow for flexibility.

Risk-based technical specifications have recently been a focus of investigation within the nuclear industry. Assuming risk-based technical specifications are incorporated in either current or new plants, modifications of surveillance testing and maintenance intervals may be possible for these plants. Although current surveillance testing was designed to improve plant safety by ensuring that standby systems are available during off-normal conditions, overtesting may actually reduce plant safety through several mechanisms, including (a) reduced personnel efficiency due to workload or technical specification testing priorities, (b) accelerated wear on overly tested equipment, (c) reducing component availability, and (d) the potential for an increased number of test-caused transients. Consequently, to improve plant safety, surveillance testing and maintenance may need to be integrated using Methods 3 and 4 in conjunction with risk-based technical specifications.

This work was supported by the U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Under DOE Idaho Field Office Contract DE-AC07-76ID01570. This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights. The views expressed in this report are not necessarily those of the U.S. Nuclear Regulatory Commission.

REFERENCES

1. Curtis L. Smith, Phillip G. Ellison, and John A. Schroeder, *An Assessment of the Risk Impact of Integrating Surveillance Testing and Maintenance at Nuclear Power Plants*, NUREG/CR-5992.

EMPIRICAL BAYES ESTIMATION OF THE AVERAGE RELIABILITY OF NUCLEAR POWER PLANT EMERGENCY DIESEL GENERATORS TO LOAD-RUN UPON DEMAND

Harry F. Martz,[1] Lee R. Abramson[2]

[1]Los Alamos National Laboratory
Los Alamos, NM 87545
[2]US Nuclear Regulatory Commission
Washington, DC 20555

INTRODUCTION

If offsite power is interrupted, the availability of onsite alternating current power supplies is a major factor in assuring acceptable safety at commercial light-water-cooled nuclear power plants. To control the risk of severe core damage during station blackout accidents at a given plant, the reliability of the emergency diesel generators (EDGs) to load-run upon demand must be maintained at a sufficiently high level. The minimum EDG reliability is targeted at either 0.95 or 0.975 per nuclear unit consistent with the reliability level that the plant operator assumed in the coping analysis for station blackout. Because the reliability of the EDGs is critical to safety, it is important to estimate this reliability as accurately as possible. We are also interested in comparing the estimates to the target reliability values.

In soliciting public comment on the target reliability levels, the US Nuclear Regulatory Commission (NRC) asked the following question [SECY-93-044 (1993)]: Is there a method which could utilize industry-wide EDG performance experience to estimate EDG reliability, while providing adequate reliability degradation information for plant specific use? As we shall see, empirical Bayes (EB) is one such method; thus, the answer to the question is affirmative.

Denote the probability that an EDG successfully load-runs on a given demand d as p_d, which we refer to as the *time-dependent (or demand-dependent) EDG load-run reliability*. We are interested here in estimating the average value of p_d over time and station, the so-called *time-and-station average (or, simply, average) EDG load-run demand reliability*, which we denote by $\bar{p}$. Martz(1993) also considers EB estimation of p_d.

EDG reliability data for 63 US commercial nuclear power plant stations have recently been collected and summarized by the Institute of Nuclear Power Operations (INPO) and made available to the Nuclear Management and Resources Council (NUMARC). Among other things, this data presents the total number of EDG load-run demands and failures for each of the 63 stations for the four-year period 1988-1991. For this period, the total number of station EDG load-run demands ranges between 65 and 1120, with a mean of 310. We use this data for estimating $\bar{p}$.

EMPIRICAL BAYES ESTIMATION

EB methods are appropriate for use in inference situations where a parameter, such as $\bar{p}$, cannot be assumed to be constant over a corresponding population of interest (the population of stations). Rather, EB methods are appropriate when $\bar{p}$ is *not* constant but varies unpredictably (thus randomly) across the population according to some unknown prior distribution [Maritz and Lwin (1989); Martz and Waller (1991)].

Although the distribution of $\bar{p}$ is labeled the "prior distribution", EB must not be confused with, and indeed differs markedly in philosophy from, Bayesian statistics [Press (1989)] The notion of probability embodied in the EB prior distribution is that of relative frequency, while the notion of probability used in Bayesian statistics is that of degree-of-belief (subjective probability). For this reason, EB prior distributions are sometimes also referred to as *population variability* distributions because they express the variation (in a relative frequency sense) in a parameter of interest over a corresponding population. In order to emphasize this important distinction, we will refer to such priors as *EB prior distributions*.

Now consider the sampling (data) structure required in the next section. We have NUMARC data from N = 63 stations in which, for the *ith* station, x_i successful load-run starts have been observed in n_i load-run demands. Further, let $\bar{p}_i$ denote the unknown (true) value of $\bar{p}$ for the *ith* station. Further, assume that (1) the x_i values are statistically independent of each other conditional on $\bar{p}_i$ and (2) the underlying sequence of values $\bar{p}_1$, $\bar{p}_2$, ..., $\bar{p}_N$ are independent realizations of $\bar{p}$ from the common (but unknown) EB prior distribution $g(\bar{p})$. In this case, we say that the sequence of $\bar{p}_i$ values are *exchangeable* [that is, the order of the situations (or subscripts) is immaterial and may be arbitrarily assigned]. For the NUMARC data, we assume that x_i, given $\bar{p}_i$, has a binomial distribution. Let $\hat{\bar{p}}_i$ denote the usual maximum likelihood (ML) estimate of $\bar{p}_i$ given by $\hat{\bar{p}}_i = x_i/n_i$.

In order to apply EB methods, we must determine an appropriate EB prior distribution. To do this here, we will adopt the well-known *parametric* EB method which uses the marginal distribution $P(\hat{\bar{p}}_i)$ of $\hat{\bar{p}}_i$ to determine $g(\bar{p})$. We consider a beta EB prior distribution for $g(\bar{p})$ and, using the data, backsolve for the required EB beta prior distribution hyperparameters a and b which would, on average, produce the first two observed (sample) moments of $P(\hat{\bar{p}}_i)$. This procedure is known in statistics as the *method-of-moments*.

The EB estimation process we consider has six basic steps:

Step 1: Test the hypothesis that $\bar{p}$ is constant over the station population. If the hypothesis is rejected, then go to Step 3.

Step 2: If the hypothesis in Step 1 is accepted, then directly combine (pool) all the NUMARC data and use classical (non-EB) statistical methods to calculate the desired estimate of $\bar{p}$.

Step 3: Use the data to determine an EB beta prior distribution.

Step 4: Test the hypothesis that $\bar{p}$ has the EB beta prior distribution calculated in Step 3. If the beta hypothesis is accepted, then go to Step 6.

Step 5: If the beta hypothesis in Step 4 is rejected, then consider using either a different prior family or nonparametric EB methods for the desired EB estimates [see Martz and Waller (1991)].

Step 6: Calculate the desired EB estimates from the corresponding EB beta posterior distribution obtained using Bayes' theorem.

Note that these six steps utilize both sampling theory and EB methods. Box (1984) refers to these methods as *model criticism* (or *model validation*) and *estimation*, respectively, and argues that *both* methods together form an integral foundation for statistical inference.

EB ESTIMATION OF $\bar{p}$

The EB estimation process will now be applied using the NUMARC data to estimate the time-and-station average EDG load-run reliability $\bar{p}$. We statistically test the hypothesis that $\bar{p}$ is constant over the 63 stations. Because we reject this hypothesis, we then use EB methods to construct an appropriate EB beta prior distribution. We then test the hypothesis that an EB beta prior is appropriate for this data. Because we accept this hypothesis, we then use this EB beta prior and the NUMARC data to construct both point and interval estimates of $\bar{p}_i$ for each of the 63 stations.

Step 1: Testing the Hypothesis of Constant $\bar{p}$

We first use the NUMARC data to statistically test the hypothesis that $\bar{p}$ is constant over the 63 stations. That is, we test

$$H_0: \bar{p}_i = \bar{p}_j \text{ for all values of i and j}$$
$$H_1: \bar{p}_i \neq \bar{p}_j \text{ for some value of i and j .}$$

This hypothesis is easily tested using either the usual Pearson chi-square or likelihood ratio chi-square test statistic. The Pearson chi-square statistic has a value of 121 and the likelihood ratio chi-square statistic has a value of 137, both with 62 degrees of freedom. The corresponding p-values are quite small and indicate that all 63 stations are extremely unlikely to have the same $\bar{p}$ value. An important consequence of this is that the data may be directly combined over all stations if *only* a point estimate of the industry-wide time-and-station average EDG reliability is desired. In this case, the point estimate based on 19,338 successes in 19,520 load-run demands is 0.991. However, because of variation in the $\bar{p}$ values over the stations, direct combination of the data would produce a corresponding confidence interval which would be too narrow for the desired coverage. In our case, a 90% two-sided confidence interval estimate computed using the combined data is [0.990, 0.992]. What are the point and interval estimates based on the combined data actually estimating? These are both estimating the *mean* of the EB prior distribution. In order to calculate interval estimates which reflect the inherent variation in $\bar{p}$ over the 63 stations and which have the proper coverage, EB methods should be used. Because we reject the hypothesis of constant $\bar{p}$ for the 63 stations, we now proceed to Step 3.

Step 3: Constructing an EB Beta Prior on $\bar{p}$

Using the method-of-moments procedure described above, Martz and Waller (1991) present "weighted" estimators for the two beta distribution hyperparameters a and b. These estimates here are computed to be $\hat{a} = 330.110$ and $\hat{b} = 3.10684$. Note that the EB prior mean is 0.991, which is the industry-wide reliability estimate presented above. The 0.99, .95, .50, .05, and .01 quantiles of this EB beta prior are 0.9986, .9974, .9916, .9807, and .9744, respectively. The symmetric 90% two-sided EB credibility interval on $\bar{p}$ is [0.981, 0.997], and it is this interval which properly accounts for the station-to-station variability in $\bar{p}$.

Step 4: Testing the Hypothesis of an EB Beta Prior on $\bar{p}$

We test the assumption that the EB prior distribution on $\bar{p}$ is a Beta($\bar{p}$; 330.110, 3.10684) distribution. Martz(1993) describes an approximate goodness-of-fit test procedure based on the Kolomogorov-Smirnov (KS) single-sample two-sided statistic that we use here to test the null hypothesis

H_0: The EB prior distribution on $\bar{p}$ is a Beta($\bar{p}$; 330.110, 3.10684) distribution
versus
H_1: The EB prior distribution on $\bar{p}$ is <u>not</u> a Beta($\bar{p}$; 330.110, 3.10684) distribution.

Following the Martz(1993) procedure, the KS statistic was calculated to have a value of 0.08817 with a corresponding p-value of 0.73. Because H_0 cannot be rejected for any significance level less than this p-value, we look for large KS p-values. Because this is a large p-value, the hypothesis of an Beta($\overline{p}$; 330.110, 3.10684) EB prior distribution is supported by the data based on this approximate KS test procedure.

As discussed in Martz(1993), this is only an approximate test because the beta hyperparameter estimates are treated as though they have not been estimated from the data when in fact they have. Thus, when using this test, we will accept H_0 more often than we should. Thus, the size of the test (the probability of rejecting H_0 when it is true) will be smaller than desired, and the p-value for the exact test (the so-called "true" p-value) will be less than 0.73. The critical question is: How much less than 0.73 is the true p-value? We used Monte Carlo simulation to answer this question. Based on 10,000 replications, we actually observed 45% of the KS statistics to be greater than 0.08817. This is still an acceptably large percentage; thus, we accept the EB beta prior hypothesis. We now proceed to Step 6.

Step 6: Calculation of the EB Estimates of $\overline{p}_i$

Given x_i successes in n_i demands, the corresponding EB posterior distribution of $\overline{p}_i$ is a Beta($\overline{p}_i$; $\hat{a} + x_i$, $\hat{b} + n_i - x_i$) distribution. The usual EB point estimator of $\overline{p}_i$ is the posterior mean given by $(\hat{a} + x_i)/(\hat{a} + \hat{b} + n_i)$. This EB estimator is a so-called *shrinkage* estimator because it "shrinks" the ML estimator $\hat{\overline{p}}_i$ towards the prior mean. For example, for the first station in which $x_1 = 843$ and $n_1 = 854$, $\hat{\overline{p}}_1 = 0.987$, and the corresponding EB estimate of $\overline{p}_1$ is 0.988. Recall that the prior mean is 0.991.

Both the ML and the EB estimates of $\overline{p}$ for each station are plotted in Figure 1 along with the prior mean. Both target reliability levels are also shown. Notice also that it is impossible for an EB estimate to equal 1.0; thus, the EB method automatically removes the optimism inherent in the ML estimates for the case in which no failures are observed.

A symmetric two-sided 100(1 - α)% EB *credibility interval* on $\overline{p}_i$, denoted by ($\overline{p}_{i*}$, $\overline{p}_i^*$), may be obtained by individually solving the two equations given by

$$I(\overline{p}_{i*}; \hat{a} + x_i, \hat{b} + n_i - x_i) = \alpha/2$$
$$I(\overline{p}_i^*; \hat{a} + x_i, \hat{b} + n_i - x_i) = 1 - \alpha/2, \qquad (1)$$

respectively, where I(z;u,v) is the usual standard incomplete beta function ratio.

For example, consider the first station in which $x_1 = 843$ and $n_1 = 854$. For $\alpha = 0.1$, the corresponding two-sided 90% credibility interval on $\overline{p}_1$ is calculated to be (0.983, 0.993), which is plotted in Figure 1. Similarly, the corresponding 90% credibility limits for all the remaining stations are also shown in Figure 1. Note that the upper credibility limit will always be less than 1.0 regardless of the value of α. Thus, in spite of the fact that 22% of the ML estimates are 1.0, the EB procedure effectively tells us that an estimate of 1.0 is an overly optimistic estimate, which, of course, it is.

The EB posterior probability that the *ith* station meets the target reliability of 0.975 is given by 1.0 - I(0.975; $\hat{a} + x_i$, $\hat{b} + n_i - x_i$). This probability is plotted in Figure 2 for each station. The probabilities are all large and, with the exception of stations 4, 21, 33, and 36, all exceed 95%. Also, the probability is at least 0.9999 that each station meets the lower target reliability of 0.95.

Martz(1993) also considers the Bayes risk of both the ML and EB point estimators. The EB estimates have estimated Bayes risks which are all between a factor slightly less than 2 to a factor of 5 smaller than those of the corresponding ML estimates.

CONCLUSIONS

Methods of EB estimation are used here to estimate the average reliability of EDGs to load-run upon demand for the NUMARC station population. EB methods have less subjectivity and are more "data-driven" than pure Bayesian methods; thus, they are more defensible in PRA practice. Also, the critical EB assumptions are statistically examined and verified as part of the procedure. The EB estimates are superior to the usual ML estimates in the sense that they have smaller estimated Bayes risks than the ML estimates. In addition, the EB procedure removes the optimism inherent in the ML estimates in those cases in which no failures are observed. Also, the EB procedure "shrinks" the ML estimates toward the prior mean, thus effectively removing (or reducing) outliers in the population.

EB estimation methods can likewise be used to estimate the reliability (or the failure rate) of similar components/subsystems/systems for which the underlying reliability (or failure rate) is not constant across an appropriate population of interest (such as the station population considered here). Finally, although not considered here, both pure Bayesian and hierarchical Bayes methods [see Berger (1985)] can also be used to estimate EDG average load-run reliability.

ACKNOWLEDGMENTS

This work was supported by the US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, under contract FIN L1836-3 at Los Alamos National Laboratory. We gratefully acknowledge this support. We also thank Dr. Richard Beckman and Mr. Gary Tietjen, Los Alamos National Laboratory, for their assistance with the KS goodness-of-fit test procedure.

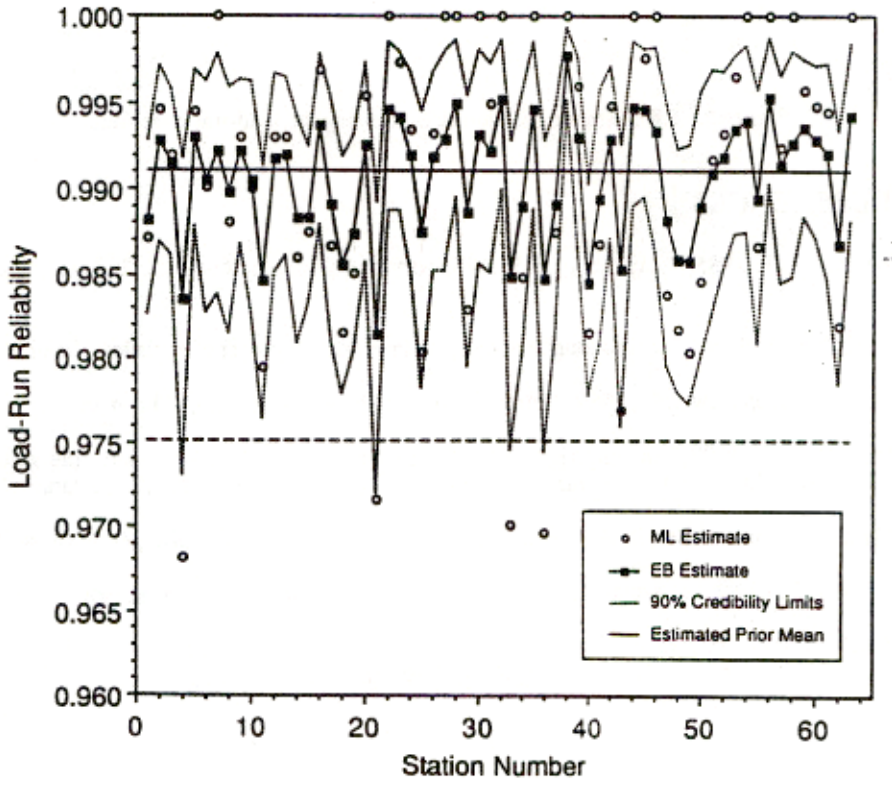


Figure 1. ML and EB estimates of the average EDG reliability to load-run upon demand.

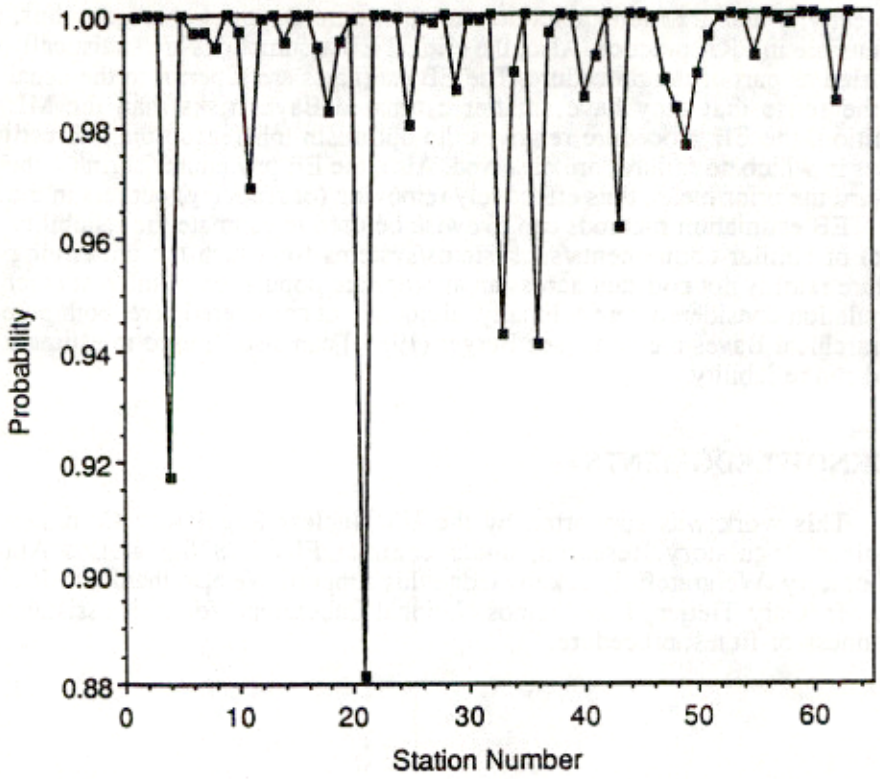


Figure 2. EB posterior probability of meeting the load-run target reliability of 0.975.

REFERENCES

Berger, J. O., 1985, "Statistical Decision Theory and Bayesian Analysis (*2nd* ed.)," Springer-Verlag, New York.

Box, G. E. P., 1984, The importance of practice in the development of statistics, *Technometrics* 26:1.

Maritz, J. S. and Lwin, T., 1989, "Empirical Bayes Methods (*2nd* ed.)," Chapman and Hall, London.

Martz, H. F., 1993, An empirical Bayes analysis of nuclear power plant emergency diesel generator reliability, *Los Alamos National Laboratory Report* LA-UR-93-800, Los Alamos, New Mexico.

Martz, H. F. and Waller, R. A., 1991, "Bayesian Reliability Analysis," Krieger, Malabar, Florida.

Press, S. J., 1989, "Bayesian Statistics: Principles, Models, and Applications," John Wiley, New York.

SECY-93-044, 1993, Resolution of generic safety issue B-56, 'diesel generator reliability', *Staff Report to the US Nuclear Regulatory Commission*, Washington, DC.

ANALYSES OF RELIABILITY CHARACTERISTICS OF AN EMERGENCY DIESEL GENERATOR POPULATION USING EMPIRICAL BAYES METHODS[1]

W.E. Vesely†, S.P. Uryas'ev*, and P.K. Samanta*

†Science Applications International Corporation
Dublin, Ohio 43017

*Brookhaven National Laboratory, Upton, New York 11973

INTRODUCTION

Emergency Diesel Generators (EDGs) provide backup power to nuclear power plants in case of failure of the AC buses. The reliability of EDGs is important to assure response to loss-of-offsite power accident scenarios, a dominant contributor to plant risk. The reliable performance of EDGs has been of concern both for regulators and plant operators. EDG failure data are routinely collected to understand the EDG reliability characteristics. In this paper, we present an approach to, and a demonstrative analysis of failure data from a large population of EDGs. The focus of the analysis is to:

- obtain reliability characteristics of individual, groups, and the entire population of EDGs;
- identify the percentage of EDG whose reliability is below certain value or unsatisfactory compared to others (outliers);
- obtain necessary statistical information (distributions, moments) for use in probabilistic safety assessment (PSA) studies;
- provide a method for routine analysis of EDG reliability data to understand any trends so that corrective measures can be identified.

We used the empirical Bayes approach to obtain both the population distribution and the individual failure probabilities from EDGs failure to start and load-run data; the survey covered four years and encompassed 195 EDGs at 63 plant sites[1].

METHODOLOGY

The available data on diesel failures consist of the number of demands, n_i, and number of failures, f_i, per year for each diesel $i = 1, \ldots, I$, $I = 195$. The number of demands and the number of failures are also summed over the individual diesels in a power plant to obtain

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

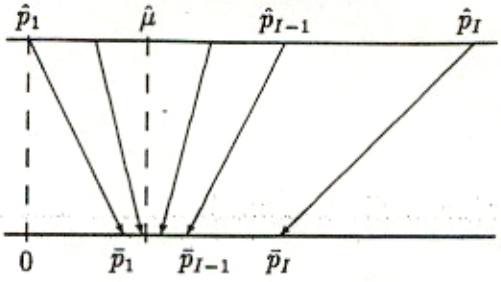


Figure 1: The Copas estimator.

station statistics. The data are divided into the numbers of failures to start and numbers of failures to load-run and the associated numbers of demands. It is supposed that each diesel has failure probability p_i and failures of the diesel follow the binomial distribution with parameters (p_i, n_i). The failure probabilities are estimated independently for failure to start and load-run tests. In using the empirical Bayes approach, each diesel failure probability p_i is treated as being a sample value from an underlying population distribution. The observed number of diesel failures for a given number of demands provides information not only on individual diesel failure probability p_i, but also on the characteristics of the underlying failure probability distribution.

For a set of failure data, such as diesel data, it is known that empirical Bayes approaches provide individual and population estimates which have desirable statistical properties (see, for example[2, 3, 4]). Shultis et al.[5] compared different empirical Bayes methods. These methods are efficient when there are not enough component-specific failure data to be used as the sole source to estimate the unreliability of the individual components, and the population of the component can be considered to obtain the component specific estimates. For example, Jänkälä and Vaurio[6] used empirical Bayes methods to estimate the common-cause failure rates of redundant equipment. This estimates have minimum mean-square errors and outperform the simple failure probability estimates constructed from the number of failures divided by number of demands.

Copas Estimator

Martz and Lian[7] evaluated nine empirical Bayes estimators for the binomial parameter p_i and concluded that the estimator proposed by Copas[8] has one of the best mean-square error over a wide range of the parameters. This estimator is optimal in a min-max sense, and does not preimpose specific distribution for values p_i, while many other empirical Bayes estimators consider some specified population distribution. Copas's estimator only assumes that the distribution has known mean and variance parameters. Since the exact values of these parameters are not available, some estimates must be used to construct the Copas estimator. Denote by $\hat{\mu}$ and $\hat{\sigma}^2$ estimates of mean and variance parameters, respectively. The Copas estimate $\bar{p}_i$ of individual diesel failure probability is an optimally weighted average of simple individual diesel failure probability estimate $\hat{p}_i = \frac{f_i}{n_i}$, and the average failure probability estimate for total population $\hat{\mu}$, i.e.,

$$\bar{p}_i = \frac{1}{1+w_i}\hat{p}_i + \frac{w_i}{1+w_i}\hat{\mu}, \qquad w_i = \frac{\hat{\mu}(1-\hat{\mu}) - \hat{\sigma}^2}{n_i\hat{\sigma}^2}. \tag{1}$$

The weighting coefficient w_i is obtained through estimates of mean $\hat{\mu}$ and variance $\hat{\sigma}^2$. The Copas estimator (1) shrinks the simple estimate $\hat{p}_i$ toward the estimate of the average $\hat{\mu}$ with shrinking parameter w_i (see Figure 1). It produces a nonzero estimate for $\bar{p}_i$, even if the number of failures for diesel i equals zero, i.e., $\hat{p}_i = 0$. The proper choice of the mean $\hat{\mu}$ and variance $\hat{\sigma}^2$ estimates is important, because they define the shrinking parameter w_i.

Originally, Copas[8] used the following estimate for the mean

$$\hat{\mu}_{cop} = \frac{1}{I}\sum_{i=1}^{I}\hat{p}_i \,, \tag{2}$$

and variance

$$\hat{\sigma}^2_{cop} = \frac{1}{I-k}\left\{\sum_{i=1}^{I}(\hat{p}_i-\hat{\mu})^2 - k\hat{\mu}(1-\hat{\mu})\right\}, \quad k=\sum_{i=1}^{I}\frac{1}{n_i}. \tag{3}$$

Estimates (2) and (3) are unbiased. A potential problem with estimate (3) of the variance is that it can be negative. If so, then $\hat{\sigma}^2_{cop}$ is set to zero with interpretation that there are no significant differences among the underlying failure probabilities.

Shultis et al.[5] identified a modified variance estimate which is similar to estimate (3) but which did not become negative. This modified estimate of variance is calculated using the formula

$$\hat{\sigma}^2_m = \frac{1}{I-1}\sum_{i=1}^{I}(\hat{p}_i-\hat{\mu})^2 \,, \tag{4}$$

to give, simply, the variance of the simple failure probability estimates.

Comparison of Predicted and Actual Diesel Failure Statistics

Assuming values for individual diesel failure probabilities p_i failure statistics can be predicted and can be compared to the actual statistics n_i and f_i. This comparison can be used to check the goodness of fit of estimated values for p_i. These comparisons can also be used to refine the estimates of p_i to minimize the discrepancy between the predicted and actual statistics.

Considering a binomial distribution with parameters (p_i, n_i) for diesel i, the probabilities of ratios of failures to trials $\frac{0}{n_i}$, $\frac{1}{n_i}$, $\frac{2}{n_i}$, ..., respectively, equal

$$(1-p_i)^{n_i}, \quad \binom{n_i}{1}p_i^1(1-p_i)^{n_i-1}, \quad \binom{n_i}{2}p_i^2(1-p_i)^{n_i-2}, \ \ldots$$

Thus, the probabilities of the ratios of the number of failures to the number of trials are known if the failure probabilities are available.

With known values for the failure probabilities, it is possible to construct predicted, expected values of the ratios of failures to trials. Let us split the interval $[0,1]$ on M subintervals U_m, with $U_m = (\frac{m-1}{M}, \frac{m}{M})$, $m = 1,\ldots,M$, where $M = 400$ in our calculations. The total (summarized over population of diesels) expected value of the discrete points (the ratios of failures to trials) in the interval U_m equals

$$b_m = \frac{1}{I}\sum_{i=1}^{I}\sum_{\frac{l}{n_i}\in U_m}\binom{n_i}{l}p_i^l(1-p_i)^{n_i-l} \,. \tag{5}$$

As discussed, the Copas estimator depends upon mean and variance parameters in formula (1); therefore p_i can be substituted with $\bar{p}_i(\hat{\mu},\hat{\sigma}^2)$ to obtain

$$b_m(\hat{\mu},\hat{\sigma}^2) = \frac{1}{I}\sum_{i=1}^{I}\sum_{\frac{l}{n_i}\in U_m}\binom{n_i}{l}\bar{p}_i^l(\hat{\mu},\hat{\sigma}^2)(1-\bar{p}_i(\hat{\mu},\hat{\sigma}^2))^{n_i-l} \,. \tag{6}$$

The predicted statistics of ratios of number of start failures to number of trials with Copas estimator for individual diesels is presented graphically in Figure 2 (black bars). As observed, there is a good correspondence between actual data and predicted values.

According to formula (6), the predicted values depend upon two parameters, $\hat{\mu}$, $\hat{\sigma}^2$, and it is possible to further adjust these parameters by best fitting the predicted and actual data values. Let us denote the values for the actual data by

$$b_m^{data}, \quad m = 1,\ldots,20 \,.$$

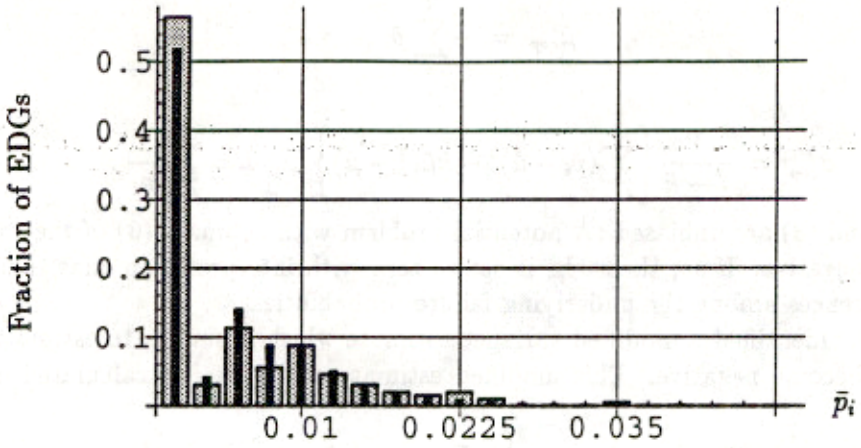


Figure 2: Histogram of real data and predicted simple failure to start probabilities for individual diesels (gray bars = real data, black bars = predicted)

The sum of squares between the predicted and actual values is

$$F(\hat{\mu}, \hat{\sigma}^2) = \sum_{m=1}^{20} \left(b_m^{data} - b_m(\hat{\mu}, \hat{\sigma}^2) \right)^2 .$$

We can adjust the parameters $\hat{\mu}$, $\hat{\sigma}^2$ by minimizing $F(\hat{\mu}, \hat{\sigma}^2)$ with respect to these parameters

$$F(\hat{\mu}, \hat{\sigma}^2) \rightarrow \min_{\hat{\mu}, \hat{\sigma}^2} .$$

We will call parameters obtained from such procedure a "matching histogram" approach.

SUMMARY OF RESULTS

Estimates of individual diesel failure probabilities and station diesel failure probabilities for a given plant are obtained with formula (1). As an example, a histogram of the load-run failure probability estimates for individual diesels is plotted on a logarithmic scale in Figure 3. The distributions of start and load-run failure probabilities that were observed for individual diesels and stations were used to:

- Estimate the mean, variance, and standard deviations of diesel failure probabilities. Table 1 presents the results for individual diesels. Table 2 presents the results for stations;
- Identify the percentage of the diesels having failure probabilities on the tails of the distribution;
- Identify the percentage of diesels with specified failure probability characteristics (for example, with reliability less then 95 %);
- Fit the population of individual diesel failure probabilities or station failure probabilities with parametric distributions (beta, lognormal) for PRA applications. The parameters of these distributions were obtained by matching moments, by equating the mean and variance of the estimated distribution to those of the parametric distribution.

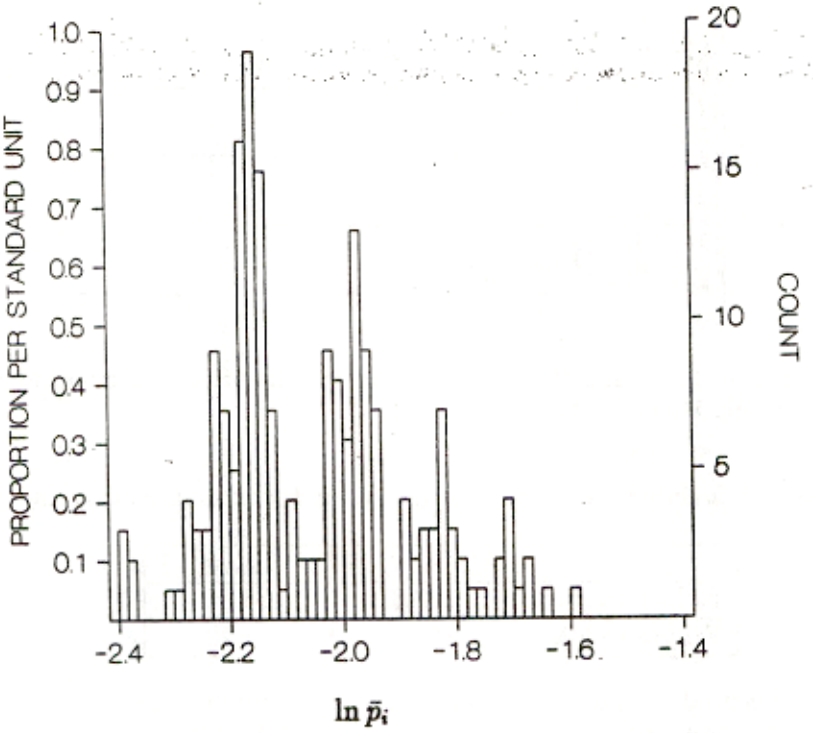


Figure 3: Histogram of load-run failure probabilities (logarithmic scale) for individual diesels

Table 1: Mean, variance, and standard deviation of diesel failure probabilities for individual diesels

	Mean	Variance		Standard Deviation	
	$\hat{\mu}_{cop}$	Copas $\hat{\sigma}^2_{cop}$	modified $\hat{\sigma}^2_m$	Copas	modified
Failure to start	5.0×10^{-3}	8.6×10^{-6}	5.0×10^{-5}	2.9×10^{-3}	7.0×10^{-3}
Failure to load	9.6×10^{-3}	5.1×10^{-5}	1.6×10^{-4}	7.1×10^{-3}	1.3×10^{-2}

Table 2: Mean, variance, and standard deviation of diesel failure probabilities over stations

	Mean	Variance		Standard Deviation	
	$\hat{\mu}_{cop}$	Copas $\hat{\sigma}^2_{cop}$	modified $\hat{\sigma}^2_m$	Copas	modified
Failure to start	5.2×10^{-3}	1.4×10^{-5}	3.0×10^{-5}	3.7×10^{-3}	5.5×10^{-3}
Failure to load	9.5×10^{-3}	2.9×10^{-5}	7.3×10^{-5}	5.4×10^{-3}	8.5×10^{-3}

Using the matching histogram approach for individual diesels, we obtained the following revised mean estimate $\hat{\mu}_{mh}$ and variance estimate $\hat{\sigma}^2_{mh}$:

Table 3: Mean and variance with matching histogram approach

	mean $\hat{\mu}_{mh}$	variance $\hat{\sigma}^2_{mh}$
Failure to start	5.9×10^{-3}	8.1×10^{-5}
Failure to load	8.9×10^{-3}	1.0×10^{-4}

This revision changes the mean values and increases the variances, both for failures to start and failures to load in comparison with the Copas estimate (3).

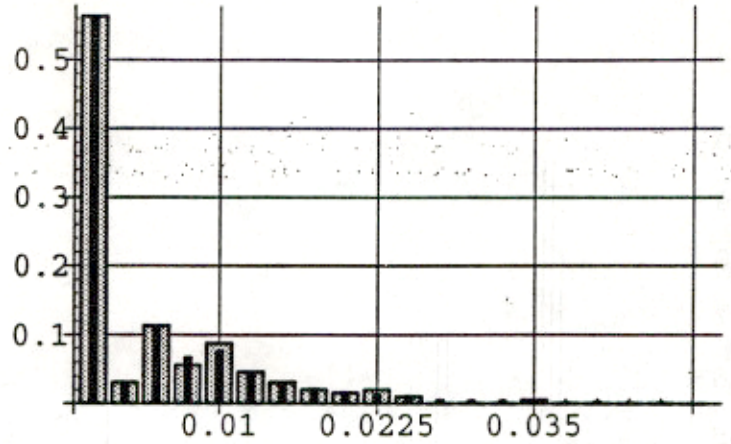


Figure 4: Histogram of real data and fitted simple failure to start probabilities for individual diesels (gray bars = real data, black bars = fitted)

Table 4: Distance function with Copas estimates and matching histogram approach

	$F(\hat{\mu}_{cop}, \hat{\sigma}^2_{cop})$	$F(\hat{\mu}_{mh}, \hat{\sigma}^2_{mh})$
Failure to start	158.8	14.51
Failure to load	154.2	48.98

Figure 4 shows the actual values and fitted values for individual diesels failures to start probabilities with the revised estimates (gray bars = simple failure to start probabilities, black bars = fitted simple failure to start probabilities).

REFERENCES

1. Letter from A. Marion, NUMARC to H.Lewis, ACRS, "Industry-Wide Data on Emergency Diesel Generator Performance", March 5 (1992).

2. J.S. Maritz and T. Lwin, "Empirical Bayes Methods", Chapman and Hall, London (1989).

3. D. Collett, "Modeling Binary Data", Chapman and Hall, London (1991).

4. H. Martz and R. Waller, "Bayesian Reliability Analysis", Krieger Publishing Co., Malabar, Florida (1991).

5. J. Shultis, F. Tillman, N. Eckhoff and D. Gosh, "Bayesian Analysis of Component Failure Data", NUREG/CR-1110, November (1979).

6. K.E. Jänkälä and J.K. Vaurio, Residual common cause failure analysis in a probabilistic safety assessment, *in*: "Proc. Probability Safety Assessment International Topical Meeting", Published by the American Nuclear Society, Florida, Vol. 2, 804-810 (1993).

7. H. Martz and M. Lian, Empirical Bayes estimator of the binomial parameter. *Biometrika*, Vol. 61, 517-523 (1974).

8. J. Copas, Empirical Bayes methods and the repeated use of a standard. *Biometrika*, Vol. 59, 349-360 (1974).

AN UNAVAILABILITY MODEL FOR ERRORS MADE DURING SURVEILLANCE TESTING

Terry F. Bott

Probabilistic Safety Assessment Section
Engineering and Safety Analysis Group
Nuclear Technology and Engineering Division
Los Alamos National Laboratory
Los Alamos, New Mexico 87545

INTRODUCTION

Periodic testing or examination is conducted routinely for some critical standby equipment or instrumentation, in an attempt to increase its availability. This is often called "surveillance testing." There is a finite probability that tested equipment will be left in a degraded or nonfunctioning state because of an error, and this important type of human error is often called a "restoration error" in probabilistic safety analysis (PSA) parlance. One would expect a trade-off between the reduction in unavailability gained by surveillance testing and the increase in unavailability incurred by surveillance testing errors. In this paper, a mathematical model of the effect of errors made during surveillance testing on equipment unavailability is described.

TYPES OF SURVEILLANCE TESTING

The simplest surveillance test involves an inspection that does not take the tested equipment out of service. This is called a "nonintrusive test" in our work. An example of nonintrusive testing is a visual check of valve stem position to determine valve seat position. In contrast, an intrusive surveillance test involves taking a piece of equipment out of operation to perform a test with dummy inputs, a detailed inspection, or an operational run. An example of intrusive testing is taking an instrument off-line and introducing a test voltage to check its response.

SURVEILLANCE TESTING ERRORS

Two types of surveillance testing errors are treated in this model: testing error and restoration error. The failure of the tester to detect an existing unavailability is a testing error. Failure to return equipment that has been taken out of service for testing to an operating status is a restoration error.

Several performance shaping factors affect the probability of failure to restore. The most important of these is often the presence or absence of alerting factors. An alerting factor serves to remind to maintainer to take some action. For example, if one of a series of instru-

ments is discovered with an out-of-calibration setting, most maintainers will be especially vigilant in testing the remaining instruments.

The unavailability model reported in this paper includes restoration-error and testing-error probability estimates. We assume that human error probabilities can be estimated using some Human Reliability Analysis (HRA) methodology such as Technique for Human Error Rate Prediction (THERP)[1] or Human Error and Reduction Technique (HEART),[2] or by expert opinion solicitation.[3]

SURVEILLANCE TESTING UNAVAILABILITY MODEL

The unavailability of equipment is represented in our model as the fraction of total operating time that the equipment is unavailable. The total operating time for the equipment is divided into intervals of length T called "operating periods." The component is serviced at the end of each operating period, and it emerges into a new maintenance interval with a probability, p_f, of being unavailable. In our model, p_f is an initial condition on the unavailability function. During an operating period, the component is subjected to q surveillance tests at regular intervals. Therefore, the operating interval, T, is divided conveniently into (q + 1) equal intervals called "surveillance intervals." The component will emerge from each surveillance test in either an available or unavailable state. The probabilities of emerging in each state are assumed to be a function of a surveillance testing error probability, p_x, and the restoration error probability, p_s. For simplicity, we assume a constant random failure rate during all operating periods, so the probability of a random failure in any surveillance interval is a constant p_r. We also assume no recovery of unavailable components between surveillance tests and constant human error probabilities. The probability of a component being unavailable at the start of the k + 1st surveillance interval of an operating period is given by the recursion relationship

$$P_{k+1} = P_k p_x (1 - p_s) + p_s \ .$$

The probability of an unavailable component in each surveillance interval is dependent on the previous interval and on the surveillance error probabilities. The total time that the component is unavailable for the operating period is the sum of the probability of being unavailable for each surveillance interval multiplied by the length of each maintenance interval. The unavailability of the component for the operating period is the unavailable time divided by the length of the operating period. The unavailability equation involves sums that are geometric progressions and can be evaluated in closed form. The resulting equation for the unavailability U is[4]

$$U = \frac{p_a}{q}\left(\frac{1-\pi^q}{1-\pi}\right) + \frac{p_b}{1-\pi}\left[1 - \frac{1}{q}\left(\frac{1-\pi^q}{1-\pi}\right)\right] \ ,$$

where $\pi = p_x(1-p_s)$, $p_a = p_f + p_r$ and $p_b = p_r + p_s$.

APPLICATIONS OF THE MODEL

The model described above was applied using the probability values in Table 1 for a base case. These parameters are based on reasonable values encountered in a number of PSAs. Variations of these parameters model different maintenance situations.

The value of the restoration error probability, p_s, can be used to model some situations of interest. When p_s is zero, nonintrusive surveillance is modeled. Nonintrusive surveillance testing always reduces the unavailability of a component because standby failures can be discovered and corrected, but no new unavailability is introduced. However, such testing may be much less likely to discover component standby failures or faults than more invasive testing. When p_s is greater than zero, intrusive surveillance testing is modeled. If the instrument is not returned to service after the test, it is unavailable for performing its intended function after the test, even if it was working before the test.

Table 1. Unavailability model parameters.

Parameter	Value
p_x	0.2
p_s	0.1
p_f	0.1
p_r	0.01

Our model includes the effects of alerting factors and second checkers on failure-to-restore errors as a refinement to the failure-to-restore model. Because of the finite probability of failing to restore a component after surveillance testing, intrusive surveillance testing can result in increasing unavailability for a given component. This unavailability growth will occur if the gain in availability arising from the discovery and correction of standby faults is relatively smaller than the unavailability introduced by errors in restoration after surveillance testing. Figure 1 is a plot of unavailability U as a function of the number of surveillance tests per operating period for various values of p_s.

Another interesting class of results can be generated by examining the derivative of the unavailability U with respect to different parameters. Figure 2 is a plot of the derivative of U with respect to the surveillance error probability, p_x, as a function of p_x when the random failure rate is very low. A parametric family of curves for different values of surveillance testing frequency represented by q is generated. In this plot, one can see that increasing the number of surveillance tests increases the importance of the surveillance error probability in determining the unavailability. The importance of the surveillance error probability also increases as its value increases. Both trends are intuitively reasonable.

Other uses of this model include evaluating the cost-effectiveness of surveillance testing. A surveillance test often will result in a reduction in unavailability for all testing frequencies. However, a cost is associated with each performance of the surveillance testing based on the operator time required to prepare, perform, second-check, and restore the component. A corresponding change in component unavailability is associated with each surveillance test. As more frequent surveillance tests are performed, the cost of performing them rises linearly, whereas the reduction in unavailability decreases exponentially. A point of diminishing returns for increasing the frequency and efficiency of surveillance tests is soon reached, where a unit reduction in unavailability achieved by increased surveillance testing is bought at an increasingly higher price.

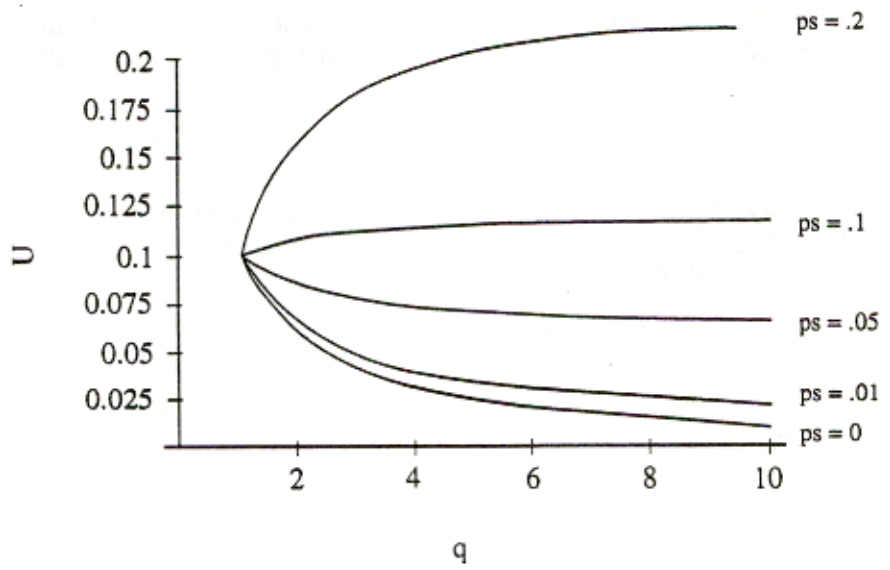


Figure 1. U vs surveillance frequency q (p_s as a parameter).

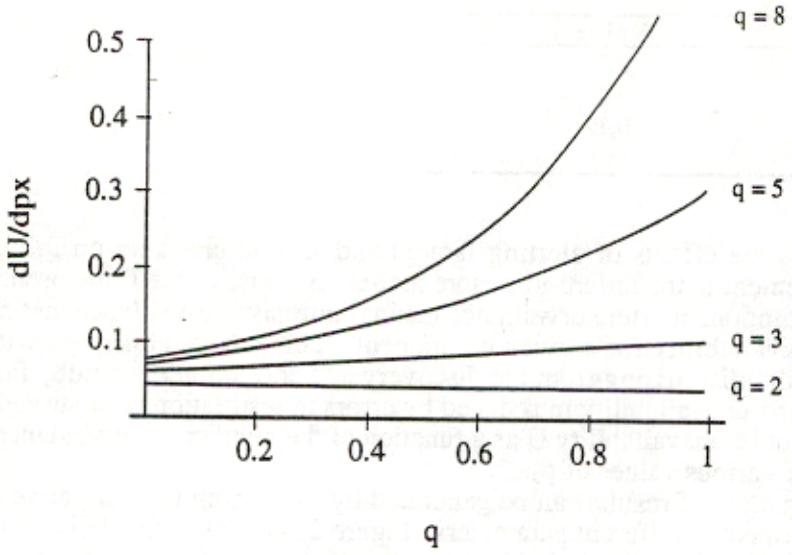


Figure 2. $\partial U/\partial p_X$ vs surveillance error probability p_X.

CONCLUSIONS

We have developed an unavailability model for surveillance testing of standby components that includes testing characteristics such as restoration error probability and failure to discover component unavailability error probabilities. This model includes the effects of surveillance tests and unavailability introduced by the tests themselves. It also includes maintenance and surveillance frequencies, random failure probabilities, and human error probabilities for failing to restore and failing to discover unavailable components during testing. The model includes the effect of alerting factors on surveillance restoration errors.

If surveillance is nonintrusive, it will always decrease unavailability. If surveillance is intrusive, unavailability can either decrease if surveillance restoration error probability is low enough or increase if this error probability is too high. An example of the cost-effectiveness of surveillance testing shows that the frequency and the efficiency of surveillance tests strongly affects costs but affects unavailability less strongly. Thus, a point of diminishing returns for increasing the frequency and efficiency of surveillance tests is quickly reached.

REFERENCES

1. A. D. Swain and H. E. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application," NUREG/CR-1278, U.S. Nuclear Regulatory Commission (Sandia National Laboratory), Washington D.C. (1983).

2. P. Humphreys, "Human Reliability Assessors Guide," RTS- 89/95Q, Safety and Reliability Directorate, Culcheth, UK (1988).

3. D. E. Embrey, "The Use of Performance Shaping Factors and Quantified Expert Judgment in the Evaluation of Human Reliability," NUREG/CR-42986, U.S. Nuclear Regulatory Commission (Brookhaven National Laboratory), Washington D.C. (1983).

4. T. F. Bott, "A Failure-to-Restore Unavailability Model for Periodically Performed Maintenance," LA-12266-MS, Los Alamos National Laboratory, Los Alamos, NM (1992).

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

Chair: D. Okrent, UCLA

Two Proposed Methods for Incorporating Deep Technical Knowledge Using Behaviorally Anchored Rating Scales into Probabilistic Risk Assessments

E.C. Abbott (ABZ); Y. Xiong , D. Okrent, (UCLA)

Level of Knowledge and Safety

L.J. Reynes (Electricite de France)

Deriving Start-Up Task Descriptions from Functional Models

M.N. Larsen, J.K. Hansen, P.C. Cacciabue (CEC-JRC, Italy)

TWO PROPOSED METHODS FOR INCORPORATING DEEP TECHNICAL KNOWLEDGE USING BEHAVIORALLY ANCHORED RATING SCALES INTO PROBABILISTIC RISK ASSESSMENTS

Edward C. Abbott,[1] Yongjie Xiong[2] and David Okrent[2]

[1]ABZ, Incorporated
14595 Avion Parkway, Suite 900
Chantilly, VA 22021
[2]Mechanical & Nuclear Engineering Department
University of California, Los Angeles
405 Hilgard Avenue
Los Angeles, CA 90024

INTRODUCTION

Over the past several years, some researchers have noted that some nuclear power plants with lower than average core melt frequencies have had a poor regulatory performance as indicated by Nuclear Regulatory Commission (NRC) reports, such as Systematic Assessment of Licensee Performance (SALP) ratings and Licensee Event Reports (LERs). The conclusions drawn from this are either the current methods of performance monitoring are flawed as they do not really assess risk, or the Probabilistic Risk Assessments (PRAs) are flawed in that they do not adequately account for the effect of the plant's organization on risk. On the one hand, the NRC's, and perhaps the Institute of Nuclear Power Operations (INPO's), assessment processes, such as routine inspections, team assessments and periodic evaluations, may not be appropriately focused on risk and, therefore, the protection of public health and safety. On the other hand, the PRA may be overly optimistic in assuming that the plant data used to calculate is representative since the plant risk is missing a significant contributor, the people that manage and operate the plant. This paper describes two preliminary approaches for folding one aspect of a plant's organization into the PRA. That aspect is called Deep Technical Knowledge.

INCORPORATION OF DEEP TECHNICAL KNOWLEDGE INTO WORK PROCESSES

Very few will argue with the premise that a person must know something about a job to perform it successfully. In highly complex, technical industrial work such as the operation and maintenance of a nuclear power plant, the distribution of knowledge for successful performance varies over many scientific and engineering disciplines. It is, therefore, unreasonable to assume that everyone needs to know everything about each discipline, but appropriate knowledge is needed at every level in the organization for success. This is recognized in the power plant's organizational position descriptions and INPO's task analysis programs. To better understand the distributions of appropriate knowledge within the nuclear power plant organization, a system of Behaviorally Anchored Rating Scales (BARS) was developed which describes the knowledge needed for successful performance for selected positions in the plant's organization.[1] The five-point bar scale describes the level of knowledge needed for each scientific, engineering and technical area for the positions analyzed in the study. Where 1 is best and 5 is worst on the scale. If the incumbent in that position

has the requisite knowledge as described by the BAR, then the incumbent is likely to perform successfully. Preliminary reviews show that this approach is reasonable.

The plant organization operates in an administrative structure which attempts to assure that sufficient information is available to the plant personnel for performing work in the plant. This work may include the design of a system modification, control of the plant during a trip or replacing an electric motor in a safety-related system. The maintenance work process has been modeled and the published preliminary results are encouraging.[2] The model provides insights to common cause failures that would not have otherwise been found by relying solely on plant data. Combining the model of the work processes and the deep technical knowledge BARS for the people in the plant's organization may provide the quantitative adjustment needs to account for the effect of organization and management on risk.

Each work process contains several steps that require a person in the plant organization to act. The work process for maintenance has been modeled. This process includes procuring the replacement parts, installation of the parts, quality control checks of the installation and returning the system to normal. Each of these steps in the process is needed to assure the "structure, system or component" (SSC) will operate successfully once the maintenance is complete. Any breakdown in the process can lead to the SSC not being available to perform its function and thereby increase the core melt frequency. Some have suggested that such unavailability is already included in the plant data such as LERs, plant performance logs or surveillance tests. These data, however, have an inherent delay and only measure past performance. They do not include information on the performance of current organization or reflect changes in the work processes that may have been instituted. Combining an up-to-date model of the work process with an accurate assessment of the organization knowledge overcomes these shortcomings.

A preliminary model was developed to test the reasonableness of this approach and is shown in Figure 1. An important step in the maintenance work process is Quality Control (QC) checks. During this step, a QC Inspector will review the work performed to assure that it has been done according to specification. Tolerances, procurement specs, in-process assembly, et cetera will be checked. This is critical in the maintenance of safety-related equipment, such as the safety injection pump, as it is the final inspection of the equipment prior to its return to service. Inadequate knowledge of the Inspector could lead to failure of the equipment to perform and an increase in the core melt frequency.

Several questions must be answered to determine whether or not this step is performed successfully. They are:

- Who is important to the successful completion of the step?
- What areas of technical knowledge are needed?
- How important are the areas of technical knowledge?
- What are the knowledge levels required for the areas of technical knowledge for the people that are important to the step?
- How well do the people that are important to the step know the areas of technical knowledge?

The answers to these questions are developed in Figure 1. The people that are important to the step, "QC checks," are the QC Inspector, Quality Assurance (QA) Manager and Training Manager. The QC Inspector performs the checks, the QA Manager provides supervision and guidance for the conduct of the QC Inspector's work, and the Training Manager provides the QC Inspector's training. The knowledge areas that are important to the successful completion of the work process step include Plant Knowledge, Thermal Hydraulics, Plant Configuration, Safety Analysis and Regulations. Each of these areas is given a ranking of importance on a scale of 1 (not very important) to 5 (important). The BAR for the technical areas associated with the positions in the plant organization is then listed and compared to the knowledge level of the current person (incumbent) filling the position. If the incumbent's ranking in knowledge of the area is greater than or equal to the BAR for the area, the incumbent's score for the area is 1. If it is less, the incumbent's score is 0. The rankings shown in the figure are for illustration.

For the purposes of this example, the performance of each incumbent is equally important to the successful performance of the step and are independent events. Therefore, the probability of successfully completing the work process step is the product of the probability that each incumbent will perform the step successfully. The probability that each incumbent will perform the step successfully is the sum of the product of the incumbent's score and the ranking of the area divided by the sum of the area ranking. For the examples provided, the incumbent probability of the QA Manager is 1, the Training Manager is .6 and the QC Inspector is .3. Therefore, the probability of performing this work process step successfully is .18.

This approach appears to have merit, but requires further review and development. In large

measure, the approach depends upon developing the BARS for the nuclear power plant organization, assessing the knowledge of the organization's incumbents and determining what technical areas are important to the successful completion of the work process steps. A significant amount of work has been done on each topic, but no topic has been completely developed. In addition, considerable amount of work is needed to obtain a consensus among knowledge experts that the BARS, area of importance and work process models are appropriate. However, the coupling of the work process and BARS as described in Figure 1 has merit.

INCORPORATION OF DEEP TECHNICAL KNOWLEDGE INTO THE PRA

The effect of organizational factors on the risks of nuclear power plants has received more and more attention recently. The research on this issue focuses on: (1) what are the organizational factors; (2) how to measure these factors; and (3) how to quantitatively include the impact of these factors into the PRA. Deep technical knowledge is one important factor. A preliminary approach to the definition of deep technical knowledge, the knowledge categories in nuclear power plants has been proposed[2]. The BARS method has been used to develop the measurement scales for some of the knowledge categories[1].

Now the question is how to use these measurement scales and include the influence of deep technical knowledge into the PRA. From existing PRAs, it is found that a large fraction of operating events is attributed to human error. Analysis of the root cause of 180 significant events reported to INPO shows that 210 among 387 root causes (52 percent) were classified as human performance problems. Therefore, accurately calculating the human reliability is very important in PRA methodology. The existing human reliability analysis techniques predict human error probabilities without considering the influence of knowledge depth of the personnel. A knowledge influence tree or causal tree of human error is developed in this paper to incorporate the operating level personnel's deep technical knowledge impact into the PRA.

In principle, the knowledge depth of all positions within the organization should affect the plant's safety. From the study of LERs and accident analysis reports, it is found that the influence of people in different positions on safety is different. For the operating level personnel, the portion of their performances, which depends on their depth of knowledge, can contribute directly to the occurrence of events. This is included in the PRA analysis as human error. The manager level personnel will also affect plant safety, but usually in a more general way. The depth of their knowledge affects the factors such as decision-making and safety culture of the plant. In our present approach, only the operating level personnel are studied. The operating level personnel include:

Senior Reactor Operator
Control Room Operator

- Auxiliary Operator
- Instrument Technical Foreman
- Instrument Technical Level 1
- Electrical Foreman
- Electrical Level 1
- Mechanical Foreman
- Mechanical Level 1
- Radiation Protection Foreman
- Chemistry Technician

In the PRA, the initiating event is caused by either human error, hardware or an external event. A reasonable assumption is that human error is influenced by the deep technical knowledge of the operating level personnel in the plant. A Knowledge Coefficient (KC) is used to modify the existing human error probabilities. To calculate the coefficient KC, a knowledge influence tree or causal tree of human error was developed (Figure 2). In the tree, the starting point is human error (Level 1). The second level is the human error types. The error types are the simplification and a further classification of present PRA human error classification. They are: operator error in operation, operator error in maintenance, failure to restore after test and maintenance, miscalibration and others. Level 3 is the working places or work units where the errors occurred. At present, five work units are examined: operation, instrumentation and control, mechanical maintenance, electrical maintenance and procedure review. Level 4 is the operating personnel involved in the work units. The logic of this tree can be expressed in another way: the depth of the technical knowledge of the personnel affects how the work units carry out the task. The quality of the work units has an impact on the quality of the execution of the task and, therefore, affects the probability of occurrence of the human errors.

Combining the existing PRA data and the Analytic Hierarchy Process (AHP) method for this

tree, the percentage contribution of different position people to the human errors for an event can be obtained. In Figure 2, the results of two events are given, one event is loss of offsite power, another is loss of containment heat removal. For each event, the basic steps are as follows:

(1) From the event tree identify the systems involved.

(2) Analyze the human errors in the fault trees of the systems, classify them according to the error types for all systems involved and normalize to obtain the weights between Level 1 and Level 2. At present, assume all errors are equally important.

(3) From the human error properties and classification in the fault trees, identify which work unit the error belongs to and the weights between Level 2 and Level 3 are obtained.

(4) Using expert opinion to obtain the weights between Level 3 and Level 4.

(5) Calculate the percentage distribution or weights of personnel at different positions for the human errors of the event.

As a next step, the knowledge coefficient is calculated from the weights and the deep technical knowledge measurement ratings (BARS). The model in Figure 2 is used. For each person, the success trees are developed for all tasks needed to be done. All the incumbent probabilities are averaged to get the average incumbent probability of success:

$$AIP = \sum_i (IP)_i$$

The knowledge coefficient:

$$KC = \sum_i W_i (AIP)_i$$

Where W_i is the weight in the knowledge influence tree and $(AIP)_i$ is the average incumbent probability of the personnel.

How to use such Knowledge Coefficient to modify the existing probability of human error needs be worked out. It is clear that the deeper the knowledge level, the safer the plant and the likelihood of human error is reduced. The simplest linear approach can be used. But first, how much the knowledge coefficient will change the existing probabilities of human errors must be decided. Further study is needed in the future.

REFERENCES

1. D. Okrent, E.C. Abbott, J.D. Leonard and Y. Xiong, Use of Behaviorally Anchored Rating Scales (BARS) for Deep Technical Knowledge, Conference on Probabilistic Safety Assessments, PSA '93, Clearwater Beach, January 1993.
2. G. Apostolakis, O. Grusky, D. Okrent, etc., Inclusion of Organizational and Managerial Factors into Probabilistic Safety Assessments of Nuclear Power Plants, NUREG/CR-5751, 1991.

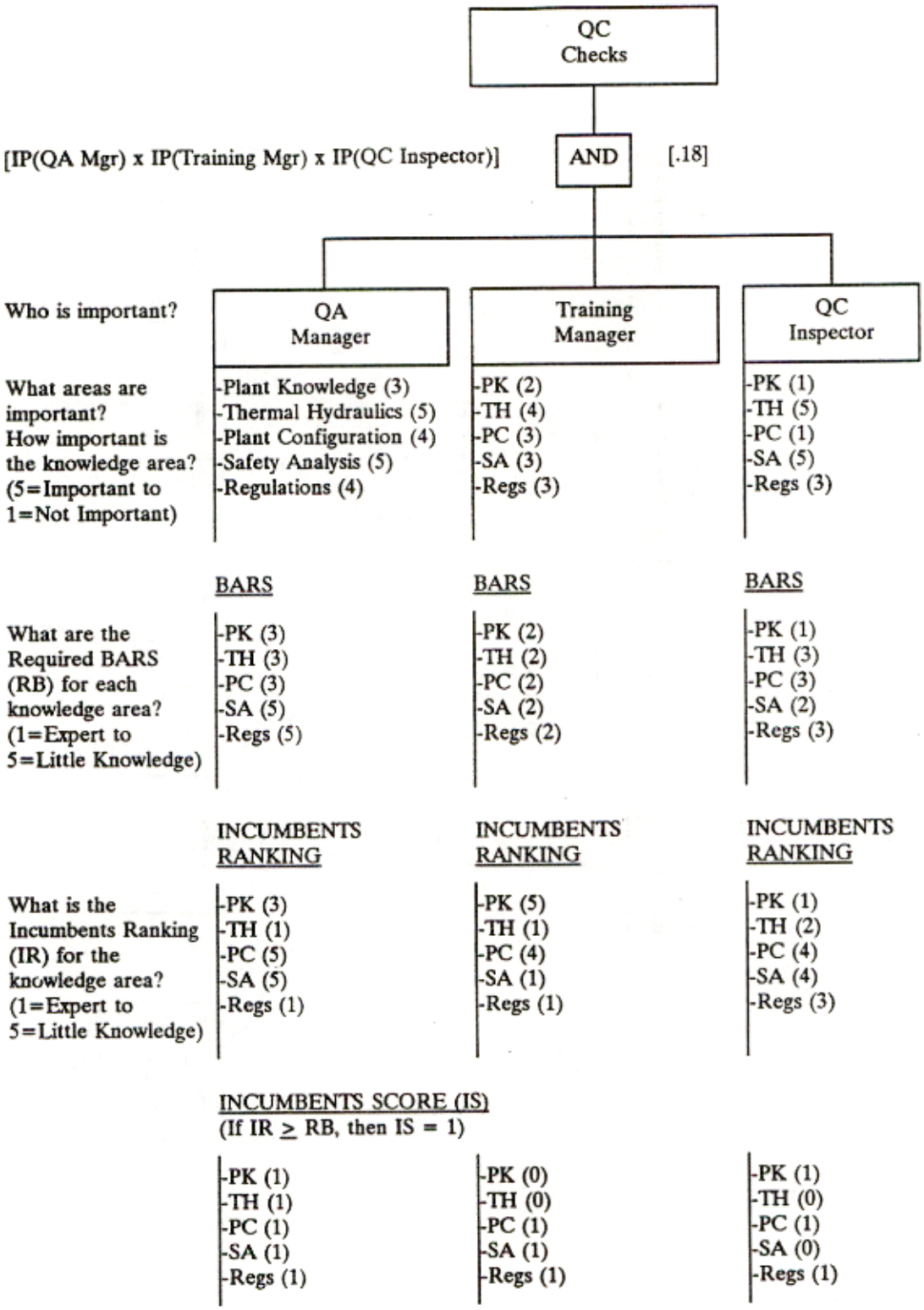


Figure 1. Safety Injection Pump (Contribution from Maintenance Due to Unavailability)

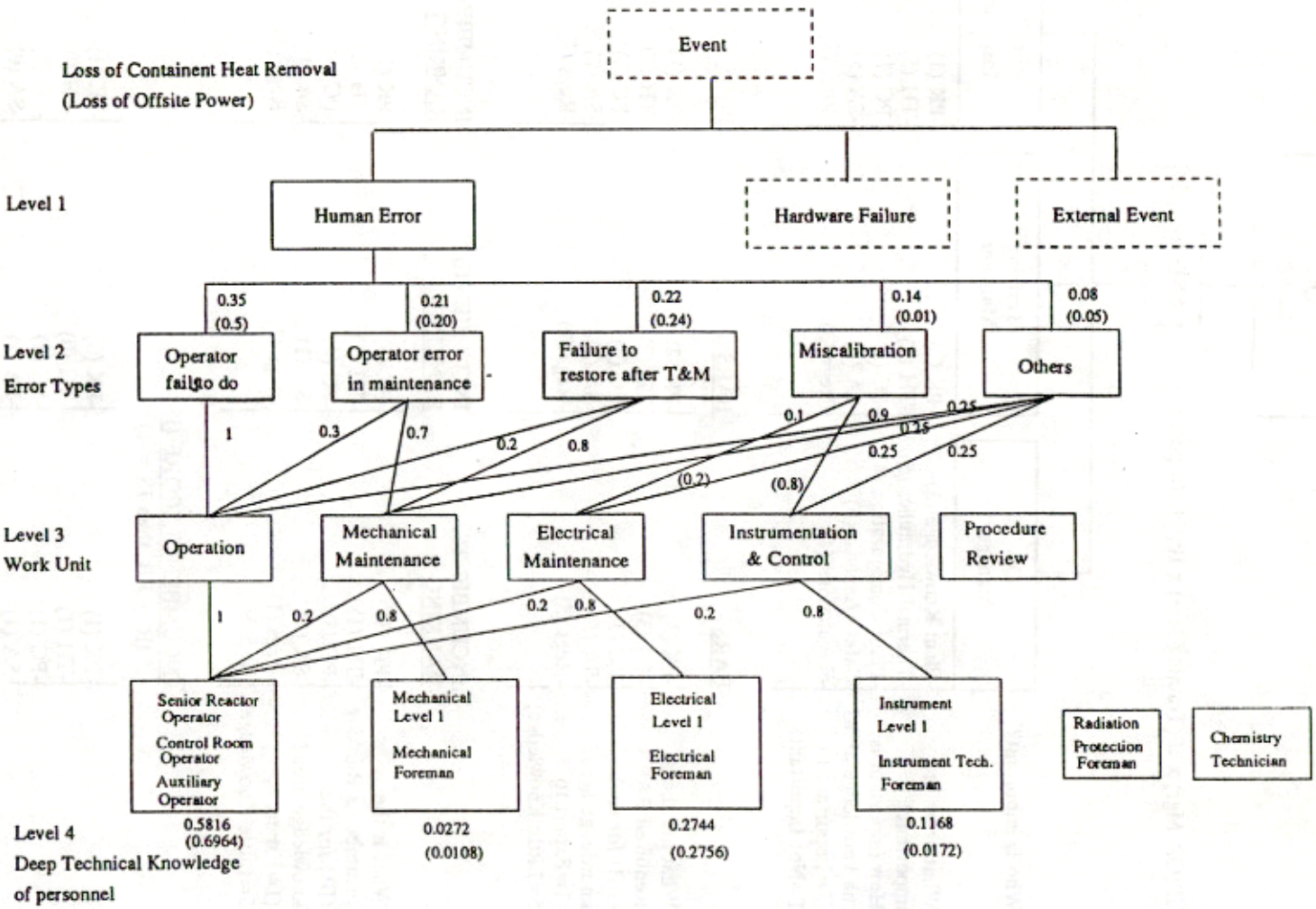


Figure 2. Casual Tree of Human Error (Knowledge Influence Tree)

LEVEL OF KNOWLEDGE AND SAFETY

Louis J. Reynes
Electricité de France
DG - IGSN
32 Rue Monceau
75008 PARIS

Abstract :

The favorable effect of a good level of deep technical knowledge for the personnel on the safety of a nuclear power plants seems incontestable ; it is, however, quite another matter to evaluate and to measure its importance in quantitative terms. To attempt to answer this question, as far as the situation in EDF plants is concerned, we are going to examine succcessively the three areas in which the problem of knowledge is of major importance : training, analysis of operating incidents and probabilistic studies.

1 - INTRODUCTION :

General knowledge alone is insufficient to allow operators to take control of a highly complex process such as a nuclear reactor. A practical training is essential to develop the necessary skills. This training can take place in training centers (simulators) or directly on the plant (on the job training). This kind of training, which is difficult to formalize (inherent skills), provides generally high levels of operator efficiency in normal situations.

However, general knowledge is quite important because it allows organization and hierarchisation of the skills [1]. Futhermore, it is essential in understanding and managing the unusual operating situations [2].

For these reasons, the favorable effect of operator general knowledge on the safety of a nuclear plant seems incontestable. Is it possible to quantify this relationship ? To answer this question, we are going to examine successively the areas in which such knowledge is important : training, analysis of operating incidents and probabilistic studies.

2 - TRAINING :

EDF's light water nuclear power plant program was set in motion at the beginning of the eighties by the redeployment of staff from conventional fossil fuel plants and from nuclear plants of the "graphite-gas" type. The training programs were then adapted to this situation. From time to time, these programs were added to or modified as necessary in order to keep up to standard.

As the rapid growth of the program entailed the hiring of a number of agents without professional experience in the nuclear industry, all training programs were reviewed in 1987, the objective being to build a coherent system using the "Referentiel Métier" (Job Reference) method. The following stages are carried out, job by job :

1 - list of tasks to be performed
2 - fine-turned analysis of the task (operator in situation)
3 - deduction of skills required (in the conditions in which they are used)
4 - abilities (move from skills to knowledge)
5 - training scheme (move from knowledge to the course)

For point 1 above, the word "task" has to be regarded in its general context. For example, a task will be not only filter cleaning and oil change on a given motor. It will be the complete maintenance operation for the lubrication system of a component, including of course the filter cleaning and oil replacement.

Concerning the point 3, it is important to stress that the skills have to be given in a way allowing the teacher to observe and quantify them.

Analysis of point 4 ends with the drawing up of specifications which is used as a basis for preparing point 5. As an example, analysis of the job of operator brought to light more than 700 tasks. The new training system, currently in service for all jobs related to plant running, is being extended to maintenance jobs. It is therefore now possible to describe the knowledge required for each work station.

Renewing the training system led to thinking about the means of assessing knowledge. Prior to this, accreditation for fulfilling a particular function was granted to staff once they had passed a certain number of training modules. The current trend is to check knowledge and skill acquisition in a more direct way.

The question remains of how to validate the training. This can only really be done in the field by analyzing operating incidents or by observing the behavior of operating teams on simulators.

3 - ANALYSIS OF OPERATING INCIDENTS :

All incidents occurring in EDF plants are analyzed to determine the causes (this causal analysis has recently started to be backed up with an

analysis of potential consequences, with special attention given to precursors). Causal analysis first looks at the possible existence of human error in the incident sequence. If such is the case, the "Human Factor" group from the central departement is brought into the analysis.

This type of analysis was formerly limited insofar as the operators were asked to work within the logic of the carrying out of procedures. With this way of looking at the operator's task, the only possible errors arise as a result of incorrect application of the sequence of actions laid down in the procedure. Given the information gathered in the incident file, it was difficult to take the analysis very far and especially to bring to light cases where knowledge might have been inadequate. However, it had been observed that certain operators had difficulties whenever it became necessary to leave the sequential running logic and to move to a control logic in which it was necessary to keep track of several parameters (rod position, xenon effect, boron content etc.) In such cases, it had been noticed that the operators' theoretical knowledge was sometimes rather limited.

Another type of difficulty is imperfect operator understanding of reactor behaviour during an accident situation. For example, a supervisor has recently reduced the power from 100 % to 30 % by using only the control rods. This power level was maintained during several hours to allow a maintenance action. Several days later, an analysis of this transient showed that in the event of a LOCA, the clad temperature of certain fuel elements would have risen above the design value.

Given the experience acquired in the analysis of several hundred incidents, it was decided in 1992 to redesign a data base which would correct the inadequacies of the previous one in order to take causal analysis further, especially in the area of the human factor. This data base is currently in service and it will be possible to deal with all the incidents of 1993 with his new tool. The analyses will be performed in the central department. Ultimately, it is planned to decentralize this analysis and the keying-in of data to each of the sites where a group for analyzing experience feedback, including a human factor specialist, is currently being set up.

4 - PROBABILISTIC SAFETY ASSESSMENTS :

In French PSA's, special attention has been given to the human factor. To achieve this, a human reliability data base has been drawn up, using information obtained from simulator tests. Such tests may make it possible to validate a training system. This is not generally the aim in view, as we are usually content to measure performance (adequate or otherwise) and the level of knowledge is not taken into consideration in this very overall approach. Should performance be judged to be inadequate, a more detailed analysis can still be used to determine the level of knowledge.

The simulator test is therefore another means of analyzing the behavior of operators during incident situations, which is probably more effective than direct analysis of operating incidents, even though a simulator bias does exist. A statistical effect can be brought out by presenting the same incident (whether or not it is drawn from operating experience) to different operators. It

is possible to present accident situations on the simulator which have never been observed during real operation.

Finally, analysis is of better quality since each test is followed by an on-the-spot debriefing, sometimes with a "self-confrontation" (a video presentation of the test session), which makes it easier to see how the operators reason[3]. This discussion with the operators is not of such good quality when a real incident is involved since the time lag means that information is lost as the operators reconstruct the real event in their mind.

Up to now, EDF has been using 6 simulators (full scope - full scale) to train the operating teams of 54 units (with each agent having one week of training per year). To double the time of training on the simulators, EDF has ordered two further simulators. In addition, it has been decided to design and order a simulator for the training of maintenance staff. The need to order more maintenance training simulators will be decided after validation of the prototype.

Experience has shown that the operators need to understand what they are doing and they do not hesitate to say so during interviews. Practical knowledge is not sufficient if an overall coherence cannot be given to his knowledge. If we do not understand something, we tend to invent an explanation for it[1]. We know that a certain level of theoretical knowledge - some would speak of a level of culture - enables us to order our knowledge as a whole. Experience has shown that this level of knowledge is only effective if it is put into practical application.

The quality of a plant running or maintenance action depends not only on the behavior of the staff taken on an individual basis, but also on the team to which they belong. What counts is indeed the overall behavior of the team, which functions as a result of the combination and the exchange of individual skills. Experience has shown that the team can tolerate the existence of weak links, provided that this situation does not last forever. The role of the team is so strong that training at EDF is now carried out more and more in teams, both for operation and for maintenance.

PSA is a safety indicator which includes technical aspects and human factors. It enables the operators' performances to be quantified on an overall basis. But PSA does not bring to light the impact of the various aspects of human behavior, and especially of the role of basic knowledge, on the probability of a core meltdown. At EDF therefore, studies remain, for the time being, qualitative, with special emphasis on simulator tests. A test compaign is planned in 1993 to study the behavior of operators in accident situations, using a "symptom-oriented" approach. The move from event-oriented to symptom-oriented procedures poses a number of problems which will probably tax the level of theoretical knowledge. It would therefore be useful to be more aware of the special features of this type of running in order to specify the forms of knowledge at stake. This compaign will be followed by another aimed at assessing operator behavior in the final version of the computerized control room of the new N4 type reactors. A new human reliability data base concerning on-screen running will be opened in liaison with the PSA of this N4 reactor.

5 - CONCLUSIONS :

The question of the level of knowledge is central to the preoccupations of the departements in charge of training, of analyzing incidents and of probabilistic risk studies. This question is for the moment dealt with qualitatively. As far as training is concerned, current efforts are tending to raise the level of knowledge (by in-service training and by requiring a higher level when staff are hired), by better integration of theoretical training in the training course and by improving the assessment of knowledge[4]. The main difficulty is in the scale and nature of a complete national training system which takes a long time to set up and which is then difficult to change. The analysis of incidents should improve in 1993, through the setting up of a new data base, richer than the former one, especially as regards the human factor. Concerning PSA's, emphasis is currently laid on the study of specific problems, such as the status oriented approach or operating with the computerized control room : two situations in which the level of theoretical knowledge could play a major role. Provision has been made, during the course of the simulator tests, for clarification of the role that the level of basic knowledge may play.

REFERENCES

1. De Montmollin "L'intelligence et la tâche" Peter Lang (1984)
2. Amalberti "Savoir-faire de l'opérateur" Modèles en analyse du travail, Mardaga (1991)
3. F. Mosneron-Dupin Analyse d'entretiens avec des opérateurs de conduite de centrale nucleaire (Document EDF)
4. Formation des exploitants nucléaires" - Rapport du Comité Consultatif sur la formation des exploitants nucléaires (1990).

DERIVING START-UP TASK DESCRIPTIONS FROM FUNCTIONAL MODELS

M. Norby Larsen, J. Kjær-Hansen, P. C. Cacciabue

Commission of the European Communities
Institute for Systems Engineering and Informatics
Joint Research Centre
I-21020 Ispra (VA)
Italy

INTRODUCTION

Procedures describing a start-up sequence for modern process plant are made up by a sequence of actions and checks. Conventional procedures are often rigid and do not allow for deviations from predefined courses of action. Further, the purpose of the actions is not readily understood from the purely sequential descriptions where only the last result of the last action is explicitly shown as a goal (Lind and Larsen, 1992). To capture and organize deep technical knowledge about the link between the purposes of the plant components, their behavior and the actions needed for plant operation, some navigation instrument is needed.

To support the operator in performing a start-up, a system has been developed that permits the operator to design his own start-up plan. A start-up plan consists of a series of actions that will bring the system from an initial state to a goal state, by which is meant a system state where total or partial functionality of the plant is established.

To "design" a start-up plan, knowledge is needed to describe the relationship between the actions available to the operator and the functions of the plant. It is an underlying assumption of this work that the operator uses the notion of function (the deep knowledge) in his understanding of the workings of the plant, and that he will be supported by a system based on this notion.

When a plant is viewed as a collection of functions supporting either each other or the top-level goals of operating the plant, a start-up may be seen as the task of establishing these functions.

For this purpose task descriptions centered on the establishment of functions have been developed, based on the Multilevel Flow Modeling (MFM) methodology (Lind, 1990). MFM is based on a means/ends organization of the plant, and uses the notion of function to capture the workings of the plant. As the name implies, the functions are organized in multiple levels, where the

functions on the lower levels support those on the higher levels. A short description of MFM will be given below[1].

By focusing on the functional aspects of the physics of the plant, the same model may be used (in different interpretations) for diagnosis of faults, explanation of consequences and planning of start-ups.

This paper describes how the MFM methodology can be extended so that knowledge from the model can be transformed into task descriptions suitable for both automatic construction of start-up sequences and feasibility validation of a plan constructed by the operator himself.

MULTILEVEL FLOW MODELING

MFM models describe the plant in terms of means and ends, where ultimate ends are the main goals for operation of the plant and the ultimate means are the components of the plant. In between these extremes are the functions that are abstract descriptions of the workings of the various parts of the plant with respect to the goals of the operation. Apart from the functions of the plant, the MFM technique characterizes the plant by the flows of mass and energy that are in the plant, and is hence best suited for processes that have conversion and processing of energy as the main purpose.

There are six types of function in MFM for both types of flow, shown in Figure 1 along with their graphical representations. In the upper right hand side the two main relations between MFM elements are shown: (1) the *condition relation* expressing how (goal) states condition functions, and (2) *achieve relations* expressing how functions participate in the achieving of a goal. Last, the structure element is used to group functions into networks.

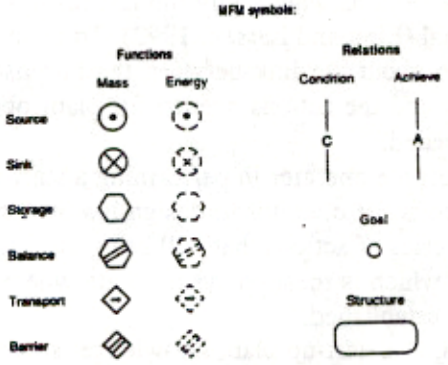


Figure 1. The symbols for graphical representation of MFM. Mass and energy flow elements are distinguished by dashed lines.

SPECIFICATION OF CONDITIONS FOR THE FUNCTIONS

Functional models often prescribe conditions on components or physical structure to be fulfilled in order for the functions to *exist*. A function can be

[1] Readers interested in a more thorough description are referred to (Lind, 1990).

viewed as a certain behavior of a component or system which serves to achieve a goal, and hence the conditions for the existence of a function express the state(s) in which the component helps to achieve the goal. An example of how this can be done in mechanical engineering can be seen in (Hodges, 1992), where three types of condition are defined: (1) *Applied* preconditions (forces), (2) *behavioral* preconditions (interactions with other objects) and (3) *physical* preconditions (object properties and shape). As MFM is defined in (Lind, 1990), there is only one type of condition for a function, which on the other hand may take any form it pleases the designer of the model.

If the MFM model is to be used as a basis for specifying tasks for the operator, the semantics of the model must be made more precise on this aspect. As a consequence, three types of condition for MFM elements have been defined. They deal with the following aspects of a function in process plant, and are to some degree congruent with the types of (Hodges, op. cit.):

- the structural support
- the materials being treated
- fitness of the function to the surroundings

The structural support is either provided by equipment of the plant or by a lower level function that provide the means. As examples of this, a pipe carrying hot water may be considered. In an MFM model this would normally be modeled as an energy transport function conditioned on a goal. The goal would be to provide a mass (water) flow in the pipe. This is shown in Figure 2, where a fragment of a hypothetical plant is seen alongside with a fragment of the corresponding MFM model. The dashed line from the goal to Tr11 indicates that the goal is achieved by means of that function[2].

The energy transport function in this example gets its structural support from the water flowing in the pipe, and the goal becomes its structural condition. The structural support of the mass transport function, however, is provided by the pipe.

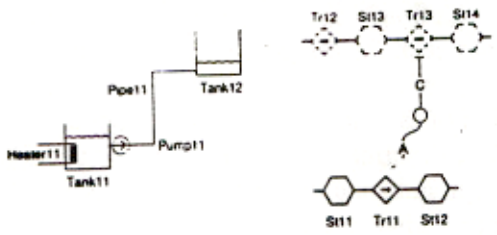


Figure 2. A simple example of components and an MFM model.

Existence of the structural support ensures the *basic behavior* of the function, but the problem is that functions only exist in the context set by the current operation of the plant – or a required one. This means that a function needs other functions surrounding it to provide the context, i.e., the environment in which it makes sense to talk about it as a function.

---

2 This is a non-standard notation used to keep the example simpler.

Hence, the environment must on one hand provide the *material* (water or heat, for instance) that the function must treat. On the other hand it also induces limits on the states of the components themselves or the operation of them to ensure that the behavior is useful for the group of functions as a whole. By useful behavior is meant the behavior of the function where other functions can cooperate with it, i.e., where the functions *fit* each other. Examples of this could be a minimum flow in a transport function or a minimum level in a storage function.

Fulfilling the material condition is done by the surrounding functions, which in this case have the function of delivering material to the function in question. The fitness condition, on the other hand, must be met by tuning the state of the plant to ensure that the levels and the flows have correct values. Some functions are implemented such that this condition can be controlled directly, for instance by means of a pump or a control valve. These functions are active, whereas the behavior of systems without such means of control is determined by the behavior in other parts of the plant. Such functions are passive, and do not by themselves provide means to meet the fitness condition.

The Actions

Functions on the lowest levels are established by performing actions directly relating to the functional conditions, such that the condition fulfillment is a consequence of an action. The actions carried out by the operator may therefore be seen in the light of which functions they contribute to establish, thus providing a framework for explaining the purpose of an action.

The establishment of functions on the higher levels is done by establishing the lower level functions, and will hence be a further consequence of the actions to establish the lower-level functions. The model combined with this description of the actions therefore provides the operator with a deeper explanation of the actions than is normally provided through "flat" procedures.

TASK DESCRIPTIONS

When the semantics of the model are made explicit regarding the physics, task descriptions based on functions concerning the start-up may be derived. The tasks each have a goal of establishing a function and subgoals that, when achieved, will ensure that this goal is met. Each subgoal corresponds to a condition of the function as defined above.

Task descriptions derived from a functional model ensures that the deep knowledge obtained or developed during the design phase can be linked to the operator's knowledge used in the day-to-day operation of the plant.

In this way, the operator can be presented to tasks of the type "establish energy transport from boiler to turbine", which is a task at a high level of abstraction, related to a function at a high level of the model. Through the model this task is bound (by means of a condition) to the action of, e.g., "opening the steam stop valve", which is an action at a low level of abstraction.

When the functions of the plant are identified, safety (or risk) measurements can be assigned to the critical functions of the plant. Through the model, which provides the knowledge about how the functions are related to the states and hence to the actions, it is possible to describe how actions (or omission of actions) relate to the safety of the plant.

For instance, a consequence of an omission of a required action will show up through the task descriptions as a high level function of the plant that will not be established properly, if at all. In this way it is possible for an operator to identify missing steps in his task of establishing plant functions and especially to detect omissions that are related to safety critical goals of the plant.

The Structure of the Task Descriptions

As mentioned previously, the primary contents of task descriptions are goals related to the existence of a function and subgoals related to conditions of the three categories mentioned above. The subgoals are ordered in time (or in groups of unordered subgoals, see later example), thus giving the knowledge needed to reason about the ordering of actions in a plan.

In the task of establishing a function, surrounding functions may also be needed, typically to receive the output of the function in question. This leads to a "material recipient" requirement in the task description thus extending the task description from one function to its surrounding functions. It should be noted that this requirement does not ensure the existence of the function but corresponds to a safety requirement on the operation of the plant.

These conditions will, when the task is going to be carried out, be turned into subgoals of the task. Hence, there will be subgoals representing the need to ensure the existence of the function and a subgoal to ensure that the "material recipient" requirements are met. This can be seen in Figure 3, where a task description is shown with the generic subgoals and an example applying to the energy transport function of the flame in an oil fired power plant.

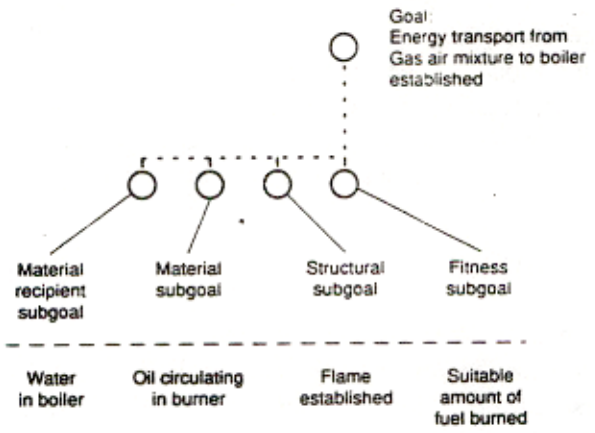


Figure 3. The structure of a task description.

The subgoals of the tasks identified this way must normally be fulfilled in a specific order, given by the physics of the plant. The order of subgoals shown in Figure 3 is typical, but to determine the correct order the requirements related to the operation of the components used must be examined. A further discussion of this can be found in (Larsen, 1993).

The example of turning on the burners is interpreted as follows: The water in the boiler, which is to receive the heat from the flame, must be present for the energy transport to function usefully, i.e. without damaging the equipment

and without loosing the energy. It is achieved by operating the feed water system, which in the model is described as a mass (water) transport function. The material subgoal is that oil is circulating in the burners, so that they are ready for the ignition. These two first subgoals may be achieved interchangeably, but both must be achieved before the next subgoal: flame is established. The flame provides the "transport" of energy from the gas/air mixture to the boiler. It is somewhat atypical for this type of modeling, however, as it is highly self-supporting. The fitness goal is simple: the flow of energy must be suitable with respect to the surrounding functions, in this case (the energy storage function of) the water in the boiler.

A plan for establishing the heat transport into the heat storage of the boiler taken from the task description in Figure 3 would therefore be: (1) Fill the boiler and circulate oil in burners, (2) ignite burners and (3) control firing.

AN OPERATOR SUPPORT SYSTEM

A prototype of a system that supports the operator in performing a start-up using the functional model and task descriptions as discussed above has been implemented using the Smalltalk programming environment. It offers the operator a feasibility check of a start-up plan or it can generate a plan that brings the plant to the specified goal state in a safe way.

CONCLUSIONS

A functional model for a conventional power plant has been developed, and the conditions for the functions have been specified. These conditions have been used to develop task descriptions for start-ups that permit to link knowledge about the physics of the plant and the possible actions on the components to the model of the functions. The task descriptions provide the operator with deeper, functional knowledge about the consequences of carrying out – or omitting – an action. They also permit checking the feasibility of a start-up plan or to generate a start-up plan automatically.

REFERENCES

Hodges, J. (1992). *Naive mechanics. A computational model of device use and function in design improvisation.* IEEE Expert, February 1992.

Larsen, M. N. (1993). *Modelling Start-Up Tasks Using Functional Models.* EUR report 15207, Joint Reseach Centre, Institute of Systems Engineering and Informatics, Ispra, Italy, 1993

Lind, M. (1990). *Representing Goals and Functions of Complex Systems.* Institute of Automatic Control Systems, Technical University of Denmark, 1990

Lind, M. and Larsen, M. N. (1992). *Planning and the Intentionality of Dynamic Environments.* Institute of Automatic Control Systems, Technical University of Denmark, 1992.

030 Uncertainities in Chemical and Physical Phenomenology-ConsequenceAnalyses

Chair: M.L. Brown, AEA Technol.

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

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

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

INTERNATIONAL ASSESSMENT OF PCA CODES*

Lev Neymotin,[1] Christiania Lui,[2] Sarbes Archarya,[3] and James Glynn[2]

[1]Department of Advanced Technology
Brookhaven National Laboratory
Upton, NY 11973

[2]Probabilistic Risk Analysis Branch
U. S. Nuclear Regulatory Commission
Washington, DC 20555

[3]Office of Nuclear Safety
U. S. Department of Energy
Washington, DC 20585

BACKGROUND AND OBJECTIVES OF THE ASSESSMENT EXERCISE

Over the past three years (1991-1993), an extensive international exercise for intercomparison of a group of six Probabilistic Consequence Assessment (PCA) codes was undertaken. The exercise was jointly sponsored by the Commission of European Communities (CEC) and OECD Nuclear Energy Agency. This exercise was a logical continuation of a similar effort undertaken by OECD/NEA/CSNI in 1979-1981.[1] The PCA codes are currently used by different countries for predicting radiological health and economic consequences of severe accidents at nuclear power plants (and certain types of non-reactor nuclear facilities) resulting in releases of radioactive materials into the atmosphere. The codes participating in the exercise were: ARANO (Finland), CONDOR (UK), COSYMA (CEC), LENA (Sweden), MACCS (USA), and OSCAAR (Japan).

In parallel with this inter-code comparison effort, two separate groups performed a similar set of calculations using two of the participating codes, MACCS and COSYMA. Results of the inter-code and inter-MACCS comparisons are presented in this paper. The MACCS group included four participants: GREECE: Institute of Nuclear Technology and Radiation Protection, N.C.S.R. "Demokritos"; ITALY: ENEL, ENEA/DISP, and ENEA/NUC-RIN; SPAIN: Universidad Politecnica de Madrid (UPM) and Consejo de Seguridad Nuclear; USA: Brookhaven National Laboratory, U.S. NRC and DOE.

The main objective of the assessment program was to analyze the results produced by the different codes, and explain the major differences in the results in terms of modeling of physical events and various radiological exposure pathways including the food chain pathway. **Since the calculations were not performed for a specific geographic location, the results predicted by all codes and presented in this paper have no absolute significance outside of the scope of the code comparison.**

---

*This work was performed under the auspices of the U. S. Nuclear Regulatory Commission.

The specific objectives established for the exercise were as follows:[2,3]

a) to compare the predictions of the participating codes under a range of conditions,
b) to contribute to Probabilistic Consequences Analysis (PCA) code quality assurance programs,
c) to guide future developments in the PCA field by identifying the merits and appropriate use of different methods,
d) to enhance the general appreciation of the applicability of PCA codes by those who develop and use them, particularly in decision-making and regulatory processes,
e) to provide a forum for discussion on various international approaches to PCA model and code development, and to encourage harmonization of codes,
f) to provide a forum for exchange between code users and developers, and
g) to produce a report on the exercise which will act as a basic PCA code comparison reference.

The purpose of the paper is to outline the scope and some details of this PCA code assessment exercise and illustrate the results of comparisons using predictions of several selected end-points for dose, health, and economic consequences for some selected cases.

SPECIFICATIONS

The participants were provided with a comprehensive set of input specifications describing a fictitious site with the surrounding area extending to 2000 km from the point of release. The data included population and agriculture/economic distributions, and site meteorology.

Although all PCA codes participating in the exercise had many similarities in the approach to modeling of the major phases of consequence calculations (meteorological sampling, materials dispersion/deposition, dose/health effects predictions, and economic consequences), there were some differences in the input data requirements. It was recognized at the outset of the project that an attempt to satisfy specific requirements of all codes would lead to a prohibitively large volume of input data and still would not eliminate some inherent ambiguities in the input data interpretation. Therefore, the designers of the input specifications chose to use the "best possible" common set of input data leaving the interpretation for the needs of the individual codes to the developers or users of the participating codes.

General Input Data

The data specified for the exercise included such information as population distribution on a geographical grid of varying scale, land use, agricultural production and economic data, and hourly meteorological information for a period of one year. In addition, the participants were given specific values for external exposure shielding and shelter filtering parameters, dry deposition velocity, wash-out coefficient for wet deposition, surface roughness, and breathing rate.

The specifications also included a set of counter-measures, which represented an oversimplification of reality in order to minimize differences in the details of the counter-measures modeling by the various codes.

Source Terms and Cases

There were five source terms specified for the exercise varying in duration and energy of release, time before release, and fractions of the isotope inventory released to the environment. The initial inventory of radioactive nuclides available for release was also specified.

Finally, a series of seven cases to be analyzed were provided (Table 1). Details on the specifications can be found in the Overview and Technical Reports of the exercise to be published by the OECD/NEA and CEC.[2,3] A description of the source terms is given in Table 2. As indicated in Tables 1 and 2 the various combinations of scenarios and source terms selected for the exercise cover a wide range of accident conditions and counter-measures thus providing an opportunity to exercise different features of the codes. The objectives for each calculation can be found in Column 4 of Table 1.

Table 1. Matrix of Calculation Cases

Case*	Case Reference Name	Description	Objective
C1	Single-Phase	Source term ST2. Single-puff release. With economic predictions.	This is the base case with the counter-measures modeled. All materials are released in a single puff.
C2	Long Duration	Source term ST5: same as ST2, but a long duration (24 hours) release. No economic predictions. The source term for this calculation is identical to the source term used in Case 1 except that the release duration is twenty four hours. In the BNL MACCS calculation, this release is sub-divided into four puffs of equal duration. According to the specifications of June 1992, all released materials have to be uniformly distributed among the puffs.	This case is designed to provide data on the sensitivity of consequences to the duration of release.
C3	Single-Phase, No C/M	Source term ST2. Single-puff release. No counter-measures (no evacuation/relocation, no food disposal, and no farmland interdiction). No economic predictions.	This case predicts consequences of a release with no counter-measures. The results are very valuable for comparisons between different codes where implementation of the specified counter-measures could not be accomplished exactly.
C5	Two-Phase + Energy	Source term ST1. Two-puff release. Energy of release is greater than 0 (plume lift-off). No economic predictions.	In this calculation the materials (same fraction of the total inventory as in the base case) are released in two puffs of different duration. The effect of the release energetics is investigated (plume lift-off).
C6	Low Magnitude	Source term ST3. Single-puff low magnitude release. Radius of Fixed (Evacuation) Area is 5 km (note: in the base case scenario, the radius is 10 km). With economic predictions.	In this case the content of aerosols release is reduced by two orders of magnitude (fraction of released noble gases is reduced only by one order of magnitude). In addition, radius of the sheltering zone is reduced by a factor of two.
C7	Three-Phase	Source term ST4. Triple-puff release. No economic predictions.	In this case, the base case release is split into three identical puffs but with different release times.

*Cases numbers are not contiguous which reflects the evolution of the cases matrix over the life of the project.

Table 2. Source Terms

Source Term	Warning Time* (h)	Release Time (h)	Duration of Release (h)	Energy of Release (W)	Xe/Kr	I	Cs	Te	Sr	Ru	La	Ce	Ba
ST1	1.0	2.0	1.0	2.0E+6	1.0	0.101	0.1	0.05	0.0	0.0	0.0	0.0	0.0
		3.0	5.0	2.0E+5	0.0	0.0	0.0	0.05	0.01	0.01	0.001	0.001	0.01
NUREG-1150**													
BHADBCAADEA	0.36	1.03	0.5	1.9E+6	0.99	0.07	0.072	0.0094	0.0024	4.3E-4	1.2E-4	5.5E-4	0.0027
BHADBCAADDA		2.8	6.1	1.7E+5	0.01	0.047	0.0076	0.033	0.011	3.1E-4	0.0013	0.0014	0.0093
ST2	1.0	2.0	1.0	0	1.0	0.101	0.1	0.10	0.01	0.01	0.001	0.001	0.01
ST3	1.0	2.0	1.0	0	0.1	0.00101	0.001	0.001	1.E-4	1.E-4	1.E-5	1.E-5	1.E-4
ST4	1.0	2.0	1.0	0	1.0	0.03333	0.033	0.033	0.0033	0.0033	0.00033	0.00033	0.0033
		3.0	1.0	0	0.0	0.03333	0.033	0.033	0.0033	0.0033	0.00033	0.00033	0.0033
		5.0	1.0	0	0.0	0.03333	0.033	0.033	0.0033	0.0033	0.00033	0.00033	0.0033
ST5	1.0	2.0	24.0	0	1.0	0.101	0.1	0.10	0.01	0.01	0.001	0.001	0.01

*Time in the table is counted from the time of SCRAM according to the MACCS convention

**This is a two-puff release corresponding to the V-sequence (by-pass) in the NUREG-1150 Study (NUREG/CR-4551) for the Surry-1 nuclear power plant (three-loop PWR). This accident sequence is initiated by a failure of the check valves separating the RCS and the Low Pressure Injection System (LPSI). A release into the environment through the auxiliary building develops following a subsequent failure of the LPSI piping. This source term with some modifications served as a prototype for the International Intercomparison Exercise

Counter-Measures Specifications

The exercise specifications included the following counter-measure scenarios:

a) full circle evacuation from a 10 (or 5) km circle,
b) timed sheltering followed by instantaneous evacuation,
c) exposure criterion for relocation and return of relocatees, and
d) crop bans/crop farmland interdiction based on the specific crop contamination levels.

It should be noted that the last set of specifications—crop bans/farmland interdiction criteria—could not be designed in such a way as to fully accommodate all of the particular input data needs of all codes participating in the exercise.

Calculated Results Requested for Comparison

Three major sets of consequence measures were subject to inter-code comparison: dose predictions, health effects, and economic losses. Some intermediate measures, such as the air and land contamination were also compared. The specific consequences requested for comparisons were collective dose, health effects (e.g., numbers of early fatalities and latent cancer fatalities), effect of counter-measures on people (e.g. total number of people relocated), effect of counter-measures on agriculture (e.g., area of interdicted farmland), and economic effects (e.g., cost of food bans). The results requested from all participants included Complementary Cumulative Distribution Functions (CCDFs) for various effects, as well selected parameters (e.g., percentiles and mean values).

INTER-CODE COMPARISON

Predictions of major measures (end-points) for Case 1 (base case) are presented in Fig. 1. This format of comparison provides an overview of the results across all the important end-points starting from doses to health effects to the results of counter-measures for each case. The observed differences are attributed to differences in modeling and weather sampling techniques employed in the participating codes. Comparisons for three major measures across all cases are presented below. This format is advantageous in the evaluation of the sensitivity of each particular measure to the calculation scenario and source term characteristics.

Doses and Health Consequences

The results predicted for the collective dose calculations for Case 1 show a spread of about a factor of 2 in the mean values. The spread in the 99th percentile values was approximately twice as large resulting from meteorological sampling variations (Fig. 2). Spreads in these results for other cases are of similar magnitude. The large variation observed for the predictions of early health effects was caused by the threshold-type models used in the codes which made the results very sensitive to variations in meteorological samplings. The spread in the predicted latent effects in general reflected that observed in the collective dose predictions.

Economic Consequences

The spread in prediction of the number of relocated people (Fig. 3) was about a factor of four for the mean values and about an order of magnitude for the 99th percentile. The spread is attributed to differences in the meteorological sampling schemes employed by the different codes as well as in the atmospheric dispersion models.

Summary of Codes Inter-Comparison

The magnitude of differences in the predictions of expectation values of various measures (expressed as a ratio of a group's maximum value to the group's minimum value) was generally found to be below a factor of five. The observed differences have been attributed to differences in modeling and weather sampling techniques used in the different codes participating in the exercise.

Figure 1. Codes Inter-Comparison (Mean Values). Case 1: Single Phase, Base Case

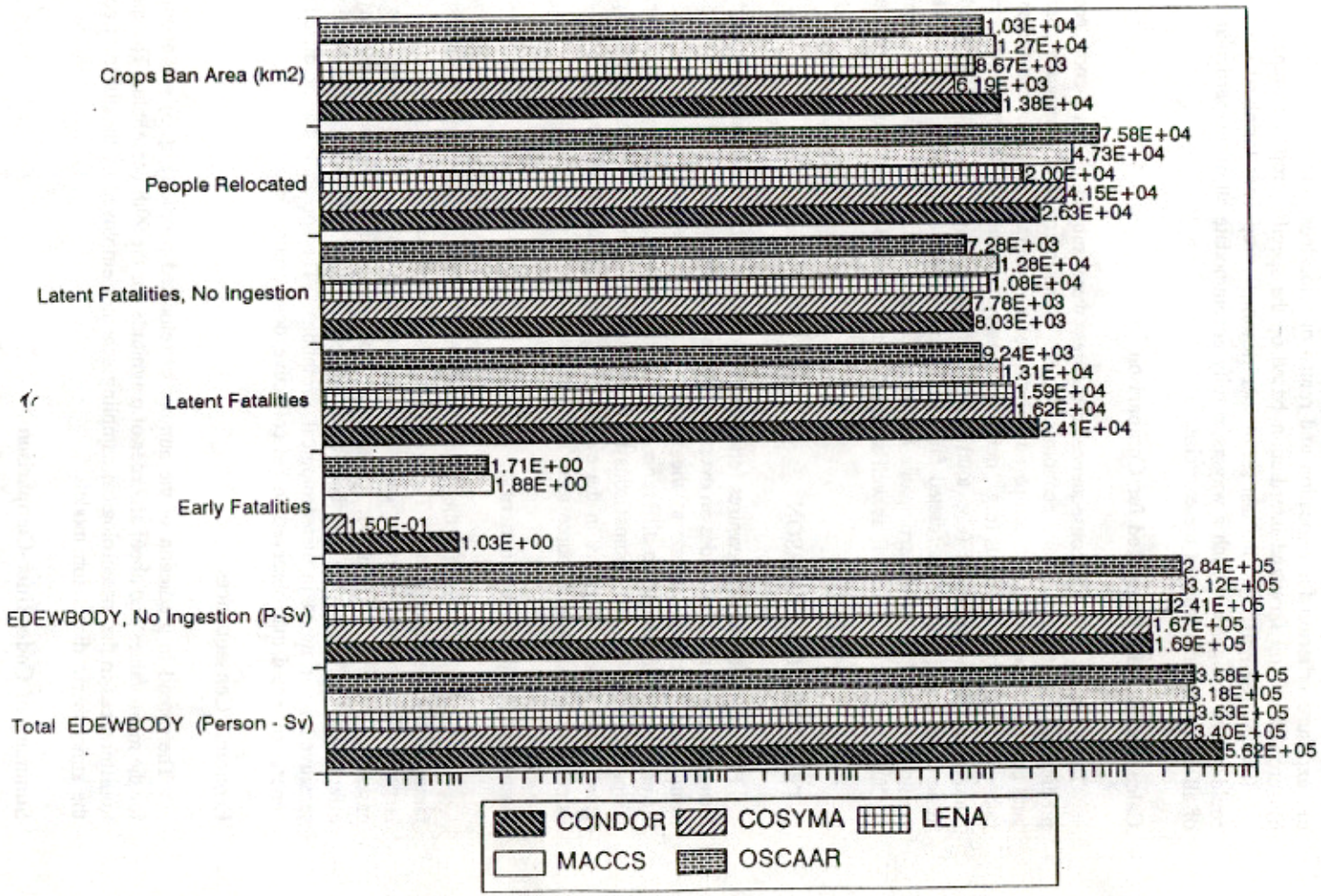


Figure 2. Inter-Code Comparison: Prediction of Total CEDEC

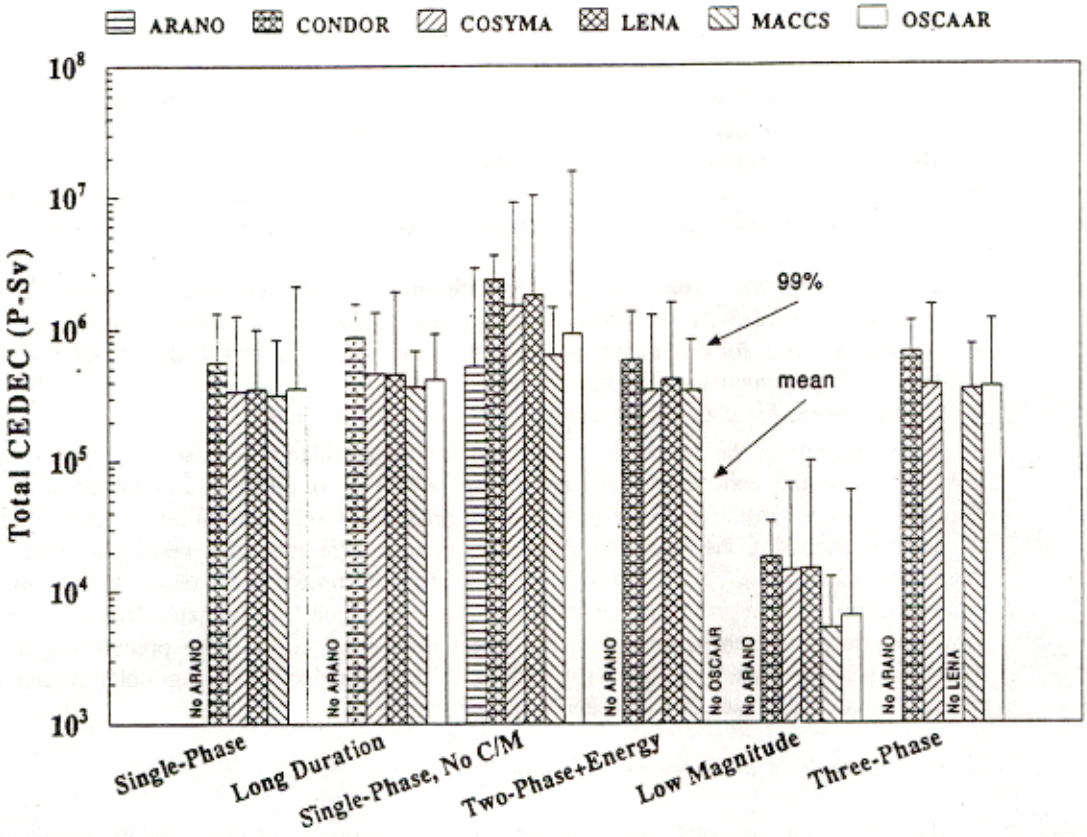
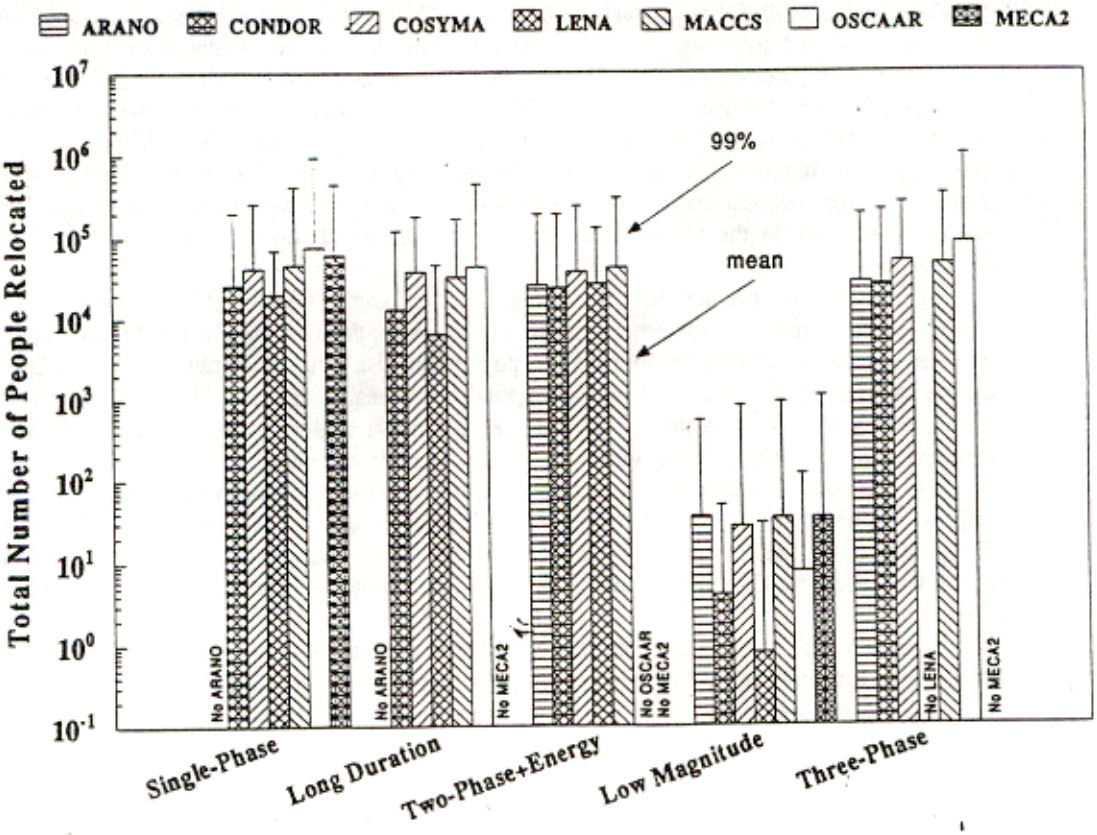


Figure 3. Inter-Code Comparison: Prediction of Total Number of People Relocated



MACCS USERS GROUP COMPARISON

The objectives[4] established for the MACCS Users Group inter-comparison effort included the following:

- demonstrate the **"user-friendliness"** of MACCS enabling the users from different countries to interpret specifications and use them to prepare the input data as well as test the **code's flexibility** in accepting generic specifications,
- screen out and eliminate possible inconsistencies in the input data intended for further use in the calculations performed for the inter-code comparisons, thus providing quality assurance,
- analyze results and explain reasons for differences between the four calculation results, evaluate the sensitivity of results to choices users make in the course of input preparation,
- provide a forum for discussion of users experience in working with the MACCS code and using it's documentation, and
- identify areas for code improvement.

Note that out of the seven cases specified for the calculations, Case 7 was not calculated by MACCS since the code does not have an option for food disposal and farmland interdiction. Counter-measures in the code are based on the predicted **food contamination level.**

Before discussing the results of the comparison for different cases, results obtained for Case 1 (base case, mean values) are illustrated in Fig. 4. The differences in the results are mainly attributed to some differences in grids and population distribution which was extracted from the demographic data separately by each participant. The major differences in the dose predictions (specifically, ingestion pathway dose) are due to variations in interpretation of the agricultural and food dose pathway related data which was specified for the exercise.

Doses and Health Consequences

The predictions of total collective dose are very close for all the calculations with variations attributed to the differences in grids, population distribution, and meteorological data. The major differences in the predicted total societal doses are caused by the ingestion pathway dose predictions, which can be ascertained by comparing Figs. 5 and 6 which show the doses predicted in all six cases. This conclusion is illustrated clearly by Fig. 6 which displays the total doses calculated without the ingestion dose pathway: agreement between the four calculation results is excellent.

Note that in all cases the differences in the ingestion dose predictions did not significantly affect the total dose results. The exception is Case 3 where **no counter-measures were modeled** and the ingestion pathway was an important contributor to the total dose. The differences in the dose predictions are mainly due to differences in the mapping of the agricultural production and in the dose criteria for crop disposal and farmland interdiction. Other causes of differences between predictions are the variations in the values of retention and transfer factors for different crops used by the participants.

Differences in predictions of the number of **early health effects** (early fatalities and hypothyroidism morbidities) are attributed to some variations in the meteorological input files and weather sampling, differences in grids and population distributions combined with the impact of the threshold-type models used for predicting the early health effects. It has to be noted that the differences are greatest in the CCDF's higher percentile regions which is caused by an increased sensitivity of the results to the variations in the weather sampling.

The **number of fatal cancers** predicted **without the ingestion pathway dose** showed very small differences between the four MACCS Users Group results for all six cases. As expected, the differences in the total number of fatal cancers predicted by taking into account the ingestion pathway doses are largest for Case 3 (no counter-measures) resulting from the differences in the ingestion dose predictions.

Similar to the early fatalities predictions, the predictions of **conditional individual risk of latent and early fatalities** as a function of distance agree well with the differences between results increasing at farther distances from the plant site where the effects of differences in the weather sampling become more pronounced.

Figure 4. MACCS Inter-Comparison (Mean Values). Case 1: Single-Phase, Base Case

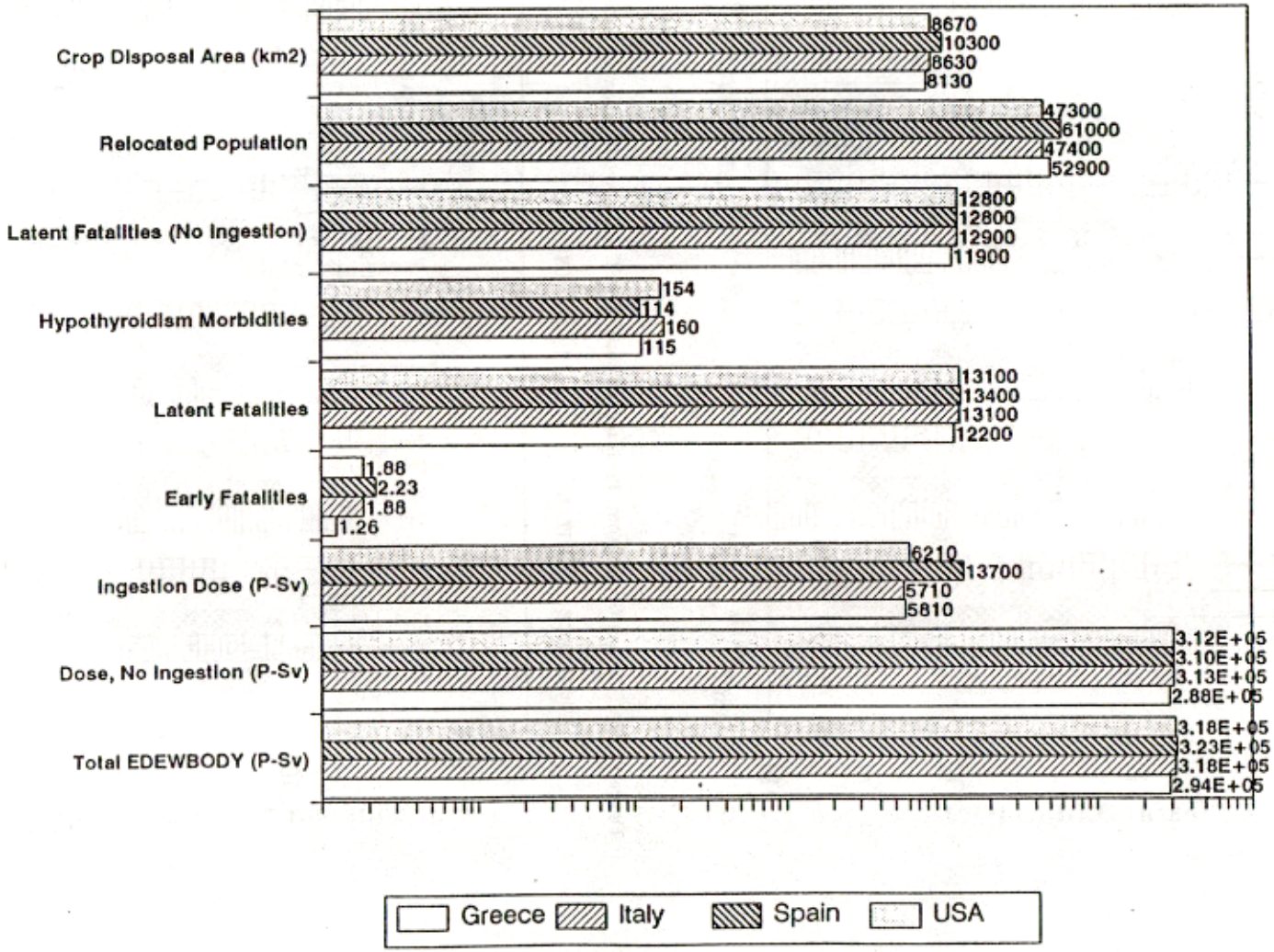


Figure 5. MACCS Inter-Comparison: Prediction of Total CEDEC

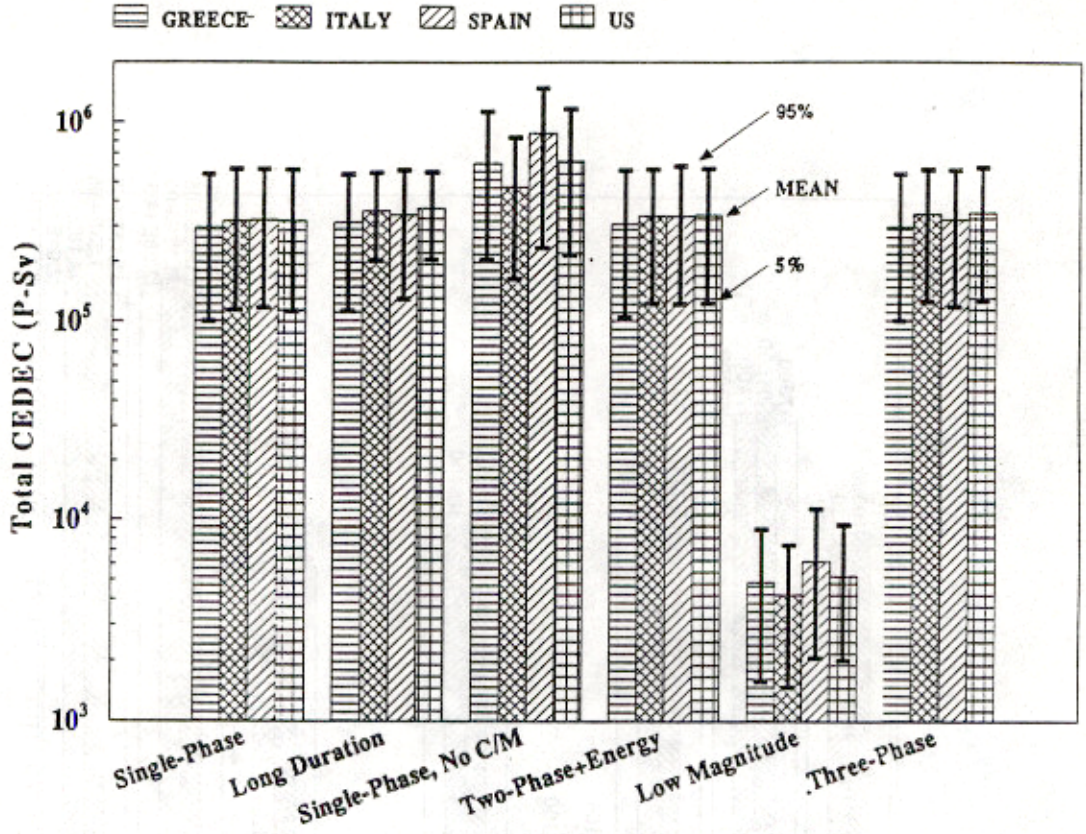


Figure 6. MACCS Inter-Comparison: Prediction of Total CEDEC Excluding Ingestion

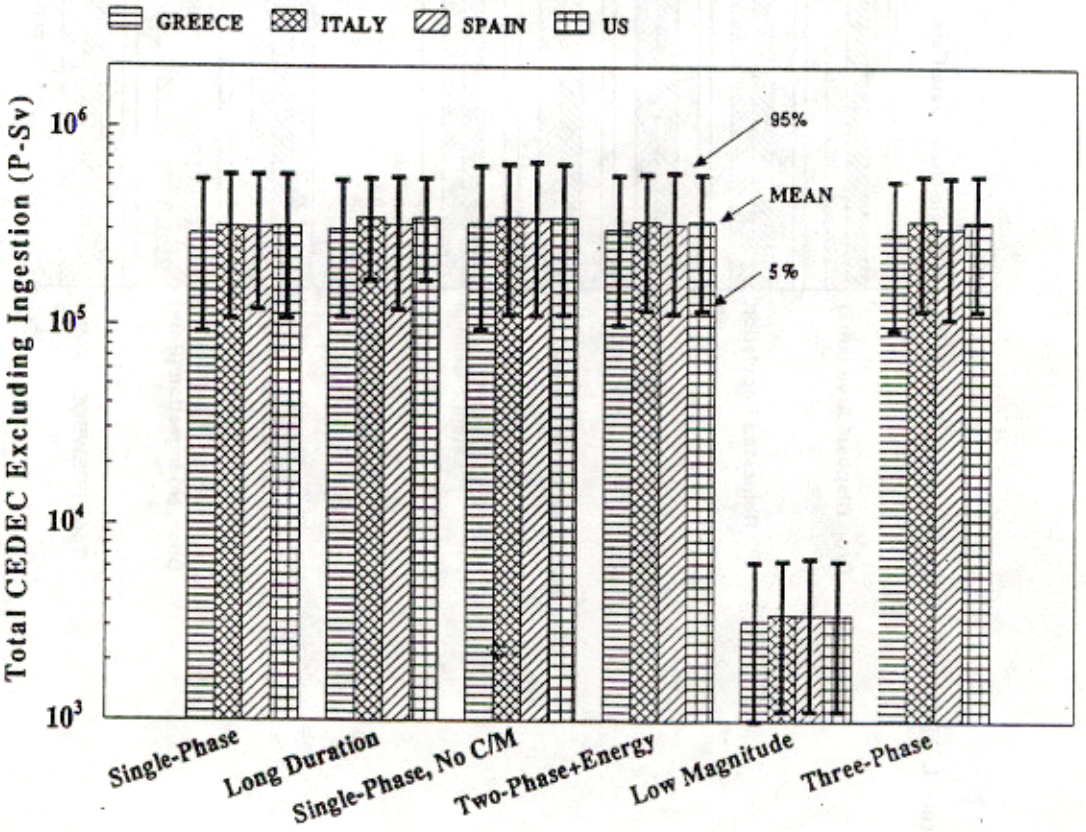
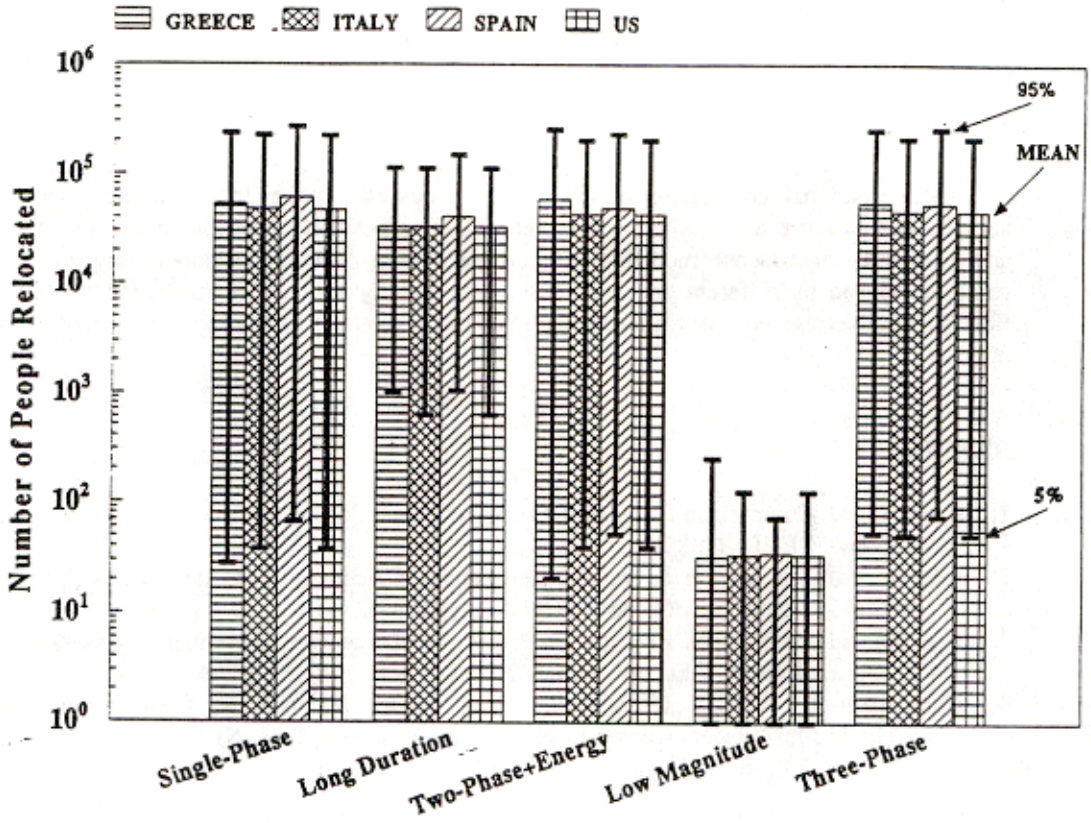


Figure 7. MACCS Inter-Comparison: Prediction of Number of People Relocated



Economic Consequences

The predictions of the **total number of relocated people** for five cases which modeled countermeasures are shown in Fig. 7. The 5th percentile values predicted for the low magnitude release (Case 6) indicate a significant number of weather sequences requiring no relocation (CCDFs show that the median value of number of relocatees is also zero). The differences between the results are attributed to differences in the weather sampling, grids, and dispersion model options.

The differences in predictions of **total costs related to people relocation** are, to a large extent, a reflection of differences in predictions of the number of people relocated since the variations in the unitary relocation costs used in the calculations are not significant. Note that these costs include the values of interdicted land and capital investment and constitute the bulk of population related costs; the daily evacuation costs which depend on the daily cost of evacuation/relocation are insignificant in comparison.

Differences in predictions of **costs of crop disposal** are mainly due to differences in the mapping of agricultural production (homogenized versus distributed) and in the crop banning criteria. Sensitivity calculations for Case 1 (Single-Phase Release) also showed an influence of other factors (meteorological data and weather sampling) on the differences in predictions.

Summary of MACCS Inter-Comparison

In general, good agreement between the results produced by the four MACCS Users Group participants was achieved, with the exception of the results related to the ingestion pathway dose predictions. The main reason for the differences in the latter results is attributed to variation in approaches to implementation of the specifications for the agricultural production and counter-

measures criteria provided for the exercise. Significantly smaller differences between predictions of other consequences can be explained by differences in weather sampling, grids, rain distance intervals, dispersion model options, and population distributions.

CONCLUSION

An international comparison of PCA codes provides a forum for researchers specializing in accident consequence analysis to discuss their technical position on various aspects of dose, health, and economic consequence modeling. The exercise also provides an opportunity to compare the results produced by different codes/countries and identify and explain differences in predictions. Finally, the exercise provides a mechanism for international cooperation in accident consequence modeling.[4]

REFERENCES

1. International Comparison Study on Reactor Accident Consequence Modelling, Nuclear Energy Agency, OECD, (1984).
2. International Comparison Exercise on Probabilistic Accident Consequence Assessment Codes, Overview Report, CEC and OECD/NEA, (1993).
3. International Comparison Exercise on Probabilistic Accident Consequence Assessment Codes, Technical Report, CEC and OECD/NEA, (1993).
4. Comparison of MACCS Users Calculations for the International Comparison Exercise on Probabilistic Accident Consequence Assessment Codes, BNL-NUREG-52380, NUREG/CR-6053, (1993).

QUANTITATIVE GUIDELINES FOR SAFE STORAGE OF A REACTIVE CHEMICAL: AMMONIUM PERCHLORATE

Steven D. Emerson, Ph.D.

Kerr-McGee Corporation
123 Robert S. Kerr Avenue
Oklahoma City, OK 73102

INTRODUCTION

An extraordinary fire and series of explosions destroyed half the U.S. production capacity for ammonium perchlorate (AP) in one afternoon in May 1988. The strategic oxidizer, primarily blended into solid-propellant rocket motors for NASA and the military, suddenly became the subject of intense scrutiny.

The destroyed facility had been operated by Pacific Engineering Production Company of Nevada (PEPCON) since the 1950s. Its sole domestic competitor, Kerr-McGee Chemical Corporation, operated a facility two miles away. As a result of the explosion, Kerr-McGee's plant was temporarily shut down.

Kerr-McGee management promptly began a comprehensive independent safety assessment of its operation. In addition, at a congressional hearing soon after the accident, the company committed to a research program to guide safe manufacturing, storage and transportation of the product. Meanwhile, the need for similar work was identified within the Department of Defense and NASA. Efforts were consolidated after solid-rocket motor manufacturers were invited to participate.

Over the next two years, the joint industry/government research consortium oversaw numerous theoretical studies, laboratory experiments and large-scale field tests. Results of that work were considered in the preparation of company standards now employed at the two Kerr-McGee operations with AP inventory.

BACKGROUND

Ammonium perchlorate, NH_4ClO_4, is a colorless crystalline compound with density of 1.95 g/cc. It is commonly produced by a double decomposition reaction between sodium perchlorate, ammonia and hydrochloric acid, as outlined by Emerson[1]. The article of commerce is shipped as a dry free-flowing bulk powder having nominal particle size of 200μ. To all outward appearances, the product looks like table salt.

Historically, the manufacture of AP has been inextricably tied to electrochemistry. Major strides were made in perchlorate chemistry in the early to mid 1800s. In 1871 Schloesing first produced the ammonium salt of perchloric acid by adding ammonium chloride to sodium perchlorate (Schumacher[2]). Researchers around the world then perfected perchlorate chemistry, so that AP could eventually fulfill its key role in the dramatic development of solid-rocket motors following World War II.

Output of a rocket-motor reaction-engine is measured as "impulse," the product of thrust force and time. It depends on temperature of the hot gases produced and on the molecular weights of the combustion products. AP closely approaches the characteristics of an ideal oxidizer for solid-rocket propellants, having a low heat of formation, high content of available oxygen and a low average atomic weight of components. It is also stable at low temperature, nonreactive at ambient conditions and reasonably insensitive to shock.

Commercial development and manufacture of the product had been largely unremarkable until the PEPCON fire and explosion. This event forced a fundamental reexamination of the safeguards and standards imposed on shipping and storing the energetic product.

REQUIREMENTS

For transportation issues, a U.N. publication[3] delineates standard test protocols for packages such as the 55-gallon drums and 5,000-lb. aluminum tote bins commonly used. The concern is whether the energetic material, in the given container, could undergo transition to detonation under the types of stimuli that might occur in a transportation accident.

Under the joint industry/government research program, three test sequences -- a #8 blasting cap detonation initiator, black-powder ignition source, and five-package external bonfire -- each yielded results indicating that no explosion occurred. The tests confirmed that propellant-grade 200μ AP is appropriately classified as an "oxidizer" according to DOT. Merrill et al[4] provide a complete description of the tests and results.

For storage issues, the subject of this paper, no such definitive guidance from test protocols exists. Instead, the specific hazards to be guarded against must be enumerated and suitable experiments devised to satisfy the inquiry. For the joint industry/government program, a working group of experts, led by Dr. Claude Merrill of the Air Force Astronautics Laboratory at Edwards Air Force Base, planned numerous tests. The objective was to qualitatively (and quantitatively, if possible) define the mass and spacing limits for AP explosive reactions.

The two mechanisms for propagating loss in AP inventory are:

(1) fire spread, and

(2) sympathetic explosion.

The first can occur by either radiant heat flux or by firebrands. Findings from this research suggest that the second can occur primarily by high-speed metallic fragments or, to a lesser extent, by shock wave overpressures.

Contamination of the product with sensitizing agents or fuels can have extraordinary effects. Since 1898, mixtures of AP and fuel oil have been effective commercial explosives. The incentive to maintain integrity of the product during shipping and storage is obvious.

EXPERIMENTS

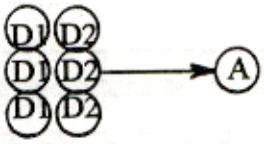
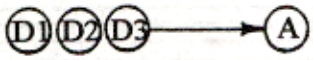
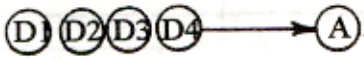
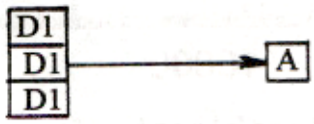
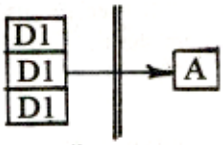
During 1988 and 1989, the research program consumed nearly 330,000 pounds of AP.

Table 1 summarizes results from sympathetic detonation tests.

Essentially, these tests require that a "donor" quantity of AP be initiated to detonation by a sufficiently-sized booster. An "acceptor" package is situated some distance away across an air gap. At close proximity, the acceptor will undergo sympathetic detonation caused by the donor. At far distances, the donor will have no effect on the acceptor. Between the two extremes, a detonation limit distance, S_{50}, exists below which the very violent response occurs from the acceptor, and above which it does not.

The vector of effects from the donor explosion can be somewhat directed, and the ideal explosive velocity within the AP can be approached by using one donor package as an initiating booster for another sitting immediately beside it. The acceptor then is situated across the measured air gap away from the last donor. In such a way, the multiple donor tests (dual, triple, etc.) in Table 1 show the effect of increasing donor quantity.

Table 1. Summary of AP explosion propagation distance as a function of test types and container.

Test Type and Configuration	Container	Max go/ Min no-go	Ratio
E. one-on-one 	500 lb. steel	3.0/3.5 ft.	---
F. one-on-one	500 lb. Al. 0.125"	3.5/4.0	F/E 1.2
G. one-on-one	500 lb. Al. 0.188"	4.5/(5.0)	G/E 1.4
H. one-on-one	500 lb. PE	--/2.0	---
I. dual donor 	500 steel	5.5/6.0	I/E 1.8
J. dual donor	500 PE	1.5/--	J/I 0.5
K. dual donor	500 steel w/plywood	--/3.0	K/I 0.3
L. 3 dual donor 	500 steel	6.0/7.0	L/I 1.1
M. triple donor 	500 steel	6.0/6.5	M/I 1.1
N. quad donor 	500 steel	(6.0)/6.5	N/I 1.1
O. one-on-one 	5000 lb. Al.	28/32	O/E 9.2
P. three-on-one 	5000 lb. Al.	36/40	P/O 1.3
Q. dual donor 	5000 lb. Al.	56/64	Q/O 2.0
R. three-on-one 	5000 lb. Al. concrete wall	--/20	R/P 0.5
S. one-on-one 	5000 lb. Al. concrete wall	--/16	S/O 0.5

By plotting S_{50} on log-log paper, propagation distances for sympathetic detonation of AP in the various storage containers can be seen to depend on:

1) mass of AP in each container,
2) number of containers,
3) individual container construction and configuration, and
4) arrangement.

The commonly used cube root scaling function, $S=kW^{1/3}$, does not conform to the data, (where S is separation distance, k is "risk" factor, W is mass of explosive donor). Instead, the graph suggests that an asymptote is reached with increasing donor quantities for a particular container type. Separation distance is not a straight line upward with a 1/3 slope. (Cube root behavior would apply when an explosion-generated shock wave dampens over three-dimensional space according to the cube root of distance. Equivalently, distance to a comparable shock wave effect would vary with the third power of explosive mass.)

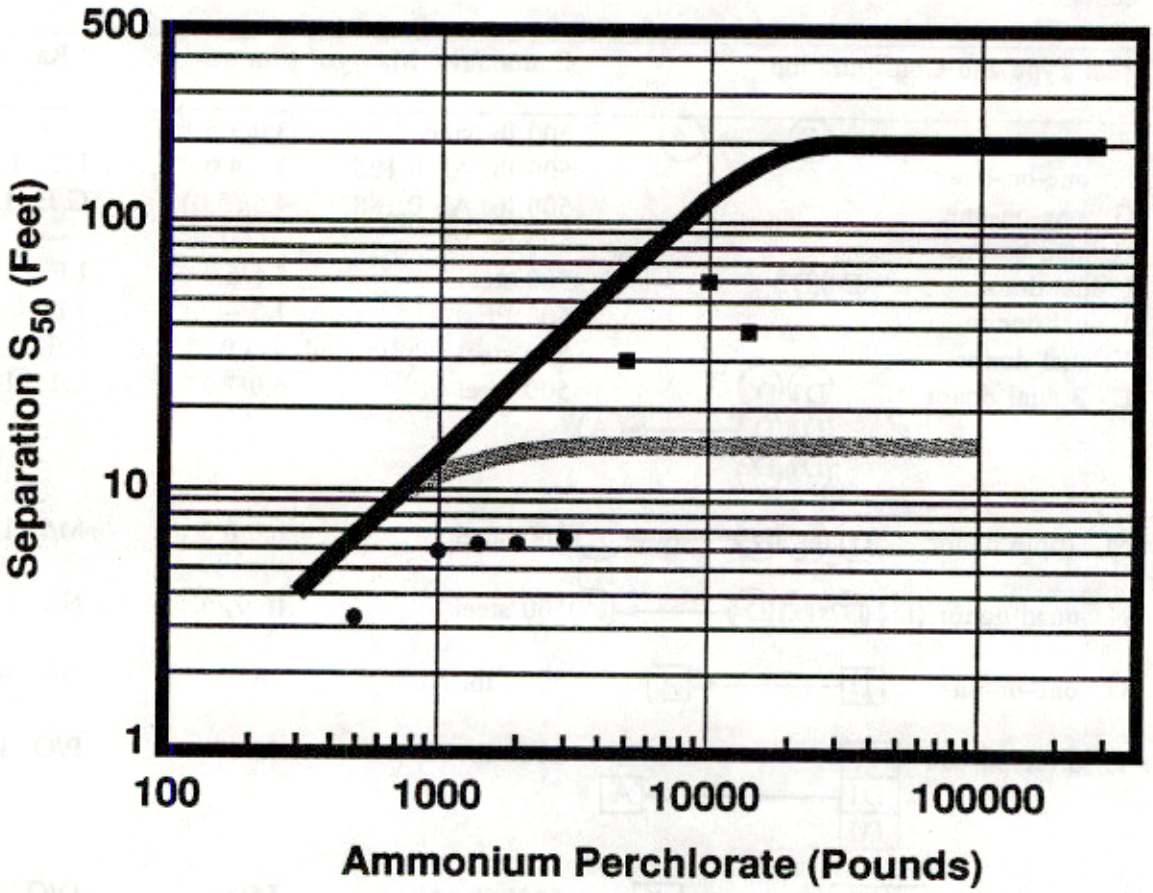


Figure 1. Data graphically depict 50/50 separation distances for 500-lb. steel drums (dot markers) and 5000-lb. aluminum tote bins (square markers). Safe separation distances are shown in solid lines for the two types of containers.

Asymptotic behavior is instead thought due to container fragments flung at very high velocities across the air gap. With sufficient velocity, the fragments impart kinetic energy to the acceptor material, causing localized overheating and initiation of mass detonation. (The results of tests E, F, G and H highlight the effects of different container materials.) Fragment reach is limited by such factors as aerodynamic drag and by the initial explosive

energy of the donor. Multiple donor experiments, e.g. two-on-one compared with one-on-one, suggest that detonation is not well established in single donors. An additional container is necessary as donor for run-up to maximum detonation velocity. This is particularly the case with energetic materials like AP that show imperfect explosive behavior.

For tests with steel drums arranged as sequential donors, the detonation limit distance reached a maximum at 75 inches. Laterally enlarging the donor array to a "sixpack" (test L) extended the S_{50} distance by 13% over the linear donor outcome. This suggests that an ultimate "pancake" donor would probably not show an effect exceeding an extrapolated S_{50} of 85 inches.

It is possible that overpressure could become the dominant mechanism for explosion propagation at very large quantities. This is unlikely, however, because of the geometric limits encountered by simply accommodating the added AP inventory.

In any case, the traditional and reasonable approach for separating energetic materials is to double the S_{50}. Applied to 500 lb. steel drums, the resulting 170 inch (14 ft.) air gap should virtually eliminate explosive propagation between AP stores.

For tests with aluminum tote bins, each containing 5000 lb. AP, the assumption was made that they would behave in similar fashion to the steel drums, that is by establishing an asymptotic limit at three or four linear donor bins. Applying safety factors to the resulting 66 ft. distance for S_{50} and extrapolating to the expected performance of an array, a final cluster S_{50} of 100 feet is established. Thus, a very conservative safe air gap for an inventory of such aluminum bins would be 200 feet.

Finally, tests R and S amply demonstrate the efficacy of frangible walls between inventory -- safe distances can be halved. While destroyed by the donor explosion, the wall evidently attenuates the reach of container fragments.

Separation of inventory to prevent explosion propagation is one issue; separation to prevent fire spread is another. Two DOT classifications exist for energetic materials that burn without explosion: 1.3 mass fire hazard and 1.4 moderate fire hazard. According to tests detailed by Merrill et al[4], commercial AP is properly classified 1.4. The U.N. publication "Recommendations on the Transportation of Dangerous Goods[3]" sets a 50-foot separation distance for above-ground quantities of such material.

Since the explosion protection criteria for 5000 lb. tote bins (discussed previously) set a more conservative distance (100 ft. with wall) than does the fire protection requirement, the explosive guidance will cover both issues. The 100 ft. barricaded/200 ft. air gap distance is applied to any type of inventory, drums or bins.

Finally, the amount of AP per pad is limited such that in the unlikely event of an explosion, effects at the plant boundary can be tolerated. Our Kerr-McGee standard specifies 300,000 lb. per pad, single-stacked, to limit potential blast overpressure effects. Assuming 0.3 tons TNT equivalent per ton AP and using quantity-distance equations from the DoD Contractors' Safety Manual[5] then recommended setbacks are estimated.

$$D_{\text{inhabited building}} = 40 \ (0.3 * \text{Wt. AP})^{1/3}$$

and

$$D_{\text{public highways}} = 24 \ (0.3 * \text{Wt. AP})^{1/3}$$

A setback of at least 150 feet from the nearest plant boundary provides ample safety margin.

CONCLUSION

Criteria have been developed for storage of AP at Kerr-McGee facilities where large inventories can be maintained. For circumstances that differ from those at Kerr-McGee operations, the test data should be considered to arrive at appropriate storage configurations. The experiments provide a wealth of information on behavior of the product and lend confidence to the steps taken to ensure product safety.

ACKNOWLEDGEMENT

Dr. Wilbert J. Robertson provided invaluable counsel in preparation of the storage guidelines. His expertise is gratefully acknowledged.

REFERENCES

1. S. D. Emerson, Continuous Process Manufacture of Ammonium Perchlorate, *Proceedings of the JANNAF Propulsion Meeting*, CPIA Publication 515, May 1989.

2. J.C. Schumacher, "Perchlorates - Their Properties, Manufacture and Uses," Reinhold Publishing Corporation, New York, 1960.

3. United Nations, "Recommendations on the Transportation of Dangerous Goods: Tests and Criteria," (ST/SG/AC.10/11), first edition, 1986.

4. C.I. Merrill, J. Marshall, A.G. Taliancich, W.J. Ledden, Jr., K.L. Woods, "Ammonium Perchlorate Transportation Hazards Testing." Astronautics Laboratory (AFSC), Edwards Air Force Base, California, April 1989.

5. Department of Defense, "DoD Contractors Safety Manual for Ammunition and Explosives," DoD 4145.26-M, DoD Publications System, Washington D.C., 1986.

PROBABILISTIC CONSEQUENCE ASSESSMENT OF POSTULATED ACCIDENTS IN THE DEFENSE WASTE PROCESSING FACILITY USING MACCS2 (U)

Jacqueline M. East and Kevin R. O'Kula

Process Safety Technology Section
Westinghouse Savannah River Company
1991 South Centennial Avenue
Aiken, SC 29803-7657

INTRODUCTION

The Defense Waste Processing Facility (DWPF) at the Savannah River Site (SRS) has been designed and built by the Westinghouse Savannah River Company for the U. S. Department of Energy (DOE) to process high-level radioactive waste from decades of materials production for national defense, space, and medical applications. All of the high-level liquid waste produced at SRS is stored in several different types of tanks on site. Nearly ninety million gallons of high-level waste have been concentrated by evaporation to a present volume of approximately 34 million gallons. Beginning in 1994, the sludge in the waste tanks (which contain most of the radioactivity), along with the radioactive cesium from separations process by-product salts, will be incorporated into borosilicate glass in DWPF.

Prior to the initial phase of operation of DWPF, the Chapter 9 accident analysis section of the Safety Analysis Report (SAR) was significantly revised. The accident analysis now reflects risk-based perspectives, complying with DOE Order 5480.23, *Nuclear Safety Analysis Reports* (April 1992). The revision includes an accident progress event tree (APET) analysis for both internal and external events. These events are postulated and associated frequencies are developed using standard risk evaluation logic models. Source terms are developed from the APET with an algorithm built specifically for modeling postulated accident conditions in DWPF. Once source terms are defined, a consequence analysis methodology is applied to estimate the effects to the general public in the vicinity of SRS.

Both APET and source term algorithm methodologies are based on the NUREG-1150 comprehensive risk evaluation performed in the late 1980s for five commercial power reactors.[1] NUREG-1150 methods were applied for K and N Reactors at SRS and Westinghouse Hanford, respectively, as part of their probabilistic safety assessment programs.

The DWPF source terms are input into deterministic dose models for individual worker and general public consequence calculations. These estimates produce "dose-at-a-distance" perspectives using adverse meteorological and exposure assumptions. However, to evaluate source terms for facility compliance against DOE safety policy contained in Secretary of Energy Notice (SEN)-35-91 (*Nuclear Safety Policy*, September 9, 1991), best-estimate approaches are employed. The MACCS2[2-7] code is used to calculate average co-located worker and average general public risk indices for acute and latent fatality.

NUCLEAR SAFETY POLICY

The DOE safety policy for the neighboring offsite general public was issued in 1991.[8] The safety policy is similar to the NRC safety goal statement[9], and is stated in terms of acute and latent fatality indices applicable to the average individual as a member of the general public neighboring the DOE reservation. The indices of risk are:

> Acute: The risk to an average individual in the vicinity of a DOE nuclear facility for prompt fatalities that might result from accidents should not exceed a tenth of one percent (0.1%) of the sum of prompt fatalities resulting from other accidents to which members of the population are generally exposed. For evaluation purposes, individuals are assumed to be located within one mile of the site boundary. [5×10^{-7} per year]
>
> Latent: The risk to the population in the area of a DOE nuclear reservation for cancer fatalities that might result from operations should not exceed one-tenth of one percent (0.1%) of the sum of all cancer fatality risks resulting from all other causes. For evaluation purposes, the individuals are assumed to be located within ten miles of the site boundary. [2×10^{-6} per year]

The numbers in brackets indicate the numerical value of the risk index for the general public in the vicinity of the DOE reservation.

Worker risk indices are not explicitly stated in SEN-35-91. Quantitative safety policy is still under consideration by DOE for both co-located (neighboring facility) and workers directly involved with the subject facility. In this analysis, the same numerical latent fatality risk goal is applied to onsite, co-located workers as for the general public. The area of applicability is defined by a ten-mile radius from DWPF.

METHODOLOGY

Safety goal estimates are developed by applying the MACCS2, version 1.01 probabilistic consequence assessment computer code. MACCS2 provides complementary cumulative distribution functions (CCDFs) showing a range of dose and health effects depending on the meteorology at the time of the postulated release. The mean health effect is also calculated for measures of consequence. The mean health effect over a population distribution of interest is determined for each DWPF source term, frequency-weighted, and then summed over all internal and external events to produce the compliance risk estimate. Normal operation is included in the analysis.

The MACCS2 has been released by Sandia National Laboratories for U. S. Department of Energy facility evaluation. MACCS2 has an expanded nuclide list to accommodate isotopes beyond those of concern from a reactor perspective, a new decay chain processor, an enhanced emergency response model, and a more complete food ingestion model that accounts for plutonium isotopes in the source term. For the DWPF calculations, input files were constructed to incorporate SRS-specific meteorology, regional crop and other economic mapping, onsite and offsite population distributions, and DWPF-centered grids. Although the development of the source terms used in this analysis include mitigating events to control accidents, in the calculation of doses and health effects no credit was taken for emergency response activities by either the onsite population or the general public.

To accommodate the expanded nuclide list, the traditional MACCS fission product groups could not be used. For this analysis, the new fission product groups were taken from the chemical grouping of fission products in previous MELCOR studies for light water reactors[10] and MELCOR/SR studies for the SRS production reactors.[11]

RESULTS

The individual prompt fatality risk for both the onsite co-located workers within one mile of the DWPF control perimeter and the offsite general public living in the vicinity of SRS was identically zero for the total integrated risk and the normal operational releases.

The mean individual latent fatality risk to co-located workers within ten miles of the DWPF facility control perimeter is 2.4×10^{-7} per individual facility-year of operation for the combined total integrated releases and the normal operational releases. This overall risk value

is well below the draft DOE safety goal of 2.0×10^{-6} per individual facility-year of operation. The mean individual latent fatality risk by initiating event is shown in Figure 1.

The mean individual latent fatality risk to the offsite general public living in the area of SRS is 4.5×10^{-8} per individual facility-year of operation for the combined total integrated releases and the normal operational releases. This overall risk value is well below the DOE safety goal of 2.0×10^{-6} per individual facility-year of operation. The mean individual latent fatality risk by initiating event is shown in Figure 2.

The co-located worker's individual latent fatality risk is higher than the offsite general public individual latent fatality risk as excepted. Since no credit was taken for emergency response in either case, the major differing factor in the analyses was the location of the populations. The co-located workers were evaluated at 10 miles from the facility. The offsite general public does not start for six to twelve miles from the facility, depending on direction. However, the members of the general public traveling along the approximate 33.3 km (20.7 miles) of South Carolina (SC) Highway 125, which transverse the site and at closest approach is six miles from DWPF, are considered in the calculations, but they account for less than 1% of the risk to the total offsite general public.

CONCLUSION

Traditional reactor-integrated risk methods have been applied to the DWPF at SRS. Both the average co-located worker and average general public risk indices for acute and latent fatality were calculated using the MACCS2 code and were found to be below the onsite draft DOE safety goals and offsite SEN-35-91 safety goals. The co-located worker's individual latent fatality risk was higher than the offsite general public individual latent fatality risk as excepted, since no credit was taken for emergency response in either case. The offsite public risk compares to the SEN-35-91 safety goals as follows:

- Individual acute fatality risk within the vicinity of the DWPF (5×10^{-7} per year) is identically zero for the total integrated risk and the normal operational releases.
- Individual latent fatality risk within the vicinity of the DWPF (2×10^{-6} per year) is 4.5×10^{-8} per individual facility-year of operation. The normal operational releases account for 89% of the risk, the internal initiating event releases account for 1% of the risk, and the external initiating event releases account for the remaining 10% of the risk.

The onsite public risk compares to the draft DOE safety goals as follows:

- Individual acute fatality risk within one mile of the DWPF control perimeter (2×10^{-6} per year) is identically zero for the total integrated risk and the normal operational releases.
- Individual latent fatality risk within ten miles of the DWPF control perimeter (2×10^{-6} per year) is 2.4×10^{-7} per individual facility-year of operation. The normal operational releases account for 54% of the risk, the internal initiating event releases account for 4% of the risk, and the external initiating event releases account for the remaining 41% of the risk.

ACKNOWLEDGMENT

This paper was prepared in connection with work done under Contract No. DE-AC09-89SR18035 with the U. S. Department of Energy.

REFERENCES

1. *Severe Accident Risks: An Assessment for Five U. S. Nuclear Power Plants*, Sandia National Laboratory, Albuquerque, NM, NUREG-1150, Vol. 1 (1990).
2. D. I. Chanin, J. L. Sprung, L. T. Ritchie, and H-N Jow, *MELCOR Accident Consequence Code System (MACCS), Volume 1. User's Guide*, Sandia National Laboratory, Albuquerque, NM, NUREG/CR-4691, SAND86-1562 (February 1990).
3. H-N Jow, J. L. Sprung, J. A. Rollistin, L. T. Ritchie, and D. I. Chanin, *MELCOR Accident Consequence Code System (MACCS), Volume 2. Model Description*, Sandia National Laboratory, Albuquerque, NM, NUREG/CR-4691, SAND86-1562 (February 1990).
4. J. A. Rollistin, D. I. Chanin, and H-N Jow, *MELCOR Accident Consequence Code System (MACCS), Volume 3. Programmer's Reference Manual*, Sandia National Laboratory, Albuquerque, NM NUREG/CR-4691, SAND86-1562 (February 1990).
5. D. I. Chanin, *A New Emergency Response Model for MACCS*, Technadyne Engineering Consultants, Albuquerque, NM (November 1992).
6. D. I. Chanin and J. Foster, *Expanded Nuclide List in MACCS2*, Sandia National Laboratory, Albuquerque, NM (draft, April 1993).
7. J. A. Rollistin, *New Food Pathway Model for MACCS*, Sandia National Laboratory, Albuquerque, NM (draft, April 1993)
8. *Safety Goals for the Operation of Nuclear Power Plants*, Policy Statement, Federal Register, Vol. 51, No. 149, August 4, 1986, pp. 28044-28049.
9. *Nuclear Safety Policy*, U. S. Department of Energy Secretary of Energy Notice SEN-35-91 (September 9, 1991).
10. D. A. Powers, *Fission Product Behavior During Severe LWR Accidents: Modeling Recommendations for the MELCOR Code System, Volume I: Fission Product Release From Fuel*, Sandia National Laboratory, Albuquerque, NM, pp. 2-43, NUREG/CR-4481 (SAND85-2743) (September 1988).
11. R. C. Smith, *MELCOR Primer: Radionuclide Package Users' Guide, Version 1.8.1 + SRIMod4*, Sandia National Laboratory, Albuquerque, NM, pp. RN-UG-4, SAIC 92/6506 (May 1992).

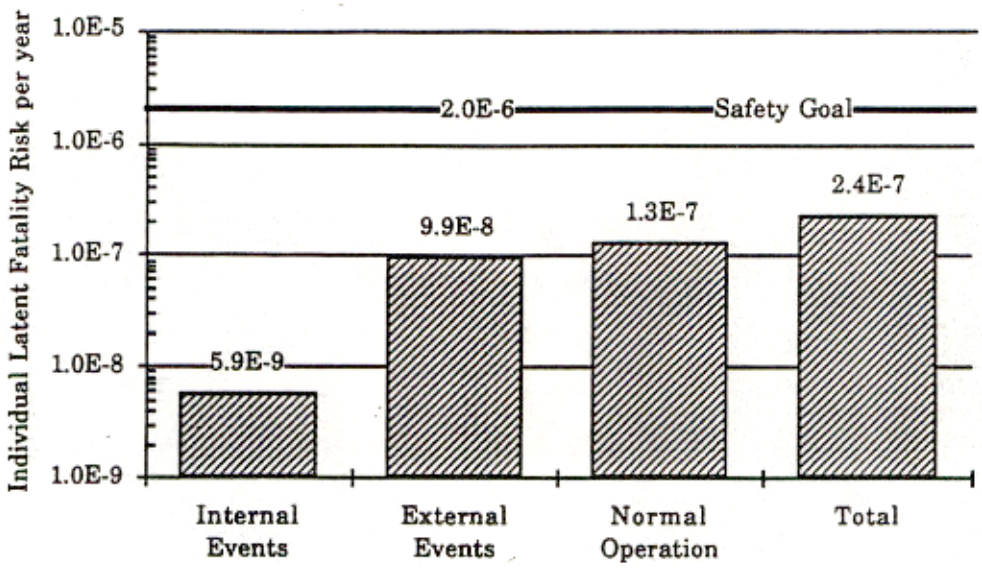


Figure 1. Individual Risk to Co-Located Workers within Ten Miles of DWPF

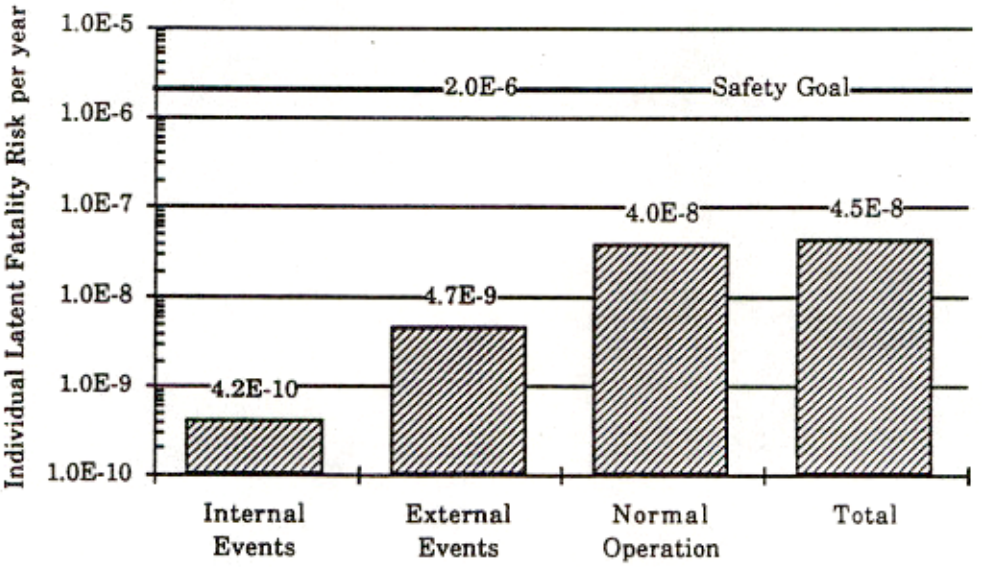
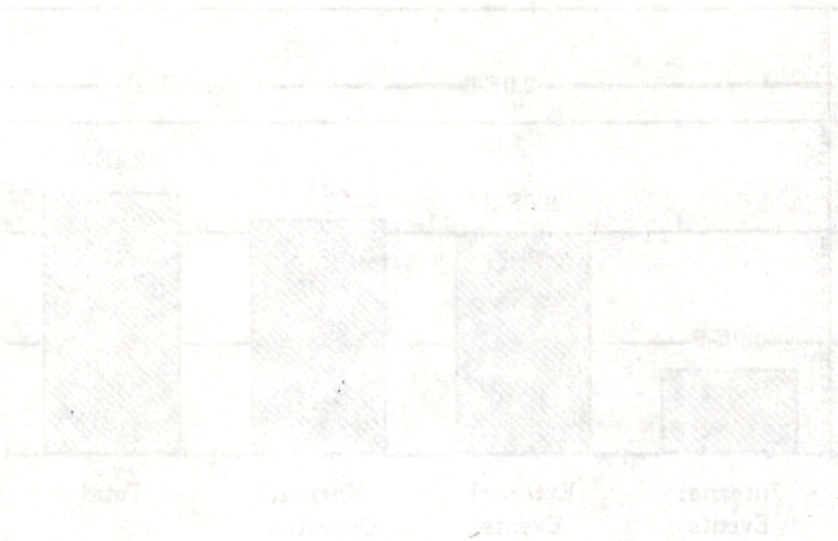


Figure 2. Individual Risk to General Public within Ten Miles of SRS Boundary



031 Computerized Monitors and Operator Aids (II)

Chair: L. Norros, VTT Finland

Evaluation of Computerized Emergency Operating Procedure Systems as an Operator Support in Nuclear Power Plants

P. Moieni (Accident Prevention Grp.); A.J. Spurgin

DIMOS: A New Generation of Nuclear Power Plant Process Monitoring Systems

M. De Vlaminck, B. Gilliot (Belgatom, Belgium)

Risk Management Insights from the Development and Use of the San Onofre Safety Monitor

T.A. Morgan (Haliburton NUS); T.G. Hook, R. Lee (S. Cal. Edison)

COSMIC Modelling with Personal Computers

R. Strong (Safety Analysis Sys.)

EVALUATION OF COMPUTERIZED EMERGENCY OPERATING PROCEDURE SYSTEMS AS AN OPERATOR SUPPORT IN NUCLEAR POWER PLANTS

Parviz Moieni,[1] and Anthony J. Spurgin[2]

[1]Accident Prevention Group
16980 Via Tazon, Suite 110
San Diego, CA 92127
[2]Consultant
4252 Hortensia Street
San Diego, CA 92103

INTRODUCTION

This paper describes the results of Phase I of a study performed under an NRC-sponsored Small Business Innovative Research (SBIR) project on evaluation of Computerized Emergency Operating Procedures (CEOP) systems[1]. An integral part of the study was to understand individual advantages, disadvantages, and limitations of computerized EOP systems in terms of their potential positive and negative impact on Nuclear Power Plant (NPP) control room operators' performance, as well as reliability of each of these systems. A literature survey was conducted and discussions were held with designers/developers of CEOP systems to obtain information on system design and reliability, operation, verification and validation (V&V), and status.

BACKGROUND

Following the Three Mile Island (TMI) Unit #2 accident in March 1979, the nuclear industry went through a program aimed at enhancing plant safety and operability. The procedures were part of this program, along with control room human factors improvements and requirements for plant specific simulators. These improvements have led to the development of what is known as symptom-based procedures. As implied, these procedures deal with the symptoms of an accident rather than its cause. Under the old event-base EOPs, the crew was forced to diagnose the cause of the accident and then deal with it. This could be a difficult task, particularly in the case of multi-failure scenarios. The advantage of the symptom-based EOPs is that they can deal with multi-failure accident scenarios.

To use the symptom-based procedures, however, the crew must continuously monitor the plant and observe changes in the symptoms, compare these with the procedure requirements, and take the appropriate actions. This means that the work load of the crews has changed from diagnosis and selection of the appropriate procedure to continuously monitoring the plant, reading the procedures and adjusting the response until the plant is stabilized.

With the advent of powerful and relatively inexpensive computers and the development of expert system techniques, it is possible to use these devices to support the crews in using the new symptom-based procedures. Computers can make up for some of the human limitations, such as short term memory and limited workload capacity, and together with the human operator can be more effective and reliable than either operating separately. Thus, computers can help the user find his way through the procedures, and help ensure that steps in the procedures are taken in the correct sequence. More importantly, they can support the crew in taking into account the correct set of symptoms, and help ensure that key elements are not ignored. In some systems, the computer can take control if the crew fails to follow the procedures as prescribed.

This, then, led to the concept of procedure support systems. Early concepts for computer-based operator supports were: the Disturbance Analysis System (DAS) developed by the Electric Power Research Institute (EPRI)[2], a similar concept by Halden (Norway)[3], and the STAR system developed by GRS (Germany)[4]. Although these systems were operator support systems, they were based on the use of disturbance analysis (*i.e.*, determining what caused the accident). The approach taken was based on a development of the cause-consequence analysis technique. These systems failed to go into operation, although a partial test of STAR was carried out in Germany at a nuclear power plant.

The next development took place under an extension of the original EPRI DAS project, the Disturbance Analysis and Surveillance System (DASS)[5]. During this project, the first symptom-based procedure support system was developed for a BWR plant and was based on the BWR owners group emergency procedures guidelines (EPGs). This application was part of a comprehensive project based on advanced display technology. Later, EPRI developed the EOP Tracking System (EOPTS)[6], from the experience with this application.

DESIGN AND OPERATION ASPECTS OF CEOP SYSTEMS

The basic function of a CEOP system should be to support control room operators' performance and reliability, and as a result, maintain or enhance overall plant reliability. CEOP systems may have additional objectives such as reducing crew work-load, supporting reduced crew size, aiding in procedure usage, and expanding and enhancing training; for example, moving from detailed training in procedure use to a deeper understanding of the physical processes and ways to manage accidents.

A CEOP system may be designed with different levels of sophistication and support to the control room operating crews. It may be simply a set of digitized EOPs with no on-line (i.e. interface with plant) capability that would simply provide EOPs on a computer screen. It may be a passive on-line operator support system that would assist operators in selecting and following EOPs as well as provide information on plant status at any time. The system may, on the other hand, be an active on-line support system that would perform diagnostic activities and identify the proper EOPs and actions to be taken by the crew. Active systems should provide operators with the capability to control the plant using paper EOPs and other support systems, if the computerized EOP system fails.

The CEOP system consists of the hardware (computer system), the software, the human-system interface (HSI), and the user. Hence, the overall reliability of the system depends on reliabilities of each of these components. Obviously, the specific needs of the user must be addressed through the interface.

The features, performance, function, use and reliability of a CEOP system as a support to crews during accidents are especially important, and this project focused on the reliability of CEOP systems and their users as well as the potential influence of CEOP systems on control room crew structure and reliability in emergency situations. The study found that, although a great deal of attention has been paid to the design of these systems from a "system specification" point of view (both hardware and software), it appears that not as much attention was given to the reliability and human factors design of these systems. Preliminary reliability models for CEOP systems were developed.

A SIMPLE CEOP SYSTEM RELIABILITY MODEL

When a comparison is made between reliability of operating crews using paper EOPs or computerized EOPs, it is important to have a model for prediction of reliability of CEOP systems. Of course, the overall crew reliability depends on how the CEOP system is designed and used by the operating crew. A simple model is presented for the assessment of reliability of CEOP systems. The failure probability of the system is broken into three elements (or causes):

a. Failure probability of the system equipment (or hardware), p_E.

b. Failure probability of the system function (or software), p_F. This

represents the probability that the CEOP system does not perform the correct function, due to either a knowledge base or a software error. This term can be reduced by system validation.

c. Failure probability of operator (or human) in using the system, p_H. This could be due, for example, to the design of the human-system interface, or the user's lack of knowledge. This term can be reduced by adequate human factors design of the interface, and by training.

The failure probability (or unreliability) of the CEOP system can be simply expressed as follows:

$$p_{CEOP} = p_E + (1 - p_E)\, p_F + (1 - p_E)(1 - p_F)\, p_H \qquad (1)$$

Each term in Equation (1) can be further broken into more basic terms. For example, simple reliability models or fault trees can be produced for p_E which include failure probabilities associated with various hardware components. Similarly, human reliability models can be used for the term p_H. However, this simple model was kept at this level for Phase I of the project.

A detailed evaluation of software reliability is beyond the scope of this project, but it is being widely addressed elsewhere[7]. Note, however, that in addressing software reliability, the usual random failures and hardware age-related phenomena which affect reliability do not apply, and hence, the corresponding methods of assessing failure rates (or probabilities) by testing systems may not be appropriate. Software does not age, but it can suffer from design faults, early failures, and software upgrade failures equivalent to the infant fatalities and maintenance-induced failures of hardware. See Levinson and Daughtrey[7] for a discussion on software reliability evaluation.

As stated earlier, overall crew reliability depends on how the CEOP system is designed and used by the operating crew. In this phase of the project, two cases were considered: 1) the CEOP system is used by the Shift Supervisor (SS) or Shift Technical Advisor (STA) as a supplement to the paper EOPs used by the Senior Reactor Operator (or procedure reader), and 2) the CEOP system is designed to completely replace the paper EOPs (although they remain available as a backup in case of CEOP system failure).

Case 1: CEOP system as a supplement to paper EOPs

In this case, the CEOP system provides a vehicle for the SS or STA to check the decisions and actions of the operating crew and provide a recovery mechanism in case of a crew error. In this case, the crew reliability estimate (or HEP) is enhanced by a new recovery factor (*i.e.*, the CEOP system unreliability presented by Equation (1)). Mathematically:

$$HEP' = HEP \cdot p_{CEOP} \qquad (2)$$

where:

HEP' = Human (operating crew) error probability supported by a CEOP system

HEP = Human (operating crew) error probability using paper EOPs

p_{CEOP} = Failure probability (or unreliability) of the CEOP system

In this case, p_{CEOP} is further simplified by replacing its p_H term with p_{SS}, which simply represents the SS (or STA) error in using the CEOP system.

Case 2: CEOP System as a Replacement to Paper EOPs

Here, the crew reliability is essentially represented by the CEOP system reliability as shown by Equation (1). It is, however, noted that the p_H term in Equation (1) represents operating crew reliability in using the CEOP system. Another consideration in this case is whether, if the CEOP system fails (*i.e.*, equipment failure), the operating crew is able to transfer back to the paper EOPs. In this case, system failure is backed up by a recovery factor representing

the operating crew using the paper EOPs. Mathematically:

$$HEP' = P_E [P_{NT} + (1 - P_{NT}) \cdot HEP] + (1 - P_E)P_F + (1 - P_E)(1 - P_F) P_H \quad (3)$$

Where:

P_{NT} = Probability of crew not transferring to paper EOPs.

It is noted that the estimates for HEP for cases when the CEOP system does not exist versus when it fails could be different even using the same human reliability models. This is mainly due to the fact that in the latter case, the operating crew may not be as familiar (or trained) with the paper EOPs. The model presented here will be revisited during Phase II of the project.

CHARACTERISTICS OF REVIEWED CEOP SYSTEMS

A literature review was conducted to obtain information on various features of the CEOP systems currently being designed, developed, and evaluated. During the review of the computer-based EOPs, it was found that there were some expert systems which could be considered similar in intent to the CEOP systems. These were included in the review, even though they are not strictly EOP based. Following the literature review, CEOP system designers were contacted to obtain additional information about the identified systems. Table 1 summarizes the characteristics of the CEOP systems reviewed as part of this research project. A brief description of these systems can be found in Reference 1.

Our review indicated that there are two main types of CEOP systems. Each is intended to help the operators during their responses to accidents, and to replace hard copy EOPs. One requires that the operators follow instructions given by the computer, whereas the other provides advice to them in determining their course of action. In practice, the distinction between these two types can disappear, depending upon the roles and responsibilities of the operating crew at a specific plant. The CEOP system designed by Electricité de France[8] is the only known system of the first type. There are a number of CEOP systems of the second type, such as EPRI's EOPTS[6]. Although systems of the second type are similar in concept, there are differences among them in specific implementation. These differences are discussed in detail in Reference 1.

DISCUSSION

The introduction of the CEOP system is one step in the process of upgrading the control room HSI being taken by the utilities and nuclear power plant suppliers. These upgrades are being driven by the need to change from analog and mechanical systems to digital systems because of availability and performance needs. A large number of utilities have already upgraded their plant computers and in the process have added a number of functions to support operations. In addition, digital control systems have been added in many plants, such as the digital feedwater control system. Also, instruments have been added in compliance with the NRC initiatives following the TMI-2 accident, such as ultrasonic detectors on safety valves. These changes have taken place in a somewhat piecemeal manner, and often the displays and controls are not integrated.

The user's confidence in CEOP systems is a function of the demonstrated system capability to provide the correct advice to the crew during simulated multi-failure scenarios. This could be done by validating the CEOP systems with a number of crews exposed to a variety of scenarios on the plant simulator. A comprehensive CEOP system validation would help eliminate potential design and software errors, which could defeat a key benefit of the CEOP system, a reduction of HEPs.

This preliminary research may be useful to potential users of CEOP systems (*e.g.*, nuclear power utilities) to help them evaluate how such a system might fit their needs; how to integrate one into their operation; how to validate it; and how to determine its potential impact on operating crew reliability and training. The research also provides the first steps toward a framework for evaluation of the safety implications of CEOP systems.

Acknowledgments

This paper is based upon work supported by the U.S.Nuclear Regulatory Commission. Any opinions, findings, and conclusions or recommendations expressed herein are those of the authors and do not necessarily reflect the views of the NRC. A Phase II contract has been awarded to APG and is currently underway. The authors thank Jerry Wachtel of the NRC for his contributions, and the CEOP system designers for providing information on the systems.

REFERENCES

1. P.Moieni and A.J. Spurgin, *Computerized Emergency Operating Procedures Research*, prepared for U.S. Nuclear Regulatory Commission, NUREG/CR-XXXX, Draft Report,(1993).
2. C.Meijer and B.Frogner, *On-Line Plant Alarms and Disturbance Analysis System*, EPRI Report NP-1379, Electric Power Research Institute, Palo Alto,CA,(1980).
3. K. Netland and J.E. Lunde, "Experimental Operation of the Halden Reactor, Utilizing a Computer and Color Display-Based Control Room", *Proceedings of the Specialists Meeting on Control Room Design*, San Francisco, CA,(1975).
4. W.Bastl, "STAR Disturbance Analysis Results from Grafeniheinfeld PWR Application", *IAEA International Symposium on Nuclear Power Plant Control and instrumentation*, IAEA SM-265, Munich, Germany, (1982).
5. A.J.Spurgin, D.G. Cain and A.B. Long, "Decision Making Aid for Operational Crews - Status of the EPRI DASS Project", *IAEA Symposium on Nuclear Power Plant Control and Instrumentation*, Munich, Germany,(1982).
6. W.Petrick,K. Ng, and C. Stuart, *Emergency Operating Procedures Tracking System (EOPTS)*, EPRI NP-5250, Electric Power Research Institute,(1987).
7. S.H. Levinson and H.T.Daughtrey,"Risk Analysis of Software-Dependent Systems", *Proceedings of PSA'93,International Topical Meeting on Probabilistic Safety Assessment*,Clearwater Beach,FL,(1993).
8. P.Lebot, *et al.*, "Developpement et Test sur Simulateur Pleine Echelle de Procedures de Conduite Accidentelles Informatisees Pour la Nouvelle Salle de Commande du Palier Rep 1400 (N4) d'EdF", *Proceedings on an International Symposium on Balancing Automation and Human Action in Nuclear Power Plants*, International Atomic Energy Agency, Vienna,(1991).
9. A.J.Spurgin, *et al.*, *The BWR Emergency Operating Procedures Tracking System (EOPTS): Evaluation by Control-Room Operating Crews*, EPRI NP-6846, Electric Power Research Institute,(1990).
10. J.Teigen and P.E. Ness, "The Computerized Procedure System COPMA-II", presented at the *IAEA/IWG-NPPCI Specialists' Meeting on Operating Procedures for Nuclear Power Plants and Their Presentation*, Vienna, Austria,(1992).
11. Y.Yamamoto, "Development of Computerized Emergency Response Guidelines Support System for Japanese PWRs", presented at the *OECD Specialist Meeting on Operator Aids for Severe Accident Management and Training*, Norway,(1993).
12. N.Netsu, *et al.*, "Development of Symptom-Based Emergency Procedure Guideline Support System", presented at the *OECD Specialist Meeting on Operator Aids for Severe Accident Management and Training*, Norway,(1993).
13. Y.Takizawa, *et al.*, "A Post-Trip Operational Guidance System for BWR Plants", *Nuclear Engineering and Design*, 110, pp. 385-393,(1989).
14. W.Malfaro and A. Zygmont, "IRIS: An Expert System to Aid Nuclear Operators", presented at *EPRI Conference on Expert Systems Applications for the Electric Power Industry*, Orlando, FL(1989).
15. L.Mampaey, *et al.* "Operator Advisor: An Expert System to Reduce Human Error in Emergency Response", *Proceedings of the International ENS/ANS Conference on Thermal Reactor Safety, NUCSAFE 88*, Avignon, France,(1988).
16. M.H.Lipner, F.S. Pitcairn and R. Bastien, "Computerized System for Procedures Execution Monitoring", presented at *IAEA/IWG-NPPCI Specialists' Meeting on Operating Procedures for nuclear Power Plants and Their Presentation*, Vienna, Austria,(1992).
17. J.O.Yang and S.H. Chang, "A Decision Support System Based on Hybrid Knowledge Approach for Nuclear Power Plant Operation", presented at *EPRI Conference on Expert Systems Applications for the Electric Power Industry*,Orlando,FL,(1989).
18. B.K.Hajek, *et al.*, "A V&V Program for a Real Time Operator Advisor Expert System", presented at *EPRI Conference on Expert Systems Applications for the Electric Power Industry*, Orlando, FL,(1989).

Table 1. Features of Computerized EOP/Expert Systems

ATTRIBUTE	SYSTEM											
	EPRI BWR EOPTS-Kuosheng [8,9]	EPRI EOPTS/TVA Browns Ferry	EdF N4 Reactor System [9]	Halden COPMA [10]	Japanese BWR Kansai Electric [11]	Japanese BWR Tokyo Electric [12]	Japanese BWR PTOG System [13]	BWR IRIS (Villanova University) [14]	PWR OPA (Tractebel) [15]	Westinghouse COMPRO [16]	Korean PWR HYPOSS [17]	Operator Advisor (Ohio State Univ) [18]
Based on EOPs	Yes	Yes	Yes *	Yes (EOPs, AOPs & OPs)	Yes, both event & symptom	Yes	Yes, symptom based	No	Yes, based on W EOPs	Yes, All procedures	Yes, both event and symptom	Yes, EOPs, AOPs & OPs)
Knowledge-based	No	No	No	Yes, Prolog & LISP	Yes		No	Yes	Yes	No	Yes, SD-Prolog	Yes
Use = Training/ Operations/ Research	Training first, operations later	Training	Both	Operations	Operations	Training?	Operations?	Training	Research	Training/ Operations/ Maintenance	Operations	Operations/ Research
Use = Simulator or Plant	Simulator (later plant)	Simulator	Both	PWR Simulator	Plant	Plant	Plant	?	?	Plant	Plant	Plant
User = Shift Supervisor or Operator	Shift Supervisor	Shift Supervisor and Operations	Operator with Shift Supervisor overview	Operators	Operators	Operators	Operators	Operators	Operators	Operators/ Maintenance	Operators	Operators
On-line or Off-line	On-line	On-line	On-line	On-line	On-line	On-line	On-line	Off-line	On-line	On-line	On-line	On-line
Active or Passive	Passive	Passive	Active	Passive **	Passive	Passive	Passive	Passive	Passive	Passive	Passive	Passive
MMI = CRTs/other	CRTs	CRTs	CRTs	CRTs	CRTs flow chart	CRTs	CRTs & voice ann	PC-CRT	PC/AT-CRT	CRTs	IBM-PC/AT	?
Unit fails?	Use paper procedure	Use paper procedure	?	Use paper procedure	Use EOP manual	Use EOP manual	Use EOP manual	?	USE EOPs	Use procedures	Use EOP manual	Use procedures
Validated?	Validated (Kuosheng simulator)	Validated (Kuosheng simulator)	Validated at Bugey (53C simulator)	Validated at NCS University Test Facility	Validated 199 at full scale simulator	Some validation	Validated BWR simulator	Not validated	Not validated (to be, at Belgium simulator)	?	Some validation using plant simulator	Partly validated using Perry simulator ****
Prototype or Commercial	Kuosheng	TVA Browns Ferry	Commercial, Chooz B1	Prototype ***	Commercial	Commercial	Prototype	Prototype	Prototype	Prototype	Prototype	Prototype

* Based on integrated procedures for normal and accidental plant conditions

** The user (*i.e.*, operator) generally has to work with a set of activities (or actions to be executed). It is up to the user to decide which activity is the most urgent one (*i.e.*, the system does not prioritize the action)

*** Experimental control room facility HAMMLAB and ENEA's Lab on a PWR simulator

**** Future validation will involve operators performing with and without the Operator Advisor

DIMOS: A NEW GENERATION OF NUCLEAR POWER PLANT PROCESS MONITORING SYSTEMS

M. De Vlaminck and B. Gulliot

Belgatom
Avenue Ariane 7
B-1200 Brussels, Belgium

INTRODUCTION

A new generation of nuclear power plant supervision systems, called DIMOS (DIstributed MOnitoring System) has been installed at the Doel nuclear power plant (Belgium) and has been monitoring reactors 1 and 2 since August 1991 and reactor 3 since July 1993.

DIMOS is progressively replacing the process computers designed in the 70's, which have reached their technical and functional limits. Indeed, the costs and risks associated with their maintenance have become unacceptable and the increasing demand from the plant management to extend the system for providing high level plant information to the operator could no longer be fulfilled due to the hardware and software limitations.

In 1987, the Belgium power utility ELECTRABEL decided to launch the study of a new generation of plant monitoring systems that would focus on the two following aspects;

- increasing the power plant safety by providing better access to the plant information;
- increasing the profitability of the plant by improving the effectiveness of the operators.

Due to its high level of flexibility, extensibility and quality, the system that has been developed is able to protect the long term investment and allows installation of similar systems at other power plants.

Furthermore, due to the success of the first installation of DIMOS in Doel 1 and 2, ELECTRABEL decided in March 1992 to replace the process monitoring system of Doel unit 3 by a DIMOS system that was installed in July 1993.

USER'S REQUIREMENTS

The objective of DIMOS is to handle the raw information available within the plant in order to help the operators monitor its operation.

This means that the system will have to :

- validate the information by assessing its level of confidence;
- synthesize the information by performing functional gathering and high level monitoring function processing (e.g. critical safety functions, automatic sequences supervision functions ...);
- filter the available information in order to reduce the mental work load of the operators.

The Man-Machine Interface of DIMOS must be designed to optimally visualize the right information in the right place. Hence, it must be distributed throughout the user's work areas (control room, technical support center, chemistry laboratory, ...).

In order to be linked with other operator support systems, DIMOS must have an open architecture.

DIMOS must also be configurable to allow its customization for a specific installation and its modification during plant operation.

Finally, as DIMOS would be the basic operator support system, its reliability and therefore its availability must be high.

OPERATIONAL CHARACTERISTICS

Starting from the information available in the plant, which is transmitted to DIMOS via the acquisition system, calculation processes reconstitute the basic physical entities of the process (a pressure measurement, a valve position, a power level, the presence of a safety protection signal or of an alarm, ...). To enable the operators to monitor the evolution of the process variables, three main mechanisms are available :

1. Display of instantaneous values on mimic diagrams (fig. 1)
   The three topics that are tackled by the DIMOS Man-Machine Interface are the following :
   - what information is needed;
   - under what form this information is the easiest to handle;
   - how to reach that information in the easiest way.
2. Trend curves, with the associated memorization mechanisms (fig. 2).
3. Event message lists.
   The following lists are available :
   - Automatic Presentation of Events (APEV) : is the actual operating tool, intended to draw the operator's attention to the significant evolutions of the process;
   - Present Alarm List (PAL) : gives a global overview of the plant malfunctions;
   - History List (HL) : contains all the events in chronological order.

The user interface distribution requirements are fulfilled by the "operator station" concept : a hardware and software entity that enables the user to monitor the process under a specific "view".

The operator stations are located in the various work areas (main control room Safety Parameters Display System SPDS; On-Site Technical Support Center, OTSC; radio monitoring laboratory, chemistry laboratory; ...). The specific configuration of each operator station enables selected information, depending upon the end user, to be made available where required.

The configuration data base is a commercial relational data base which contains :

- the plant equipment technical data;

- the parameters that enable the customization of DIMOS for a specific installation and its modification during plant operation (e.g. configuration of operator stations).

This configuration database is fully disconnected from the real-time monitoring process. This implies that the end user can modify the data off-line without disturbing the real-time process, and that once the data are checked and approved, the real-time data-base is updated.

SYSTEM ARCHITECTURE

The digital VAX(1) computer family was selected to implement the open system architecture.

Apart from the real-time and user interface requirements, the wide range of available processors, the networking facilities and the software compatibility of the successive VAX "family members" reinforced the decision.

Furthermore, this choice provides the customer with large expansion possibilities and a good protection against obsolescence.

A double Ethernet network (assuring redundancy) using the standard DECnet protocol, is the backbone of the system and constitutes the interface with the external world.

Around the network, a set of nodes (various kinds of VAX computers) is dedicated to the functional modules.

The implementation of DIMOS in Doel 3 (fig. 3) acquires more than 10.000 signals and monitors 15 screens. The logic signals are acquired every 20 ms (50 Hz), the analog signals every 1 s and some specialized fast analog signals every 500 ms. The screen update is accomplished within 2 s.

The DIMOS-MMI is built on the X-Window(2) distributed windowing system, the MOTIF(3) graphical user interface and the DataViews(4) package. It is therefore in compliance with the current industry standards.

The MOTIF widget set has been used to implement user input capabilities such as operator dialogues, as well as the formatting of data outputs like the list of alarms.

Other data outputs and more complex graphic formats that can be found in mimic diagrams are drawn using the DataViews package, a set of tools allowing to build and manipulate complex graphics.

SOFTWARE DEVELOPMENT ENVIRONMENT

To fulfill the requirements regarding quality, reliability, maintainability as well as compliance with the specifications, the application software for the monitoring system has been developed in the frame of modern software engineering methods systematically supported by CASE(5) : the general and detailed design is covered by an object-oriented method HOOD(6), supported by STOOD(7) (fig. 4), while ADA was chosen as programming language.

---

(1) VAX, DECnet are trademarks of Digital Equipment Corporation
(2) X-window is a trademark of the Massachusetts Institute of Technology
(3) MOTIF is a trademark of the Open Software Foundation, Inc.
(4) DataViews is a trademark of V.I. Corporation USA
(5) CASE, Computer Aided Software Engineering
(6) HOOD (Hierarchical Object Oriented Design) is a trademark of the HOOD user group
(7) STOOD is a tool developed by TNI - FRANCE

The main characteristics of HOOD are :

- HOOD fully complies with ADA program development.
- The method is standardized by an International group of users and has been chosen by the ESA (European Space Agency) for its projects.
- It is adapted to the design of large and complex systems. Indeed, it enforces the structuring of the objects according to abstraction, information hiding and encapsulation by introducing a hierarchy of objects and by providing a structured graphical representation of the system design.
- HOOD allows the description of the dynamic and real-time behavior of a system as well as the definition of different processes within the system, beside the description of its pure static and sequential behavior.
- HOOD defines a top-down stepped design process (based on successive decomposition) allowing the application of clear validation and verification procedures (defined by a QA plan) and the definition of milestones for project planning.

The method is strictly supported by STOOD (a CASE tool from TNI) that not only assures the management of the design documentation but also generates automatically the frame of the ADA code from the design, thus reducing considerably the coding effort.

The whole ADA code production is supported by STOOD, and thanks to the configurability of this tool, it has been possible to integrate the access to the compilation environment, the test and integration ADA libraries into STOOD. This allows the software development process, from the architectural design to the complete coding and even integration, to remain within the same environment with a consistent interface.

Furthermore, any software modification being introduced to STOOD can be directly applied to the design description guaranteeing conformity between code and design documentation.

ADA was chosen as programming language in the context of an ADA Programming Environment embedded in the design tool, because of its standardization, its portability, its strictness and its built-in real-time aspects.

CONCLUSIONS

DIMOS has successfully provided the solution to the limitations of the old system, such as functional deficiencies, low response time, data management and coherence, maintenance costs, spare parts and system availability.

DIMOS, with its different implementations in Doel 1 (1991), Doel 2 (1991) and Doel 3 (1993) NPP, is now one of the largest and most advanced process monitoring systems in operation.

The use of the software development methodologies HOOD and ADA has not only allowed a rapid integration and installation of a robust system, but will also enable further developments and improvements with a maximum flexibility.

In conclusion, DIMOS is an advanced, modular, homogenous, real-time software package, designed for highly flexible upgrades.

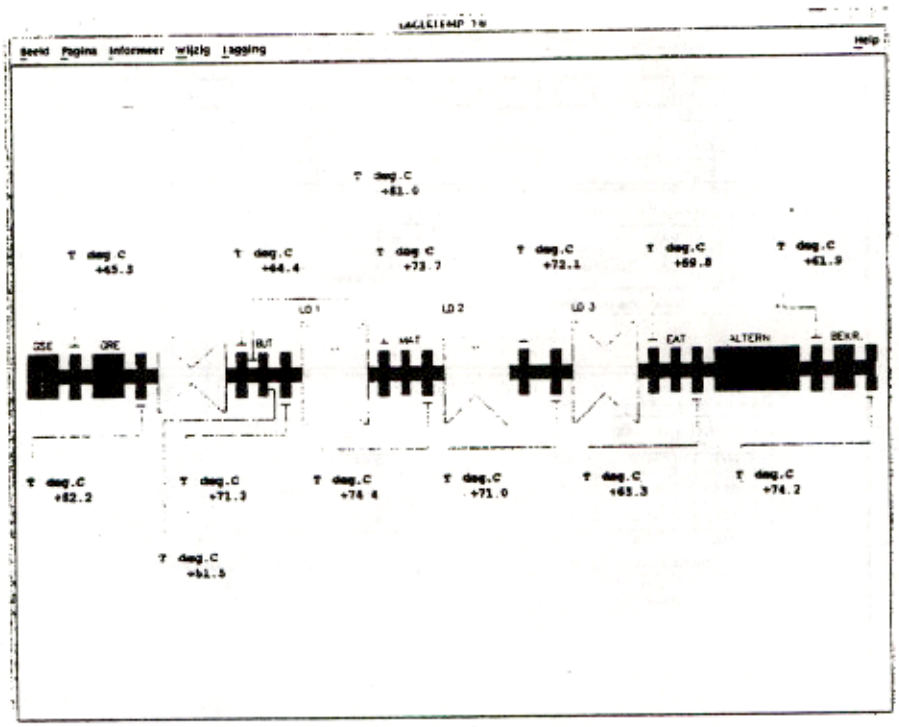


Figure 1 - Mimic Diagram

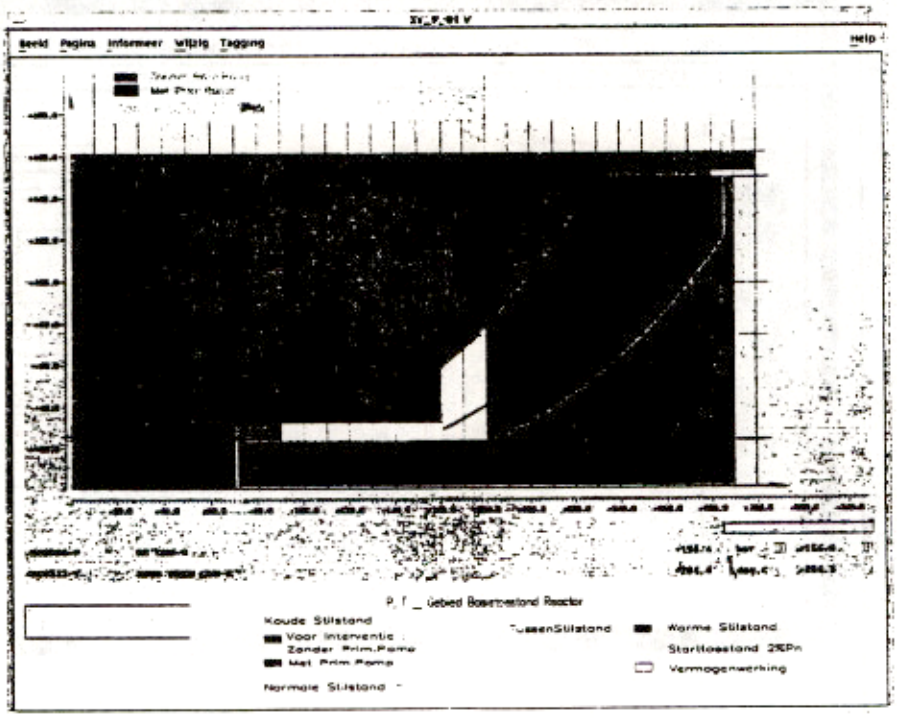


Figure 2 - Typical P.T. Diagram

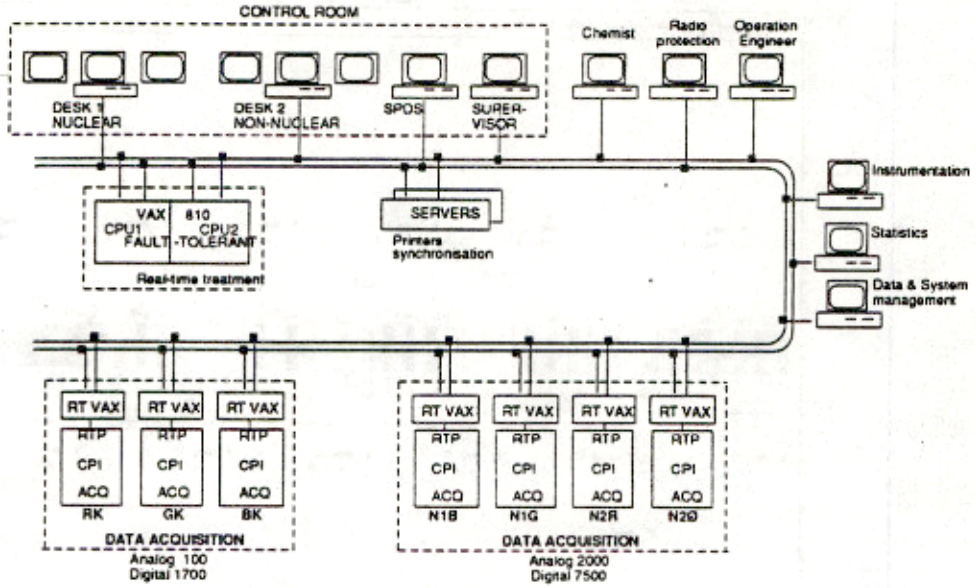


Figure 3 - Architecture - DIMOS DOEL 3 NPP

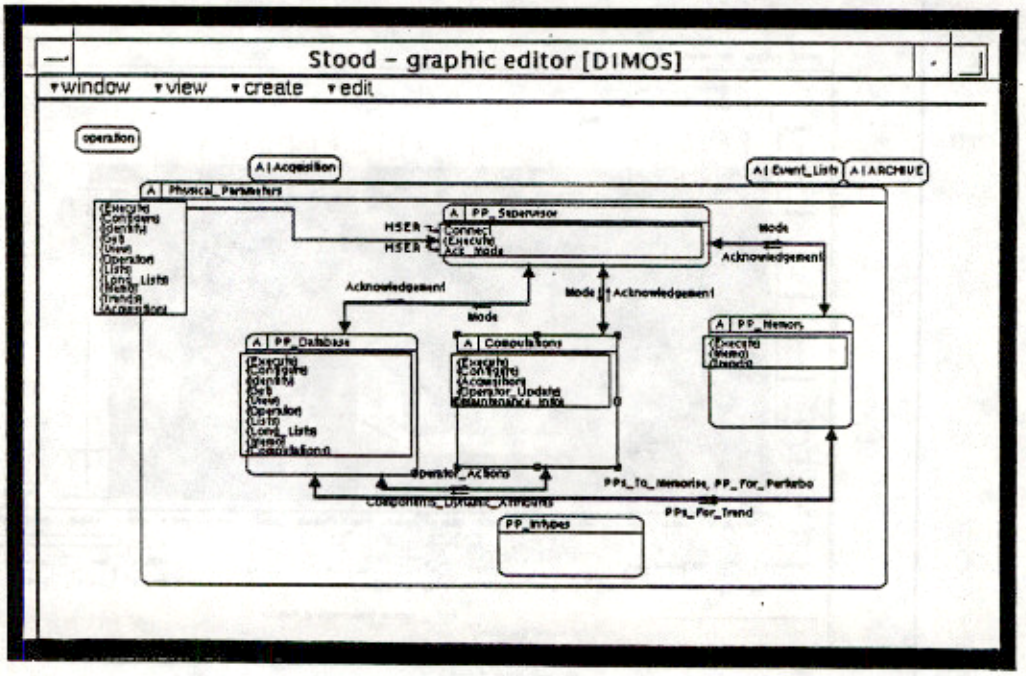


Figure 4 - Software Design Tool

RISK MANAGEMENT INSIGHTS FROM THE DEVELOPMENT AND USE OF THE SAN ONOFRE SAFETY MONITOR

Thomas A. Morgan[1], Thomas G. Hook[2], and Roger Lee[2]

[1]Halliburton NUS Corporation
200 Pringle Avenue, Suite 555
Walnut Creek, CA 94596

[2]Southern California Edison Company
San Onofre Nuclear Generating Station
5000 Pacific Coast Highway
San Clemente, CA 92672

INTRODUCTION

Southern California Edison (SCE) has actively used probabilistic safety assessment (PSA) techniques for many years to address various operations and maintenance needs of the San Onofre Nuclear Generating Station (SONGS). Typically, these applications have required the development of specialized models or have required the performance of various sensitivity studies based upon existing risk models.

In the 1980s, SCE had developed risk assessment models for many plant systems and had evaluated several important initiating events. However, these models could not be considered to be a complete PSA model. Nonetheless, quarterly estimates of actual equipment out of service times were used to provide plant management with estimates of the risk impacts of equipment failures and maintenance activities. Risk-based studies of various Technical Specification Allowed Outage Times (AOTs) were also performed.

In 1990, SCE began to develop its Individual Plant Examination (IPE) to meet NRC requirements for SONGS Units 2 and 3. The IPE model would serve as a complete Level 1 PSA for these units. SCE wished to develop a computer-based tool that could utilize the IPE model to aid operations and maintenance planning personnel in their day-to-day decision making. SCE personnel had visited Nuclear Electric's Heysham 2 station to observe the operation of its Essential Systems Status Monitor (ESSM). ESSM was used by plant personnel at Heysham to assess current plant risk and to evaluate operating strategies that reduced risk. SCE felt that the development of a similar tool at SONGS could be used to improve plant safety and could also serve to support future adoption of risk-based Technical Specifications.

SCE defined the functional requirements for a real-time risk management tool, called the San Onofre Safety Monitor. NUS developed the Safety Monitor software in accordance with these functional requirements. The completed software is now in trial use at San Onofre Units 2 and 3. Ultimately, the software will be used plant-wide by operations, maintenance, and PSA personnel. The tool will also play a key role in the plant's monitoring activities to support the Maintenance Rule (10CFR50.65).

Among the key functional requirements of the software was the display of PSA information in a format that is readily understandable to non-PSA-familiar personnel and the ability to calculate an estimate of current plant risk using a complete Level 1 plant fault tree within five minutes. It was felt that the dynamic re-solution of the actual fault tree model (rather than the use of pre-defined cutset lists) would minimize the likelihood that subtle risk impacts would be missed as plant operating configuration changed. Until recently, such a solution approach would be impractical for "real time" applications. However, recent development of very fast fault tree solution algorithms have made on-line model solution feasible.

DEVELOPMENT OF THE SOFTWARE

The Safety Monitor was developed using the C++ language and operates under Microsoft Windows on a personal computer. The software is designed to support multiple users on the plant's Local Area Network with various user privilege levels. The Safety Monitor incorporates the complete Level 1 IPE model, including common cause failures and operator actions. The software's data bases include all 73,000 components in the plant, over 2,000 of which are currently linked to failure events in the model. Ultimately, several thousand additional components (e.g., drain and vent valves) will be linked to the model to more fully reflect the effects of maintenance actions upon plant risk.

The San Onofre IPE model was developed using the small event tree/large fault tree method. To allow for rapid model solution, the IPE event trees were transformed in to a single master fault tree, whose top event is "core damage occurs". This fault tree includes all 92 core damage sequences evaluated in the IPE for 15 initiating events. Following the development of the top logic, the system fault trees were optimized to improve model efficiency. This optimization process included the elimination of duplicative logic gates, consolidation of events into "super" basic events (where possible), and restructuring the tree to move support system fault tree linkages to as close to the top of the fault tree as possible. Proper treatment of IPE model flags or "house events" was also incorporated into the optimized model. It should be noted that this optimized model yields the same numerical results as the original model and that the information concerning basic events consolidated into "super" basic events is retained in the Safety Monitor data files so that full model fidelity is maintained. The model was also enhanced to specifically address each of the various system configurations that could be experienced during power operations. For example, several systems include "swing components" that can be aligned to either of the two safety trains. The risk model results can be influenced by the alignment of these components, particularly when safety-related support system trains are removed from service.

The model optimization process (and subsequent validation of results of the optimized model) served as an excellent review of the IPE and identified a number of minor errors and inconsistencies that were not previously noted in the various reviews conducted during the IPE process. The correlation of the PSA model to the actual plant components also identified several areas for improvement of the plant's data sources. For example, the plant's master equipment list includes fields to indicate the system designator and train designator for each component. However, the data contained in these fields is not controlled by the plant's information systems group. Therefore, these fields contained many

errors and inconsistencies. The plant's data base for pre-defined maintenance tagout groups was also found to be incomplete.

SOFTWARE OPERATION

Figure 1 illustrates the main screen of the software. The Safety Monitor provides plant personnel with a "gauge-type" display of current plant risk, as well as a plot of plant risk levels over the past seven days. The display also indicates a recommended "allowed outage time" for the current plant operating configuration, based upon current plant risk and administrative risk limits. The establishment of the various administrative risk limits (e.g., "high", "warning", and "low" levels) will be performed through a series of sensitivity studies and a review of actual operating experience over a several month period. The plant operators can also view a listing of the most important equipment.

For equipment that is currently out of service, the Safety Monitor also offers advice as to which equipment should be restored to reduce risk in the most effective manner. This "component restoration advice" represents a powerful tool for maintenance and operations personnel to ensure that risk is reduced quickly when the Monitor indicates that the overall core damage risk is higher than administrative limits.

A number of security features are also provided to ensure that key data is not accidentally or intentionally modified by unauthorized personnel. Four security levels are provided. While the "administrator" level can update plant configuration, data files, and print various status reports, the "user" level can only view plant risk status and operating advice and perform various "what if" calculations.

Plant operators can input changes in plant operating status to reflect taking equipment in or out of service, changes to system configurations, and the presence of environmental factors that might affect risk. Examples of these environmental factors might be severe weather (which might affect the likelihood of loss of offsite power supplies) or the performance of surveillance testing that might increase the likelihood of a plant scram. "Real" status changes may be selected by control room operators, or the user could instead investigate the effects of possible changes by performing one or more "hypothetical" calculations. Only qualified users may select a "real" calculation, and those plant configurations that are input are used to update the current operating configuration of the plant in the various data bases. The use of "hypothetical" calculations (which are available to all users) allows maintenance planning personnel to investigate various maintenance strategies for the current plant configuration. Figure 2 illustrates the screen used to take equipment out of service. Equipment can be removed by either typing in the component ID of the equipment to be removed, selecting the system ID to access a list of all components in that system and then selecting the desired component(s), or by selecting a pre-selected equipment group based upon the BAG (Boundary Area Grouping) ID defined by San Onofre maintenance personnel.

While plant operations personnel are displayed information in a non-PSA format, features are available for PSA engineers to examine the actual risk results (e.g., the cutsets of the various calculations) and to generate various reports of risk trends and out-of-service times for plant equipment. The data bases of the Safety Monitor collect information that can be readily used to determine actual hours of power operation, fractions of time the plant is in various operational alignments, and out-of-service times for various risk-critical components. The automatic collection of this data will greatly simplify the PSA maintenance process for the SCE staff. The data collected by the software will also directly support the monitoring requirements of the Maintenance Rule, particularly paragraph a(3) requirements for monitoring the effects of maintenance activities upon plant risk.

INSIGHTS FROM USE OF THE MONITOR

Although the Safety Monitor has only been in use on a trial basis at San Onofre, the initial development process and trial use period have indicated a number of insights that are important to consider in the application of PSA models to actual plant operating conditions. These are summarized below:

- The risk model may need to be refined further to properly reflect operating conditions (e.g., components out of service, system alignments, etc.) that were not considered in the IPE. The ground rules used to construct the original models might not be valid for certain plant operating conditions.

- The determination of the risk thresholds to be used will require further refinement as additional operating experience is obtained. The calculation of a risk-based AOT can also be performed by several methods, with differing results. Further sensitivity studies will need to be performed to determine the optimum approach to be used.

- The results of various sample calculations with the Safety Monitor graphically illustrate that not all safety-related components are equally important to safety. In fact, removal of certain groups of equipment that would be disallowed by current Technical Specifications has less risk impact than the removal of single pieces of equipment in other systems.

- The inclusion of various environmental and testing factors has shown that these factors can have a large impact on plant risk, particularly for those factors that increase the likelihood of loss of offsite power (e.g., severe weather, increased likelihood of earthquakes/aftershocks, periods of peak electrical demand, etc.). Initial estimates were generated for each of these factors based upon the published uncertainty ranges for the point estimates for these initiating events; but these estimates may need to be refined. In addition, it is probably appropriate to reduce the "base case" point estimates for these initiating events. For example, the loss of offsite power frequency used in the IPE is an average value that includes periods of severe weather. Since the "base case" condition assumed in the Safety Monitor is based upon no unusual stresses to the electrical grid, this average value may overestimate the likelihood of power loss under normal conditions.

- Using a "warning" threshold of ten times the base case risk (which is the value used in Heysham's ESSM system), many maintenance actions allowed by Technical Specifications place the meter in the "warning" condition, particularly when environmental and testing factors are in effect. This result is reasonable from a PSA perspective, but may be surprising to plant personnel who assume that operation within Technical Specification constraints constitutes safe operation.

FACTORS TO CONSIDER IN USING A TOOL LIKE THE SAFETY MONITOR

The Safety Monitor represents a powerful tool that can apply the insights of a PSA model to day-to-day operations. Hopefully, the use of tools such as these will help to improve safety and to identify situations in which current regulations may be too restrictive when compared to their safety benefit. However, in using such a tool, it is important to recognize that these tools have practical limitations. Failure to acknowledge these limitations may result in erroneous decisions that might be contrary to the intended purpose of the Monitor.

Unlike other gauges in the control room, the Monitor does not display an absolute value. It is important to recognize that the Monitor provides only a probabilistic estimate of current risk. Accidents can occur even when the risk gauge indicates that risk is very low.

The results of a tool such as this are strongly dependent upon the accuracy of the risk model that is input to the software. The IPE model was developed to represent a specific set of operational alignments. In actual day-to-day use, portions of the model may become dominant that may not have been fully developed, particularly with respect to human errors and recovery actions.

Even with an accurate model, the effects of failures of minor components (e.g., drain valves, maintenance isolation valves, instrumentation, etc.) might not be considered in the original IPE model. In order to obtain accurate risk results, the impacts of these additional components need to be considered. Determining those components to be considered may require the assistance of plant operations and maintenance personnel.

Lastly, because the model currently considers only Level 1 effects, it is possible to underestimate the true worth of a particular component, particularly if its primary purpose is for accident mitigation. For example, the Level 1 model might indicate that little risk increase would occur if containment atmospheric control system components are removed from service. While it is true that these components do not impact the likelihood of core damage, they do play a significant role in mitigating radioactive releases post-accident. If the operator or maintenance person does not consider these effects, he might draw the wrong conclusions about the significance of certain maintenance actions.

AREAS FOR FUTURE DEVELOPMENT

The use of a tool such as the Safety Monitor makes it possible to develop risk-based Technical Specifications that would account for unique plant operating conditions and various environmental conditions that might influence the risk of a serious accident or transient. SCE believes that a more risk-based approach to Technical Specifications will allow greater flexibility to perform maintenance while the plant is operating, while helping to ensure that overall operating risk is minimized. Obviously, the transition to a risk-based Technical Specification approach must be accomplished over a period of time, in order to gain sufficient experience in the use of such techniques. Also, the current regulatory framework does not directly permit such an operating strategy. However, it is hoped that the insights and experience gained with this tool will serve to make the transition to a risk-based operating strategy an easier one.

The Safety Monitor may also be expanded in the future to address other aspects of plant operation. The Level 2 IPE model may be included to assess the impacts of various maintenance and operational activities upon the likelihood of a radioactive release following an accident. The consideration of such effects will allow evaluation of components such as containment isolation valves, containment pressure control systems, and containment radioactivity cleanup systems. This expansion will allow plant operators to more fully estimate the importance of plant systems to the overall mission of protecting public safety.

Another area for future development is the incorporation of risk models to address non-power operating conditions. The addition of this capability will allow operators and maintenance personnel to plan outage activities in a manner that will reduce risk. These models will also allow plant personnel to perform comparison studies to determine the risk tradeoffs of performing certain maintenance actions at power instead of during plant shutdown. Comparison studies can also be made to determine the most appropriate shutdown mode in which to perform a given maintenance action.

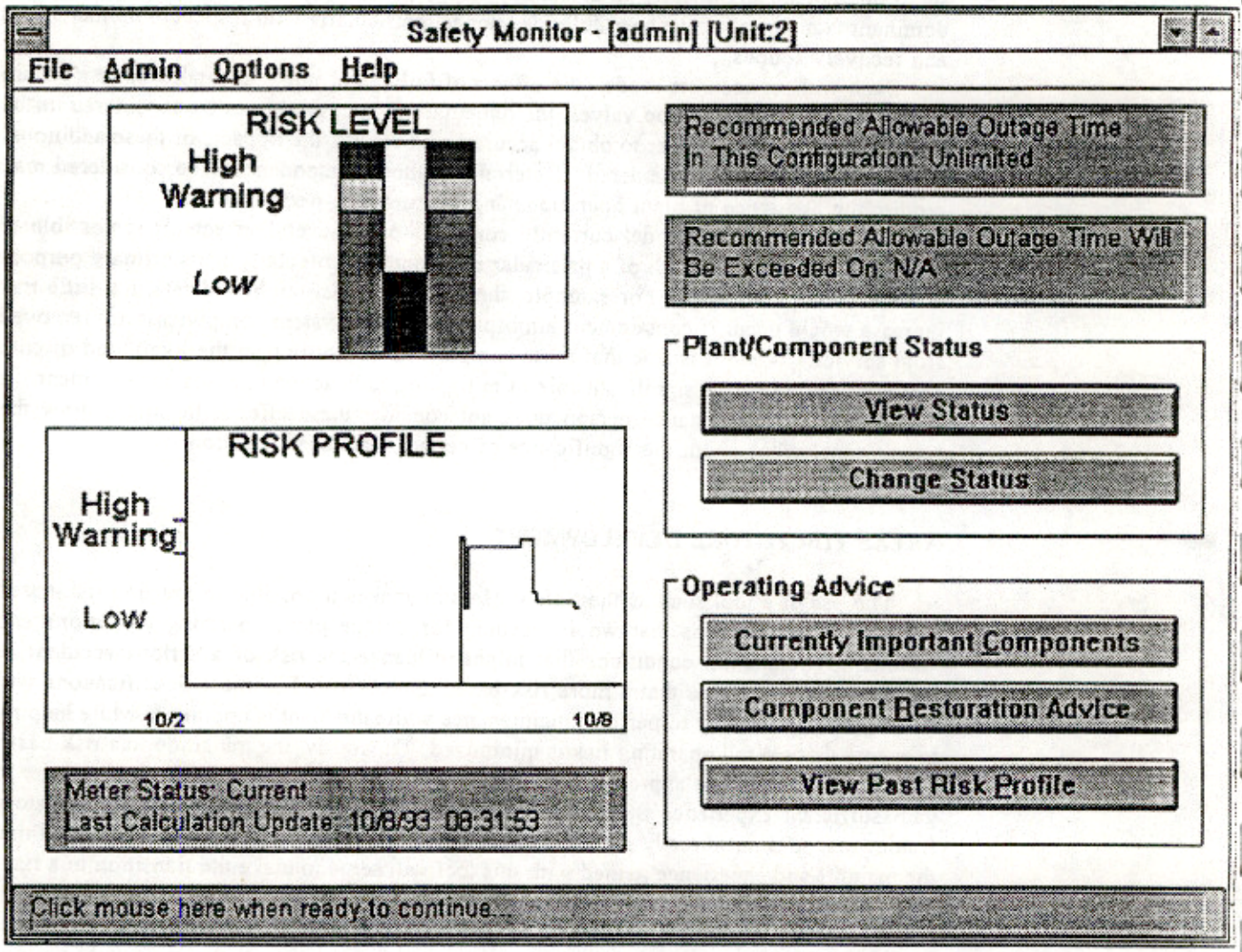


Figure 1: Safety Monitor Main Display Screen

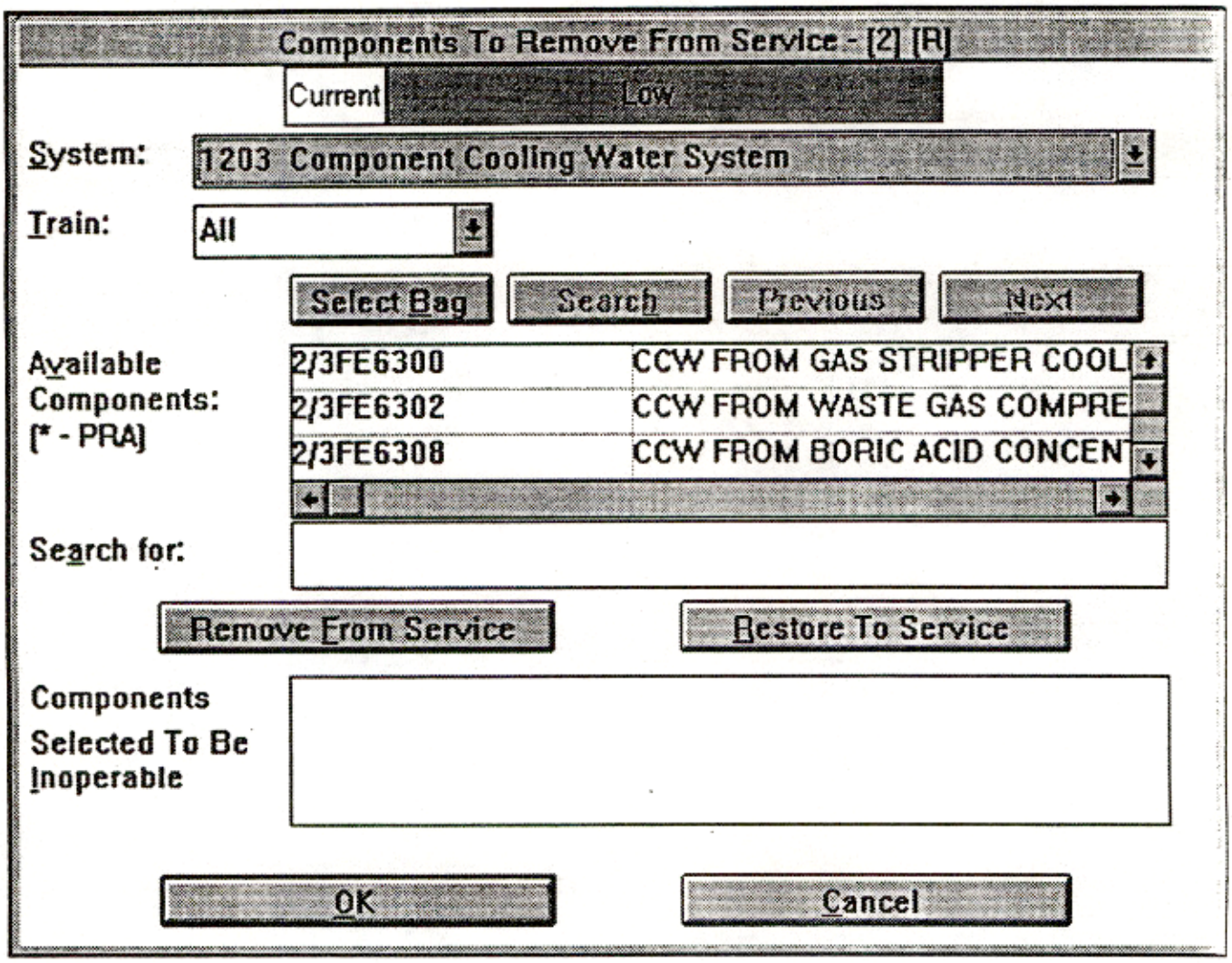


Figure 2: Remove Equipment from Service Screen

COSMIC MODELLING WITH PERSONAL COMPUTERS

Richard Allen Strong
Safety Analysis Systems
Huber Heights OH 45424-3229

AN OPPORTUNITY AND A SOLUTION

The pervasive COSMIC technology may be characterized as both a partial solution to recurring problems and an opportunity to develop innovative technologies. The overarching aim is reflected in the name of Computerized Operational System Modelling for Integrated Control, hence the acronym "COSMIC".

Objectives

The objectives are: to take advantage of modern electronic technology and create a **practical personal computer, PC, tool using off-the-shelf software** for users to create polyphony out of chaos, **"E PLURIBUS UNUM"**. The primary capabilities of the PC are seen in the database and the spreadsheet, hence the focus will be maximizing their use. The general advantages of electronic data processing are well known so will not be repeated here. The database capability will be used for documenting lessons and detailed solutions of repetitive problems in the usual manner. The spreadsheet will be used in a rather unique fashion as a diagramming tool to create an interactive model of the operational system. The database will be linked to the spreadsheet. The overall system may provide enhanced data-sharing. Emphasis is placed on quantitative financial decision-making.

SHERDQAM

Since the assurance of optimum loss and litigation is seen as an important driver for the system effectiveness, the technical objective is attaining the user's required assurance. This assurance may be gained by managing together the Safety, Health, Environmental, Reliability, Decision-Making, Quality, and Analysis via Modelling, or, to use an unwieldy acronym, "SHERDQAM" (as in "sure can"). Clearly, one desires maximum integration, where common goals and purposes prevail.

A single integrated SHERDQAM might be used by all of the activities. SHERDQAM should be capable of showing the significant risks of the operational system and accepting, calculating, and showing changes. Specifically, users will have a database of detailed hazard analysis reports and other safety data that link to a system model spreadsheet to aid in decision-making. The SHERDQAM may then be extended to encompass the operational system as a COSMIC model.

System Safety Program

The requirements were defined in Military Standard MIL-STD-882 some 20 years ago. The goal of system safety is the **optimum level** of safety, considering **COST, SCHEDULE, AND OPERATIONAL EFFECTIVENESS.** The DOD/ DOE/ DOT/ NASA standard for precluding unplanned losses is the system safety program, which **formalizes** the assurance process. The process has also been widely adopted by many defense and power and communications industries world-wide. The Standard requires the use of a System Safety Group, SSG, composed of representatives for all concerned, to ensure that omissions and oversights were minimized and communication is maximized. The SSGs served as ad hoc Quality Circles and TQM Teams, as do Safety Review Boards in the test community.

System Safety Data

Program Directors ensure that the information is acquired in a timely manner by specifying development of the reports listed: Program Plan; Progress Reports; Hazard Analysis Reports; Safety Assessment Reports; Health Hazard Reports; Mishap Analysis Reports; Change Analysis Reports; Explosives Classification. Emphasis is placed on history for lessons learned, while simultaneously requiring attention to the use of new materials. It's noted that very little evidence is known, at least to this writer who has worked with over a thousand projects, showing that the optimum level was attained in a rigorous manner. The PC spreasheets available have optimizing capabilities and can handle linear programming quite easily.

1. System/Subsystem/Comp	**: Maintenance hangar or vehicle garage.**
3. Comp/Subs Failure Mode:	**Fail to contain fumes & ignition sources**
5. Sys/Comp/Event/Phase	**: Operational, maintenance, or storage.**
6. Operation Description	**: Vehicle operating/being maintained.**
7. Hazard Description	**: Sparks & fumes leaking from tanks/HAZMAT**
8. Hazard Identification	**: Only leaks large enough to smell/see**
9. Effects of Hazards	**: FIRE/POLLUTION. Loss of garage; injury.**
10. Risk Assessment	**: $100,000; "Occasional". Risk Index 1-C.**
11. Recommended Actions	**: Fume detect/suppress; seal HAZMAT/fuel**
12. Effect of Actions	**: $15,000 installation; Risk Index 1-E**
13. Remarks: Doc,Dat,Dir	**: Manufacturer estimate. ACCIDENT FACTS.**
14. Status: Dwg,Spec,Proc	**: OPEN pending safe completion of testing.**
15. Cautions, Warnings	**: Warnings in HAZMAT handling procedures.**

Figure 1. Database for DI-SAFT-80101A, para. 10.2.3.b.

HAZARD ANALYSIS REPORTS

Much of the safety activity is concerned with analysis and reporting. particularly for DoD systems. See Figure 1; the Figure displays a database printout of the items required by Data Item Description for a common hazard as rows of data. These are iterated throughout the program in phases: preliminary; system and subsystem; and operational and support. The reports may be assimilated into a detailed and **standardized database structure that combines the various items of information from the various reports as object records.** Such a standardized structure would facilitate sharing of data among users, providing electronic communication, rapid updating, easier access to historical data, and commonality.

		Desired Hazard		Action Effect	
Comparison of "Before	P=	0.75	0.25	0.90	0.10
and After", with the	M=	-1200	-100	-1280	- 180
Desired+Hazard Plan	O=	2400	0	+2400	0
versus the	S=	- 100	-1000	- 10	-10
Recommended Action+	T=	- 300	- 500	- 200	- 80
Effect Plan.	PT	600	- 400	+ 819	- 270
PROBABLE NET BENEFIT	PNB	200		549	

1.) " P= " is for the Probability entries (sum to 1 at GT).
2.) " M= " is for the Money or cost expenses (negative values).
3.) " O= " is for the Operational Effectiveness/prOfit/Output (positive values);
4.) " S= " is for the Safety Costs: Legal; Medical; Insurance, etc. , (negative)
5.) " T= " is for the Time or Schedule costs (negative values).
6.) "PT" is the product of Probability and the sum of the Money, Operational effectiveness, Safety, and Time, a Probable Total.
7.) "PNB" is the sum of the Probable Totals for the Desired + Hazard and the recommended Action + residual Effects, the Probable Net Benefit.

Figure 2. Risk Assessment Database Calculation

Risk Assessment with MOST Procedure

With the database implemented, attention is turned to tailoring for unique applications for the system being modelled. **Common criteria are shown in Figure 2 as "MOST" factors, based on the goal of achieving the optimum level of safety.** Note that the notion of "Operational Effectiveness/Output" in terms of dollars may cause some head-scratching. In some cases, this may be more difficult to determine than the cost of human suffering, where one has at least some guidance from the courts and actuaries. This line of reasoning will lead to a notion of "Life Cycle Benefit", vice "Life Cycle Cost", which, after all, is the goal.

Hazard Report Problems

There are problems with the reports required by MIL-STD-882:

* **Difficult to describe chains of events (system aspects);**
* **Difficult to relate between elements (interfaces between elements);**
* **Difficult to describe and optimize the system rigorously;**

Operating Hazard Analysis

Another format used in the operational and support phases is based on columns and rows in landscape format. This format, known historically as an Operating Hazard Analysis, OHA, places Items 1 through 5 as rows and Items 6 through 16 as columns. This format leads naturally to the spreadsheet diagram.

FAULT TREE SYSTEM ANALYSIS

Noting the problems, safety professionals sought better ways to cope.

System

The "main claim to fame" in the system safety engineering is the so-called "fault tree", a system hazard analysis diagram which details the various causes that may lead to a particular mishap. It was derived from Bell Telephone Laboratory's work in network analysis used in ICBM guidance systems about 30 years ago. The essence is control theory, rather than breakage. The diagram is drawn as a vertical flow-chart with the main fault at the top and various blocks and paths with symbols linking together so it looks like a Christmas tree.The key process in developing fault trees is the tracing of the flows of control signals and power. As Dave Hassel has taught thousands of system safety engineers at short courses with the University of Washington,**"No matter where you begin analyzing a system, if you trace the signal and power, you will ultimately define the whole system."**

Problems

Due to a reliance on manual methods and/or unique software programs, there is no standardized method of documenting fault trees nor library of them; therefore, there is no interchangeability. Fault trees are foreign to the layperson who must interpret them. The vertical orientation is different from horizontal charts used by management. Information cannot be readily transferred to other conventional systems. They are not very useful for explaining to laypersons, as in public relations or litigation. Although the DID mentioned above requires system analysis, no guidance is provided for actually doing the analysis nor documenting the work. It's noted that, within the various safety communities, guidelines have been published from time to time, particularly in the nuclear community; however, these are not generally available nor is their use widespread. This may be critical in the international arena.

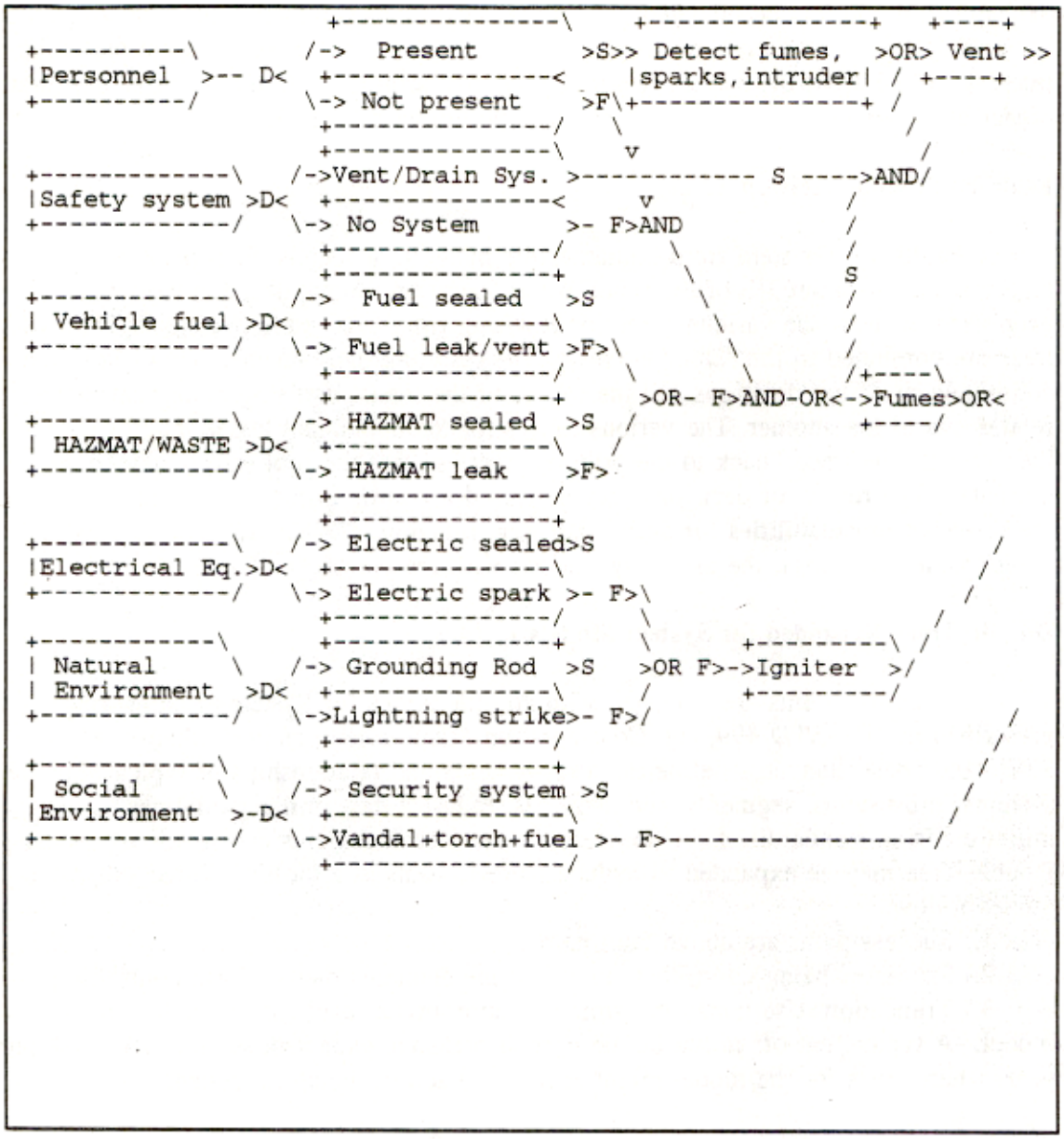


Figure 3. Spreadsheet Fault Tree for Common Hazard

SPREADSHEETS FOR FAULT TREES

The use of spreadsheets in finance has been expanded include useful functions as "smart" flowcharts. The advantage over conventional flowcharts is that the numerical calculations may also be incorporated. The MOST data from the database may be imported along with some of the hazard report narrative.

Example of Preliminary Model

See Figure 4. The previously-discussed hazard is illustrated showing: the Decision paths, "D"; the Safety paths, "S"; and the Fault paths, "F". Note that system security and environmental impact are included in the model. The system assumes inclusion of the ecosystem. Note that preliminary models require very little memory or calculations. By simply using standard spreadsheet formats, models may be easily

exchanged, modified, and updated. All of the capabilities for calculation and so on that are available with modern spreadsheets may be used in the model. Of some particular interest are the areas of interactive simulations for hazards. Note that each of the small object blocks represents a database record imported with its MOST data.

Fault Trees with Decision Trees

Faults always stem from human errors made in decisions. Experience shows that humans err about 1% of the time. In the operations arena, decision trees have been used to show the various scenarios resulting from successive decisions. The two trees are combined in the "Double-Tree". The resulting diagram then shows both the consequences of the decisions and the causes of the losses in a single diagram that relates one to the another. The various causes for the unplanned losses may then, theoretically, be traced back to the original errors so that the root errors may be corrected. The results of decisions may be traced forwards to the ensuing results. **With the spreadsheet capabilities for doing statistical functions, "What If?" calculations and audit tracing of strings, the user may interact with the model.**

Double-Trees Expanded for System Models

Defense systems are managed with considerations for Systems Engineering, prescribed in MIL-STD 499, and Configuration Management, as prescribed in MIL-STD 480. These standards define the arrangements and relationships of typical systems, subsystems, segments, and activities. Industry has similar guidelines. One might envision standardized spreadsheets for these arrangements and relationships. The Double-Tree may be expanded to include these as tools in a toolkit. Three suggested guides follow.

1.) Success paths are above fault paths;

2.) Processes being controlled are below the elements that perform controlling;

3.) Truncation. Users may determine an appropriate level for truncating the model. A typical cut-off might be the normal breakage expected, such as 1% - 2% per year, where costs for the model might exceed the actions being modelled.

SUMMARY

The schema described above may be used by any person or group which manages high hazard systems. Templates for off-the-shelf software are now available to provide users with easy setup in both DOS and Windows environments. License has been granted to DoD for official use and the Air Force Chief of Safety has indicated a favorable review for use. The database template provides a single-page report with about 180 fields, including embedded calculations for Probable Net Future Benefits and about 60 fields for occupational safety and health and environmental management. HAZMAT inventory and labels and HAZWASTE labels are included. Anyone who is familiar with the PC database and spreadsheet functions may adapt the templates to their operational system, thus aiding their decision-making to accomplish planning with a greater assurance that the safety, environmental, and quality aspects can be modelled so as to fairly accurately reflect the operational system.

032 Methodology

Chair: L.R. Abramson, LANL

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

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

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

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

A DYNAMIC GOAL TREE APPROACH FOR PROCESS SAFETY MANAGEMENT

Xiaozhong Wang, Marvin L. Roush

Center for Reliability Engineering
Department of Materials and Nuclear Engineering
University of Maryland
College Park, MD 20742-2115

The current techniques for accident sequence analysis have largely been developed for the nuclear industry, although they are also widely used in many other industries including the process safety management of chemical plants. The following example of process safety management of chemical plants presents some dynamic features which challenge the capabilities of standard accident sequence analysis. It is a revision of a previously published problem[1] which we utilize here to provide a concrete illustration of the analytical difficulties.

Example The plant safety engineer at a chemical factory reviews the combined fire-fighting resources of the fire department and the factory as listed below and finds them to be:

- The fire department has three vehicles: M – a multipurpose fire engine; T – a tanker; L – a light fire truck.
- The firefighting equipment of the chemical factory consists of: S – a sprinkler system; H – a hydrant; F – a special apparatus for fighting chemical fires.

In order to determine the adequacy of these combined hardware resources to fight a fire in the factory, he identifies the following dynamic features:

1. As shown in Figure 1, the interaction between the on-site and off-site systems depends on the action phase; the phases being: evacuation, fire containment and fire control.

   During the initial stage of a fire, either the multipurpose engine (which carries a small water supply) or the light truck (provided the sprinkler system works) suffices to enable the evacuation of the building.

   To contain the fire, the factory's special apparatus is needed, together with some auxiliary capability from the multipurpose engine or the light truck. Water can be supplied to the special apparatus by the hydrant, or if it is out of order, by the tanker through pumps in the multipurpose engine.

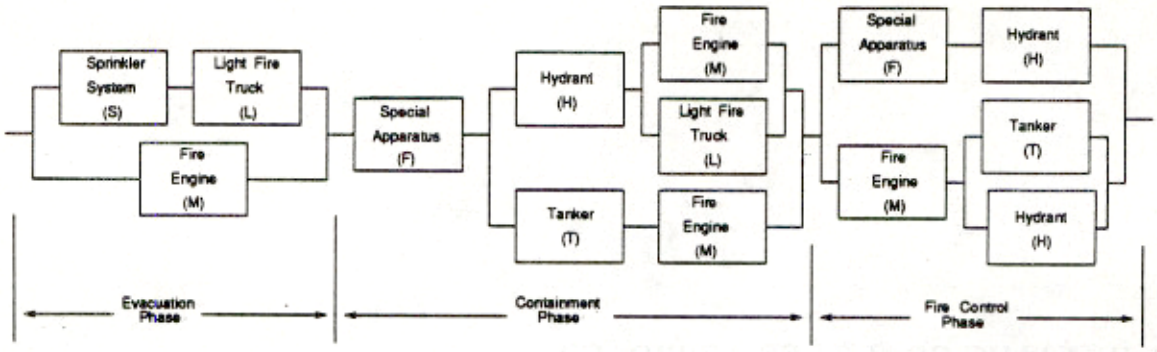


Figure 1. Block diagram for the mission of the Example.

After the fire has been contained it can be controlled either by the special apparatus or the multipurpose engine. Again, water can be supplied by the hydrant or by the tanker together with the multipurpose engine.

2. The failure probabilities of components might be time-dependent because of the different operating environmental stress levels during the several mission phases.

3. The evolution of an accident sequence is dependent on the current hardware status (e.g. the success or failure of each item of equipment at a particular time).

Accident analysis as originally developed in the nuclear industry seldom addresses the dynamic features of process safety management. Examination of the currently used methodologies of accident sequence analysis reveals that time is almost completely excluded from the picture of event trees and fault trees. This is exemplified by the approach used to calculate the probability of an accident sequence as employed in the Interim Reliability Evaluation Program $(IREP)^2$, which is:

1. to link the fault trees of the systems which are in a failure state in each accident sequence together with an AND gate;

2. determine the minimal cut sets of the top event associated with the AND gate in step 1 and;

3. compare the minimal cut sets of the AND gate to those of the fault trees for the system successes in the accident sequence. Minimal cut sets of the failure portion of the sequence which are subsets of the minimal cut sets of the success portion of the sequence are eliminated. This is done because they imply the failure of a system that is specified in the success portion to have not failed.

This approach seems perfectly logical. However, further investigation reveals a very important factor: inconsistencies can arise because time has not been taken into account in this approach. The IREP approach does not account for the fact that the success portion and failure portion of a sequence usually occur in different time phases. If we apply this approach to our example, significant non-conservative error results. We will analyze sequence S3 in the event tree shown in Figure 2 using the IREP procedure:

1. We obtain the minimal cut sets (MCSs) for "fire control", which is in a failure state in S3:

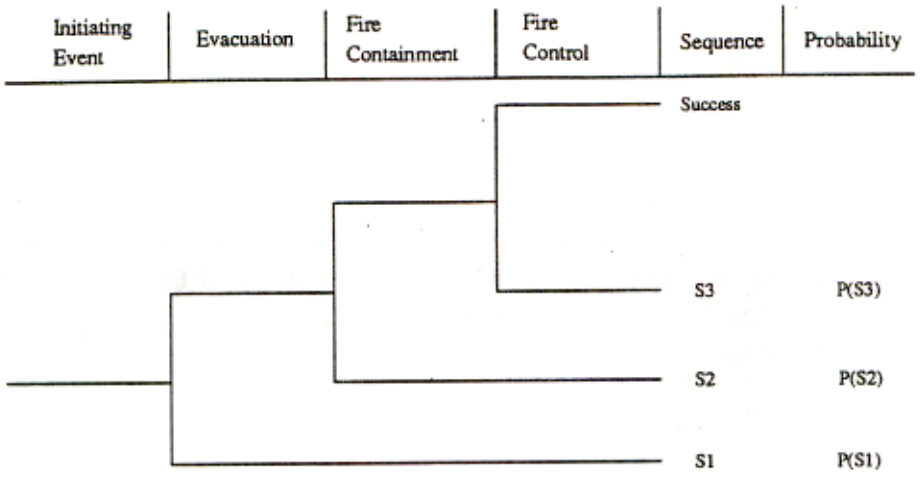


Figure 2. Event Tree for the mission of the Example.

Fire Control: {F, M} {H, M} {H, T}

2. We also obtain the MCSs for the "evacuation" and "fire containment" phases, which are in success states in sequence S3:

   Evacuation: {M, L} {M, S}
   Fire Containment: {F} {H, M} {H, T} {M, L}

3. We compare the MCSs for "fire control" to those for "evacuation" and "fire containment". The minimal cut sets of "fire control" which are subsets of those of "evacuation" or "fire containment" are then eliminated because they imply the failure of "evacuation" or "fire containment" which are successful in sequence S3.

   For our current example, all the MCSs in "fire control" are deleted because each one is a subset of "evacuation" or "fire containment". Thus, we have eliminated all of the minimal cut sets and obtain a zero-probability for sequence S3.

This overly-optimistic result shown above is clearly wrong. Here, the time-dependent aspect of the process safety management are an important factor which cannot be overlooked. We have failed to include the possibility that the MCSs of fire control were not failed during the earlier phases but could fail during the fire control phase. This recognition has fueled the recent development of dynamic event trees and their application in various fields[3-5].

Because each basic event in an event tree branches at each time step, previous techniques for dynamic event tree analysis become prohibitively difficult for real process safety management problems. When analyzing the simple example discussed above which has 6 binary components and 3 time steps, the number of developed accident sequences can be as large as $(2^6)^3 = 262,144$.

Our research work aims to greatly reduce the complexity of a dynamic event tree analysis, thus making it manageable for practical engineering problems. Instead of branching each basic event at each time step, the time scale is introduced into the conventional Boolean Algebra. Two rules concerning the union and intersection between basic events in different time steps are introduced into the conventional Boolean Algebra:

Theorem 1: $A^{(j)}$ denotes component a is in failure at the end of time step j. $A^{(k)}$ denotes component a is in failure at the end of time step k. If $j \geq k \geq 1$, then

$$A^{(j)} \bigcup A^{(k)} = A^{(j)} \tag{1}$$

Theorem 2: $A^{(j)}$ denotes component a is in failure at the end of time step j. $A^{(k)}$ denotes component a is in failure at the end of time step k. If $j \geq k \geq 1$, then

$$A^{(j)} \bigcap A^{(k)} = A^{(k)} \tag{2}$$

Here the intersection and union concepts are extended to events in different time steps. Equations 1 and 2 are added to the list of Boolean algebra principles to handle the time dependent effect between cut-sets in different time steps. As shown in Figure 3, this extended Boolean algebra constitutes a "*time dependent logic*", which is the mathematical basis of our dynamic probabilistic analysis.

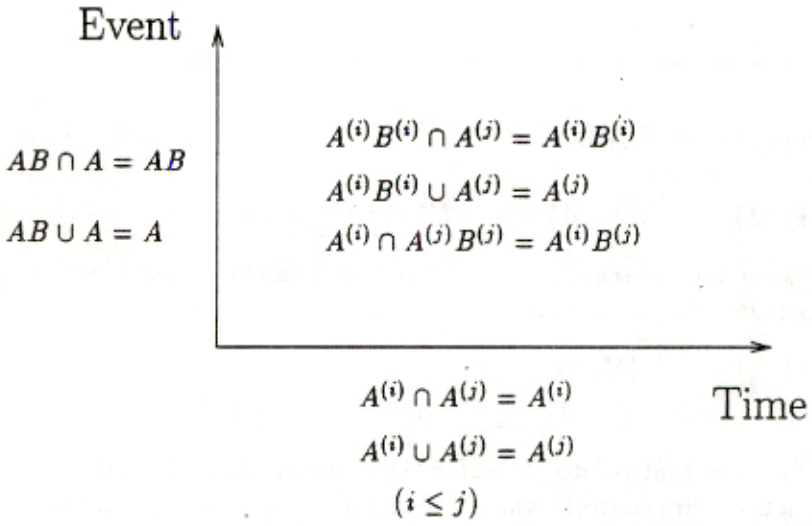


Figure 3. A two-dimensional logic.

A goal tree is a *success-oriented* logic structure which can be used to organize complex systems and their engineering knowledge into a format suitable for problem-solving[6,7]. The first step for our current problem is to define a safety goal based on the overall safety objectives, and then to identify the subgoals which must necessarily be achieved if the goal is to be satisfied. Such a successive decomposition of identified goals continues until the goal resolution reaches a level of engineering knowledge which will be further detailed by success trees.

By incorporating the time-dependent logic into the goal tree analysis, a dynamic goal tree approach can be developed as described below.

Example (Cont.): A dynamic goal tree for the mission described earlier is shown in Figure 4. Accident sequences are analyzed by the following procedures:

1. Obtain MCSs for each time step (done earlier in this paper),

2. Superscribe MCSs indicating time steps (see Table 1),

Table 1. Minimal cut sets for each time steps.

Time Phases	MCSs			
Evacuation	$\{M^{(1)}, L^{(1)}\}$	$\{M^{(1)}, S^{(1)}\}$		
Fire Containment	$\{F^{(2)}\}$	$\{H^{(2)}, M^{(2)}\}$	$\{H^{(2)}, T^{(2)}\}$	$\{M^{(2)}, L^{(2)}\}$
Fire Control	$\{F^{(3)}, M^{(3)}\}$	$\{H^{(3)}, M^{(3)}\}$	$\{H^{(3)}, T^{(3)}\}$	

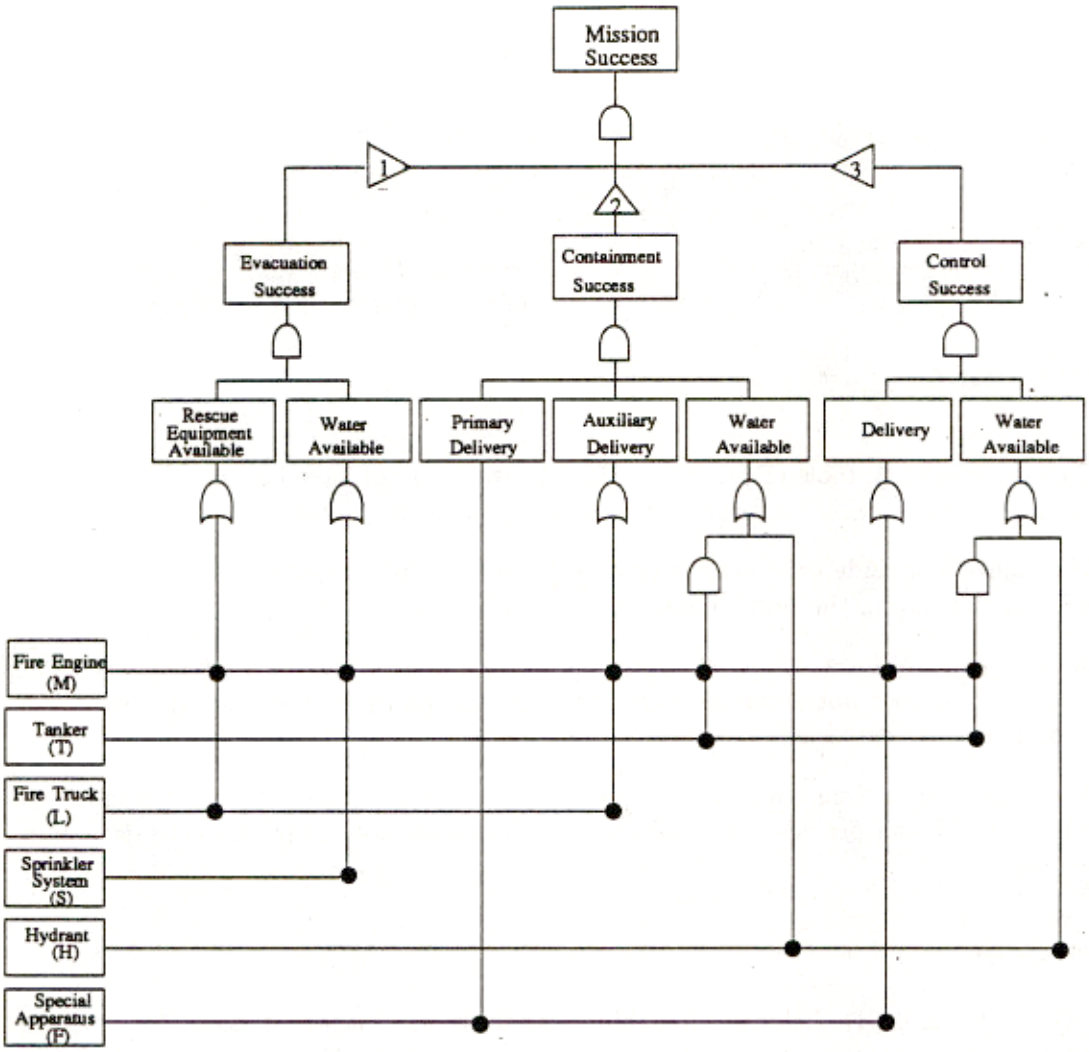


Figure 4. A dynamic goal tree for the mission of the Example.

3. Calculate the overall MCSs using time-dependent logic
   $\{M^{(1)}, S^{(1)}\}$ $\{F^{(2)}\}$ $\{M^{(2)}, L^{(2)}\}$
   $\{F^{(3)}, M^{(3)}\}$ $\{H^{(3)}, M^{(3)}\}$ $\{H^{(3)}, T^{(3)}\}$
4. Calculate system unreliability based on the MCSs

$$\begin{aligned}\bar{R} &= P(M^{(1)})P(S^{(1)}) + P(F^{(2)}) + P(M^{(2)})P(L^{(2)}) \\ &\quad + P(F^{(3)})P(M^{(3)}) + P(H^{(3)})P(M^{(3)}) \\ &\quad + P(H^{(3)})P(T^{(3)})\end{aligned}$$

5. Evaluate the development of accident sequences using proposed calculation techniques

$$P(S_1) = P(M^{(1)})P(L^{(1)}) + P(M^{(1)})P(S^{(1)})$$

$$
\begin{aligned}
P(S_2) &= P(F^{(2)}) + P(H^{(2)})P(M^{(2)}) + P(H^{(2)})P(T^{(2)}) \\
&\quad + P(M^{(2)})P(L^{(2)}) - P(M^{(2)}L^{(2)} \cap M^{(1)}L^{(1)}) \\
&= P(F^{(2)}) + P(H^{(2)})P(M^{(2)}) + P(H^{(2)})P(T^{(2)}) \\
&\quad + P(M^{(2)})P(L^{(2)}) - P(M^{(1)}L^{(1)}) \\
P(S_3) &= P(F^{(3)})P(M^{(3)}) + P(H^{(3)})P(M^{(3)}) + P(H^{(3)})P(T^{(3)}) \\
&\quad - P(F^{(3)}M^{(3)} \cap F^{(2)}) - P(H^{(3)}M^{(3)} \cap H^{(2)}M^{(2)}) \\
&\quad - P(H^{(3)}T^{(3)} \cap H^{(2)}T^{(2)}) \\
&= P(F^{(3)})P(M^{(3)}) + P(H^{(3)})P(M^{(3)}) + P(H^{(3)})P(T^{(3)}) \\
&\quad - P(F^{(2)})P(M^{(3)}) - P(H^{(2)})P(M^{(2)}) - P(H^{(2)})P(T^{(2)})
\end{aligned}
$$

CONCLUSIONS

- Current reliability tools (FTA, ETA, FMEA, etc.) do not take into consideration the dynamic nature present in process safety management problems.
- The failure to include time as an important factor can cause significant non-conservative error in calculating the probabilities of accident sequences.
- Boolean algebra, on which most approaches for dynamic event trees are based without modification, does not accommodate time sequence information efficiently resulting in a combinatorial explosion.
- By introducing a time scale into the conventional Boolean Algebra, the dynamic goal tree approach can provide a compact tool for sequence analysis in process safety management.

References

[1] J. D. Esary and H. Ziehms, "Reliability Analysis of Phased Missions," *Reliability and Fault Tree Analysis*, Society for Industrial and Applied Mathematics, pp 213-236, Philadelphia. 1975.

[2] NUREG/CR-2300, "PRA Procedures Guide: A Guide to the performance of Probabilistic Risk Assessments for Nuclear Power Plants," Vols. 1 and 2, USNRC, 1983.

[3] Amendola, A., "Accident Sequence Dynamic Simulation versus Event Trees," *Reliability Engineering and System Safety*," vol. 22, 1988.

[4] Hsueh, K. S. and Mosleh, A., "Categorization of Operator Errors in the Context of Symptom-based Emergency Operating Procedures", SMiRT, Tokyo, 1991.

[5] Siu, N., Acosta, C., "Dynamic Event Tree Analysis - An Application to SGTR," *Probabilistic Safety Assessment and Management (PSAM) (Proc . Int. Conf. Beverly Hills, 1991)*, p 413.

[6] M. L. Roush, M. Modarres, R. N. Hunt, D. Kreps, and R. Pearce, "Integrated Approach Methodology: A Handbook for Power Plant Assessment," SAND87-7138, Sandia National labs., October 1987.

[7] M. Modarres, "What Every Engineer Should Know about Reliability and Risk Analysis," Marcel Dekker Publishing, New York, 1992.

LA-UR-93-2001

CALCULATING EXACT TOP EVENT PROBABILITIES USING ΣΠ-PATREC

A. Sharif Heger,[1] Gururaj Shamanna,[1]
Desmond W. Stack,[2] and Dale V. Talbott[2]

[1]University of New Mexico, FEC 247, Albuquerque, NM 87131
[2]Los Alamos National Laboratory, N6, Los Alamos, NM 87545

INTRODUCTION

Many "real world" problems are associated with basic events with large probabilities of occurrence; the probabilities of human error and some natural phenomena are typical examples. Current quantification methods in probabilistic risk assessment (PRA) are based on the rare event approximation and therefore inappropriate in these cases and may lead to erroneous, overly conservative results. Specialized techniques for exact top event probability quantification exist, but, due to their complexity, are limited to small problems that do not reflect realistic problems in PRA.

In this paper a unique approach that combines the ΣΠ method of Corynen (Corynen, 1983; Patenaude, 1988) and pattern recognition scheme of Koen et al. (1973) is presented. The former is based on Shannon's theorem of pivotal decomposition; the latter has its foundation in artificial intelligence.

THE THEORY BEHIND ΣΠ-PATREC

Given a system, the top event, T, representing failure under a given condition, can be represented as the union of its minimal cut sets (MCS). Each MCS is composed of the interaction of the basic events. The probability of this top event equals

$$P(T) = P\left[\cup_{i=1}^{m}(MCS_i)\right]. \tag{1}$$

If the minimal cut sets are mutually exclusive, then the top-event probability reduces to

$$P(T) = \sum_{i=1}^{m} P(MCS_i). \tag{2}$$

In reality, however, minimal cut sets for most real world problems are not mutually exclusive and using the inclusion-exclusion method for the evaluating the exact top event value is NP-hard. The method described here can alleviate this problem and is based on the Σ method of the ΣΠ algorithm (Corynen, 1983). With this method, the collection of m minimal cut sets is converted to a set of n mutually exclusive events (MEE) such that

$$P(T) = \sum_{i=1}^{m} P(MCS_i) = \sum_{i=1}^{n} P(MEE_i). \quad (3)$$

This conversion process is polynomial in the number of cut sets in the expected case and in the worst case can be weakly exponential (Corynen, 1983). In either case, this method results in a substantial reduction in computational requirements compared with the inclusion-exclusion method.

THE ΣΠ METHOD

The transformation of the minimal cut sets (MCS_i: i=1, 2, ,..., m) into the set of disjoint events (MEE_i: i=1, 2, ..., n) has its foundation in Shannon's Theorem (Corynen, 1983; Barlow, 1975); that is, for any collection of Boolean variables and a structure function ϕ of these variables,

$$\phi(X_1, X_2, \cdots, X_k) =$$
$$X_i\, \phi(X_1, X_2, \cdots, X_{i-1}, 1, \cdots, X_k) + \overline{X}_i\, \phi(X_1, X_2, \cdots, X_{i-1}, 0, \cdots, X_k). \quad (4)$$

Based on this theorem and graph-theoretic ratability method, a pivot for decomposing a matrix is selected. This decomposition process reduces an n-dimensional problem to two submatrices of either equal or smaller size. This decomposition process is followed by reduction of the resultant two sets and the process continues recursively until one of the stopping criteria is met. At this point the evaluation process begins. After all of the sets are evaluated, the results are combined by a simple summation operation to calculate the exact probability of the top event.

THE PATTERN RECOGNITION (PATREC) EXTENSION

Although ΣΠ method can reduce the computational demand through its decomposition process, the scheme can demand large storage. To reduce the complexity of the scheme, it was decided to devise a scheme to avoid the evaluation of submatrices that appear more than once. This modification can lead to a substantial reduction in computation since the procedure can be exponential in the number of minimal cut sets.

Therefore by adding a pattern recognition scheme to detect those repetitions and preventing their evaluation can lead to elimination of unnecessary computational burden. To this end, an innovative approach using a pattern recognition technique called PATREC was selected (Koen, 1973). Each set first was represented as a link-list such that all variations of a given set would have one unique representation. This unique representation is then added to a library for future reference. When a set is slated for evaluation, it is compared with the content of the library before being submitted to the ΣΠ method. If the submatrix has been evaluated, its values is recorded and the ΣΠ method is skipped.

IMPLEMENTATION DETAILS

The most current version of ΣΠ-PATREC is implemented in C for three different platforms, UNIX, DOS, and Windows. Two design objectives have been incorporated in the new version of ΣΠ-PATREC. These objectives were the efficiency of the code both in terms of storage and calculation. For realistic applications with several hundred or thousand minimal cut sets and a large number of basic events, the code must calculate the exact top event probability efficiently, perhaps within minutes as opposed to hours or days. To achieve this performance objective, the storage requirement had to be minimized to reduce the expensive disk read-write operations. The goal was, therefore, set to evaluate the top event with an available four megabytes on the DOS Platform.

To achieve these objectives, a unique representation for the minimal cut set has been developed. This new data structure takes advantage of features offered by hash tables and

methods for efficient sparse matrix representation. This method alone provided a quantum leap in both speed of operation and reduction of memory allocation. A pattern recognition scheme was added to the ΣΠ code (thus the name ΣΠ-PATREC) to reduce the calculation burden by keeping track of the submatrices that were evaluated and preventing their repeated evaluation.

A second improvement in the code performance was realized by developing a non-recursive evaluation method. Recursive methods for matrix decomposition are relatively simple to implement but require a large storage space. A non-recursive method is, on the other hand, more complex but can be efficient in term of storage allocation. Prior to the actual implementation, a few test cases were evaluated to verify the superiority of the non-recursive method over the recursive approach. Experiments have demonstrated that up to 20% of the matrices created as a result of decomposition are repeated. Table 1 summarizes the improved performance of ΣΠ-PATREC using the pattern recognition technique. It must also be mentioned that in situations where the number of repeated submatrices is not large, the pattern recognition scheme could actually work the opposite way and reduce the speed of the code. This problem is still under investigation.

Table 1. Computation speed for ΣΠ with and without pattern recognition

Case	Run Time Without Pattern Recognition (Second)	Run Time With Pattern Recognition (Second)
Patenaude (1988) (MCS = 20, BE = 27)	14	10
Grand Gulf Seq. 3-14 (MCS = 1,002, BE = 79)	71	50
Grand Gulf SBO Seq. 16 (MCS = 1,053, BE = 110)	1,671	1,478

APPLICATION

The performance of ΣΠ-PATREC has been evaluated on various sample trees including those from the accident sequence analysis for internally initiated events for Grand Gulf Unit 1 (Drouin et al., 1989). In all cases the superiority of ΣΠ-PATREC over existing codes has been evident both in terms of its speed and accuracy of calculation.

To demonstrate the errors that can potentially enter in any analysis by the existing codes due to large basic event probabilities, consider a hypothetical case. In this example, consider the actions taken by an operator to recover from a service air compressor loss without automatic backup (event Y). Assume that several possible recovery options are available. The operator may choose to manually start a standby compressor (event X_1), remotely cross-connect the afflicted system with a functioning service air system (event X_2), manually bring on a storage receiver (event X_3), or cut in emergency nitrogen or cross-connect with a functioning instrument air system (event X_4). For simplicity, further assume that all of these options are equally well-known, equally difficult to perform in the required time, and equally attractive from the operation point of view. The probability of failing to perform each one of these actions will be independent and equal. Failure to perform any recovery action will result in an accident condition and is represented in Boolean algebra by a disjunction of all of the non-recovery events. Probability values well above 0.1 are common for non-recovery events of this type. For this example a non-recovery probability of 0.9 is assumed, meaning that in 9 of 10 air compressor failures, the recovery action will not be completed before accident conditions are reached. The top event (T) for this example is

$$T = \sum_{i=1}^{n} Y * X_i,$$

with n = 4, P(Y) = 1.000E-3, and $P(x_i) = 0.900$. The probability of the top event T using the rare-event approximation method is 3.600E-3. The value for T using the mincut upper bound method is 3.595E-3. Using ΣΠ-PATREC the top event probability is 9.999E-4 which is the exact value. The difference between the results obtained from the two approximate methods grows larger as n increase. For example, for n = 10 the calculated values are 9.000E-3 for the rare-event approximation method, 8.964E-3 for the mincut upper method, and 1.000E-3 for ΣΠ-PATREC.

It is evident from this example with large basic event probabilities only ΣΠ-PATREC can produce the correct top event probability and other method produce misleading values. The type of event that was used in this example is not uncommon and occurs when event Y represents a component failure, and the events represented by X_i are non-recovery factors for failure to perform some recovery option.

CONCLUSIONS

ΣΠ-PATREC is especially attractive for applications with large basic event probabilities. In these applications, the rare-event approximation and mincut upper bound methods can lead to erroneous results.

In ΣΠ-PATREC, the top-event probability is evaluated by the decomposition techniques of the original version of ΣΠ. At the same time, ΣΠ-PATREC avoids the disadvantages that usually are associated with computational complexity of the ΣΠ method. ΣΠ-PATREC detects and stores computation pattern in a library and thus avoids evaluating identical combination of minimal cut sets.

ΣΠ-PATREC has been implemented in C for UNIX, DOS, and Windows platforms. Preliminary results have demonstrate its superiority over existing codes both in terms of computation speed and delivery of exact solution.

ACKNOWLEDGMENTS

The authors wish to express their gratitude to Mr. Donnie Whitehead of Sandia National Laboratories for his technical support of this project.

REFERENCES

Corynen, G., 1983, "Evaluating the Response of Complex Systems to Environmental Threats: the ΣΠ Method," University of California report UCRL-53399.

Patenaude, C.J., 1988, "SIGPI: A User's Manual for Fast Computation of the Probabilistic Performance of Complex Systems," NUREG/CR-4800, US NRC, Washington, DC.

Koen B.V., and Carnino A., 1973, Calculation of system reliability by pattern recognition, *Transactions of the American Nuclear Society*.

Barlow, R.E., and Proschan, F., 1975, "Statistical Theory of Reliability and Life Testing Probability Models," Holt, Rinehart, and Winston, Inc. New York.

Drouin, M.T., et al., 1989, "Analysis of Core Damage Frequency: Grand Gulf, Unit 1 Internal Events," NUREG/CR-4550, US NRC, Washington, DC.

DEVELOPMENT OF THE GO-FLOW RELIABILITY ANALYSIS METHODOLOGY
- COMMON CAUSE FAILURE ANALYSIS AND UNCERTAINTY ANALYSIS -

Takeshi MATSUOKA and Michiyuki KOBAYASHI

Systems Engineering Division, Ship Research Institute, Ministry of Transport
6-38-1, Shinkawa, Mitaka, Tokyo, 181 Japan

INTRODUCTION

Since the completion of the Reactor Safety Study[1], the use of probabilistic safety assessment (PSA) has become more widespread in the nuclear and other industries. Event tree and fault tree are the basic analytical tools that have been most frequently used for PSAs, such as the Sever Accident Risks analysis[2] and IPEs. Several system analysis techniques have been also developed in support of, or in addition to, event- and fault-tree analysis.

The Ship Research Institute has been developing a new reliability analysis methodology GO-FLOW[3] which is a success-oriented system analysis technique, and is capable of evaluating a large system with complex operational sequences[4]. This paper describes the overview of the GO-FLOW analysis methodology, the GO-FLOW analysis support system, the common caused failure analysis by the GO-FLOW and the uncertainty analyses in the GO-FLOW methodology.

OVERVIEW OF THE GO-FLOW METHODOLOGY

The GO-FLOW methodology, which is a success-oriented system analysis technique, is capable of evaluating system reliability and availability. The modeling technique produces the GO-FLOW chart, which consists of signal lines and operators. The operators model function or failure of physical equipments, logical gates and a signal generator. Fourteen different types of operators are currently defined as is shown in the figure 1.

Signals represent some physical quantity or information. In the GO-FLOW the existence of a physical quantity is interpreted as both the actual and the potential existence of a physical quantity. "Potential existence" means that a physical quantity exists when all the resistance "downstream" is removed.

A quantity called "intensity" is associated with a signal. Usually the intensity represents the probability of signal existence. When a signal is used as a sub-input signal to type 35, 37 or 38 operators (standby or operating failure of a component), the intensity represents a time interval between the successive time points.

A finite number of discrete time values(points) are required to express the system operational sequence. The value does not necessarily represent the real time but corresponds to it and represents an ordering.

An analysis is performed from the upstream to the

most cases, only one or, at least, few of all the defined signals are of interest; these signals are called final signals. An analysis is completed when the intensities of these final signals at all the time points are obtained.

The GO-FLOW methodology possesses the following significant features.

(a) The GO-FLOW chart corresponds to the physical layout of a system and is easy to construct and validate.
(b) Alterations and updates to a GO-FLOW chart are readily accomplished.
(c) The GO-FLOW contains all possible system operational states
(d) The analysis is performed by one GO-FLOW chart and one computer run.

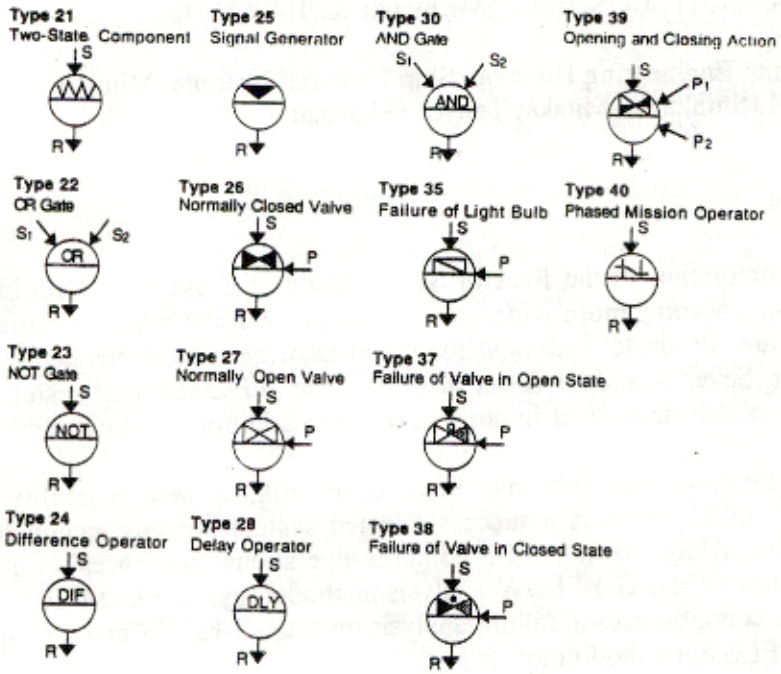


Figure 1. Operators defined in the GO-FLOW methodology.

GO-FLOW ANALYSIS SUPPORT SYSTEM

The analysis steps in the GO-FLOW methodology are: constructing a GO-FLOW chart, producing input data for the GO-FLOW analysis program, running the GO-FLOW analysis program on a main frame computer, interpreting the results of analysis, representing the results in graphic or tabular form, and producing a documentation.

If an engineering system to be analyzed becomes large, the above procedure requires a great effort, especially to construct a GO-FLOW chart and to produce input data for the GO-FLOW analysis program. Then the authors have developed the GO-FLOW analysis support system[5], which is a fully integrated personal computer (PC) based, menu driven analysis system. The objective of the development of this system is to improve the efficiency with which the GO-FLOW analysis can be conducted and

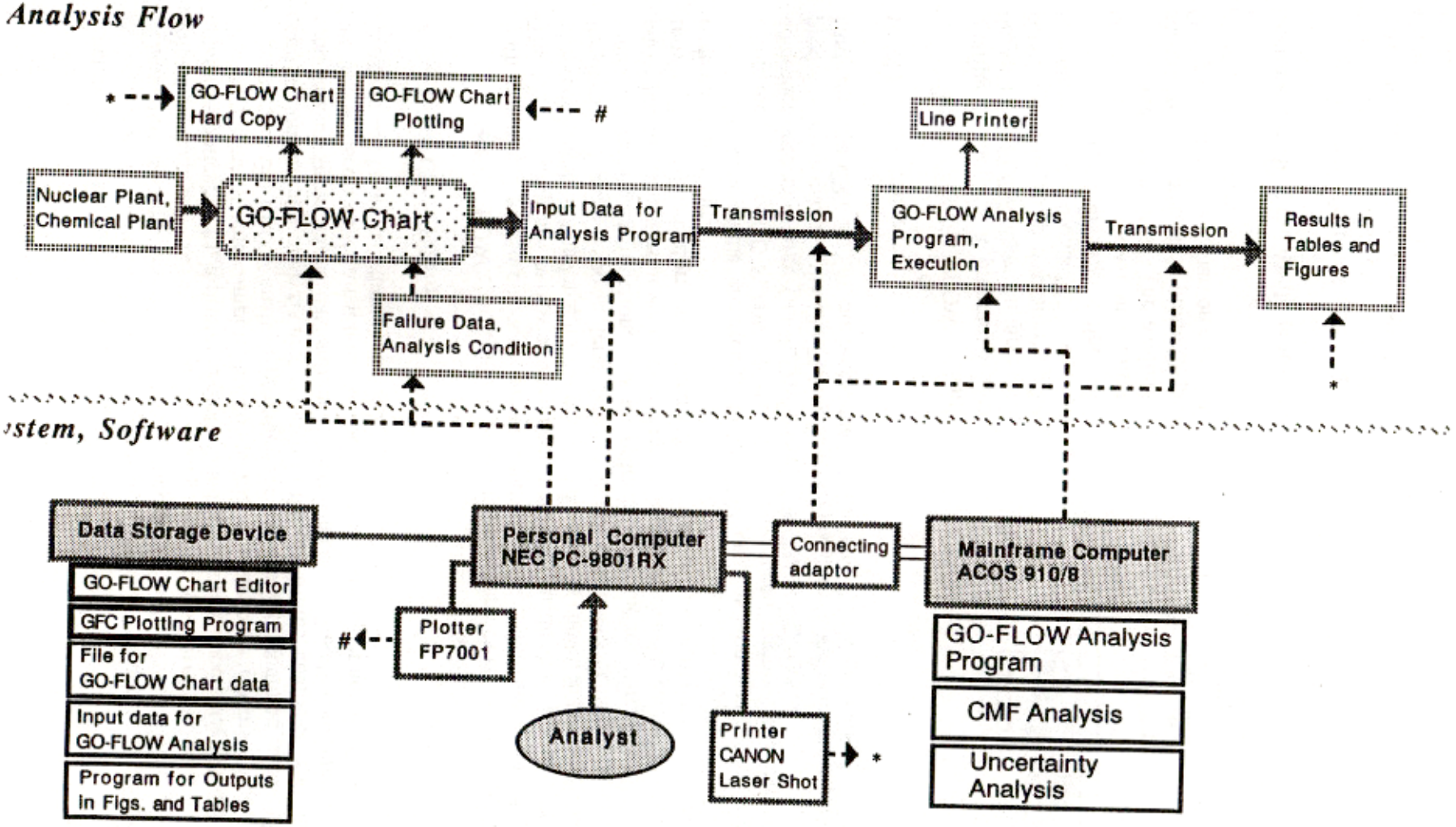


Figure 2. GO-FLOW reliability analysis support sysytem

methodology as a powerful tool in a living PSA.

Figure 2. shows the analysis steps and the hardware and software configurations. The system is composed of a personal computer (NEC PC-9801RX) with 640Kb of CPU plus 4 Mb expanded RAM board, data storage devices (20Mb of hard disk and 326Mb of a magneto-optical disk), a printer, a plotter, and a mainframe computer (ACOS 910/8). The PC and the mainframe computer are connected by a local area network.

The GO-FLOW analysis program, the programs for common cause failure analysis and the uncertainty analysis are installed in the mainframe computer, and other software and data are stored in the data storage devices which are directly connected to the PC. The PC is also used as a terminal board of the mainframe computer and the GO-FLOW analysis program can be started through the PC.

GO-FLOW Chart Editor

The GO-FLOW chart editor is an interactive graphics editor for a GO-FLOW chart with menus and mouse clicks. Icons of standardized operators are provided in the editor. The CRT display has two windows. Each window can display any part of GO-FLOW chart construction in any magnification. A main menu is shown in the upper right corner of the display. Figure 3. shows items in the main and sub-menus. Clicking on any item in the menu activates each function. As an ordinary drawing software, the GO-FLOW chart editor has the functions in which operators and signal lines are created, deleted, copied, and moved. The detailed information, such as failure data, definition of time points and comments, is given to the chart.

The data of the constructed GO-FLOW chart is stored in a file by the "Save" command. Two GO-FLOW charts, which have been previously constructed, can be combined into one large GO-FLOW chart. The "Make Data" command automatically produces input data for the GO-FLOW analysis program in the mainframe computer. The hardcopy of a CRT display can be produced by the GO-FLOW chart editor.

GFC Plotting Program

The GFC(GO-FLOW Chart) plotting program is a program which draws a GO-FLOW chart on large size paper by using a pen plotter. The program is executed on a PC.

The operators, signal lines and comments can be drawn in arbitrary colors and line widths. The available paper size depends on a plotter type. Our system can draw a chart on an usual paper up to A1 size.

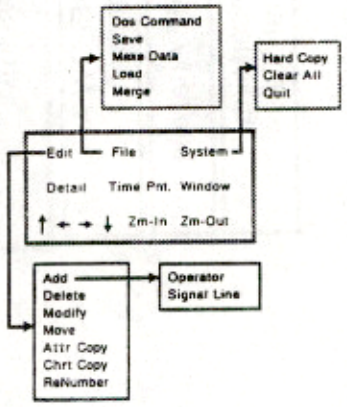


Figure 3. Items in the main and sub-menus.

Documentation of the Analysis Results

The analysis results are transmitted from the mainframe to the PC, and expressed in graphic or tabular form which could be used in a report as it stands.

The high quality figures for the results of uncertainty analysis are obtained by a laser printer connected to the PC. The development is now being carried out for a program which represents analysis conditions and input data in the form of document, and the analysis results in tabular form.

COMMON CAUSE FAILURE ANALYSIS

Common Cause failures (CCFs) have long been recognized as an important issue in the PSA for nuclear power plants. The high degree of reliability of safety systems in nuclear power plants has been achieved through the use of design principle of redundancy. If common cause failures arise over redundant systems, there is a possibility to reduce the high degree of reliability expected on the assumption of random failures.

The Authors have been developed a framework to directly treat the parametric common cause failure models in the GO-FLOW methodology[6]. In this chapter, the analysis procedure is explained and as an example of analysis, the reliability of PWR AFWS is evaluated by the MGL model[7].

Treatment of the Common Cause Failures

Usually, there are more than one common causes, and also there are many possible combinations of component failures for one common cause.

An example of CCF analysis[8] showed that the second-order terms of CCF contributed less than 1% to total system unavailability. Therefore, in this framework, each common cause is separately evaluated and the total system unavailability is obtained by summing up the contributions from all the common causes based on the following discussions.

The top event of a fault tree or a system failure will be expressed in the following general Boolean algebraic formula.

$$T(A,B)=\{A\,E + B\,F + A\,B\,G\}\,H + K \qquad (1)$$

where, A and B are basic events which are subjected to a common cause. From E to K are some Boolean algebraic terms composed of basic events. Basic events A and B are decomposed into independent events and a common cause failure as follows,

$$A = A_i + C_{AB}, \quad B = B_i + C_{AB}.$$

Substitute the above relations into equation (1), and rearrange it. Hence:

$$\begin{aligned} T(A,B) &= \{A_i\,E + B_i\,F + A_i\,B_i\,G\}\,H + K + C_{AB}\,(E + F + G)\,H \\ &= T(A_i,B_i) + C_{AB}\,(E + F + G)\,H \end{aligned} \qquad (2),$$

where $T(A_i,B_i)$ means that basic events A and B are replaced by independent failure events A_i and B_i, respectively.

The above expression could be converted into the expression of occurrence probability by considering the inclusion-exclusion relations between basic events A_i, B_i, C_{AB}, ... as:

$$P\{T(A,B)\} = P\{T(A_i,B_i)\} + P\{C_{AB}\}\,(P\{T(\mathbf{1},\mathbf{1})\}-P\{T(\mathbf{0},\mathbf{0})\}) \qquad (3),$$

where, $P\{T(\mathbf{1},\mathbf{1})\}$ and $P\{T(\mathbf{0},\mathbf{0})\}$ mean the system failure probabilities when occurrence probabilities of basic events A and B are replaced by 1.0 and 0.0, respectively. The first term is the contribution from the independent events, and the second term is from the common cause event C_{AB}.

More general formula is obtained as the next equation.

$$P\{T(A,B,...)\} = P\{T(A_i,B_i,...)\} + \sum_{C_j} \sum_{m=2}^{N} \sum_{m} P\{C_{jm}\}\,(P\{T(\mathbf{1},\mathbf{1},..)\}-P\{T(\mathbf{0},\mathbf{0},..)\}) \qquad (4),$$

where, the summations are performed on the common cause kinds C_j, the number of failed components m , and the possible combinations of m component failures.

Common Cause Failure Analysis by the GO-FLOW Methodology

The procedure for the treating the CCFs in the GO-FLOW methodology consists of the following steps.

(1) Construct the GO-FLOW chart, in which CCFs need not be explicitly expressed. Then, obtain the system unavailability which takes into account only independent events.
(2) Identify the common cause component group.
(3) Select the parametric model of common cause failure. Five parametric models are provided in this framework; Basic Parameter model, β-factor model, Multiple Greek Letter model[7], Binomial Failure Rate model, and α-factor model[8].
(4) Give the estimated values for model parameters.
(5) Obtain the contribution from a specific common cause.
(6) Repeat the steps from (2) to (5) for other common causes.
(7) Sum up the contributions from all the CCFs.

The analysis program automatically performs above steps if the analysis conditions are given in advance as input data. The input data consists of common cause component groups, type of parametric model, and values for model parameters.

Analysis by the MGL model

As a sample system, a three-train Auxiliary Feedwater System[8] of a Pressurized Water Reactor has been selected. A simplified P&ID of the AFWS is shown in figure 4. The system consists of three pump trains, which take sanction from a common condensate storage tank and supply header and provide auxiliary feedwater flow to four steam generators. There are two identical electric motor-driven pumps and a steam turbine-driven pump. There are four motor-operated valves at the pump discharge that are normally closed. Each motor-driven pump can supply flow through successful valve openings to two dedicated steam generators, and the turbine-driven pump can supply flow to up to four steam generators, depending on how many MOVs open. Although there are two kinds of pump drivers, all three mechanical pumps are identical.

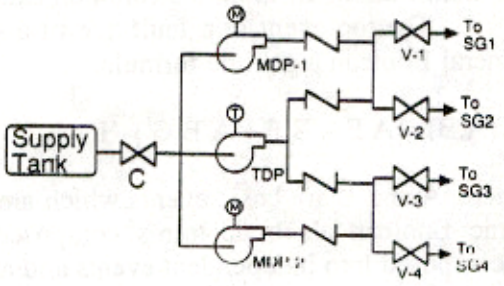


Figure 4. Flow diagram of PWR AFWS

It is assumed that the system must operate for 24 hours following its demand. For the successful operation of the system, it is needed to supply flow to at least two steam generators.

The analysis was performed by the MGL model. Three time points were declared: Time point 1 is an initial time; at time point 2, the system operation is demanded; time point 3 is 24 hours after time point 2. The values of component failure rates and demand probabilities are given in Table 1. With the assumption of independency between these failures, the unavailability of this system was obtained as 8.23×10^{-6}(time point 2) and 1.09×10^{-5}(time point 3).

Two common cause component groups were considered. The first group

Table 1. Failure rates and demand probabilities

Failure modes	Point estimates
Failure of Water Tank	2.00E-6/h
Failure of Check Valve	4.00E-6/h
Motor fails to start	1.65E-3
Turbine fails to start	3.15E-2
Motor fails to run	1.71E-5/h
Turbine fails during operation	1.01E-3/h
Pump fails to start	1.65E-3
Pump fails to run	1.71E-5/h
MOV fails to open	4.30E-3

is the electric motor and steam turbine driven pumps and the failure mode is "fails to start"(operator numbers are 8,10 and 14). The second group is the electric motors, and the failure mode was "fails to start"(operators 4 and 12).

We have assumed that the values of parameters β and γ equal to 0.697 and 0.304 , respectively for operators 8,10 and 14. The value of β has been assumed to be 0.390 for operators 4 and 12. Table 2. shows the results of the analysis by the MGL model for this sample system.

Table 2. System unavailability (MGL Method)

	Time points 2	3
Independent failure	6.86E-6	8.53E-6
Common Cause Component Group 1		
(8,10,14)	3.51E-4	3.51E-4
(10,14)	4.02E-6	4.35E-6
(8,14)	1.28E-5	2.22E-5
(8,10)	4.02E-6	4.35E-6
Common Cause Component Group 2		
(4.12)	2.07E-5	3.61E-5
Total	3.99E-4	4.26E-4

UNCERTAINTY ANALYSIS

There are two basic types of uncertainty: parameter value uncertainty and modeling uncertainty. The "uncertainty analysis" in the GO-FLOW handles the parameter value uncertainties. The distribution of a system failure probability is calculated by combining values selected by sampling from the probability distributions for all of the basic events.

The analysis procedure consists of two steps. First, the minimal cut sets(MCS) are obtained for specified signal lines. The GO-FLOW is basically a success-oriented system analysis technique. For the uncertainty analysis, basic events expressed in success probability are converted into the expression in the failure probability, and the MCSs are obtained. Next, the distributions of failure probabilities are assigned for the basic events in the MCSs and the distribution of a system failure probability is obtained with the Monte Carlo simulation. One of the following distributions can be assigned to the basic events. The Normal distribution, Log-normal, Homogeneous, Log-homogeneous, Gamma, Binomial, Weibull, Beta, and Histogram distributions.

As the analysis results, the values of median, mean, error factor, 90% ranges of uncertainty, cumulative probability distribution, and probability density distribution are obtained. These results are expressed in the form of high quality figures made by laser printer connected to the PC.

Sample Analysis

As a sample system, a simple hypothetical system was considered. The system consists of eight basic events which include recovery actions. Four time points were declared: Time point 1 is an initial time and the system operation is demanded; time points 2, 3 and 4 are 1, 2, and 10 hours after the time point 1, respectively. At the time point 2,

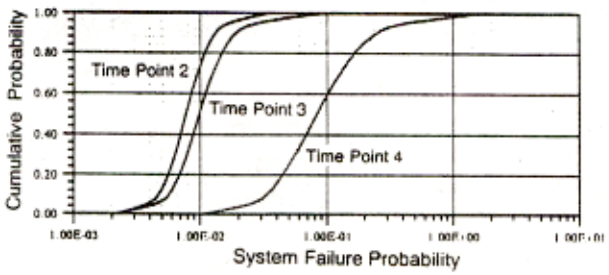


Figure 5. Result of the uncertainty analysis for a sample system

this system is equivalent to the example fault tree which was given in the Reactor Safety Study[1], Appendix II page 75.

The cumulative probability distribution of the system failure was obtained as shown in the figure 5. The log-normal distributions were assigned for basic events, and the sampling was repeated 5000 times. A variation of the distributions with time is seen in this figure. The distribution at time point 2 was exactly the same as the result given in the Reactor Safety Study.

CONCLUSIONS

In this paper, we have described the development of the GO-FLOW reliability analysis methodology. Explanations have been given for the GO-FLOW analysis support system, the common cause failure analysis by the GO-FLOW, and the uncertainty analysis in the GO-FLOW methodology.

With the aid of the support system, the GO-FLOW analysis is performed as if it were just carried out on a personal computer placed on the analyst's own desk, and the GO-FLOW methodology will be a powerful tool in a living PSA.

The framework to treat the common cause failure can evaluate CCFs effects, from the information about the CCC (common cause component) groups, CCF model and values of model parameters by the usual GO-FLOW chart which is constructed without considering CCFs-logic. That is, the parametric CCF models can be easily incorporated into a system reliability analysis with many advanced functions of the GO-FLOW methodology.

Uncertainty analysis can be also performed in the GO-FLOW methodology with advanced functions which the GO-FLOW originally has. The variation of uncertainty distribution with time is easily obtained. Failure probability distribution at any part of a system can be obtained as well as the distribution of a top event.

It has been seen that the GO-FLOW is a valuable and useful tool for system reliability analyses in PSAs.

This research is supported by a special fund of the Science and Technology Agency of the Government of Japan.

REFERENCES

1. U.S. Nuclear Regulatory Commission, Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400 (NUREG-75/014), (October 1975).
2. U.S. Nuclear Regulatory Commission, Sever Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, NUREG-1150 (December 1990).
3. T.Matsuoka and M.Kobayashi., GO-FLOW : A New Reliability Analysis Methodology, Nuclear Science and Engineering, 98:64(1988).
4. T.Matsuoka, M.Kobayashi and K.Takemura., The GO-FLOW Methodology: A Reliability Analysis of Emergency Core Cooling System of a Marine Reactor under Accident Conditions, Nuclear Technology, 84:385(1989).
5. T.Matsuoka and M.Kobayashi., Development of the GO-FLOW Reliability Analysis Support System, Use of Probabilistic Safety Assessment for Operational Safety PSA'91, IAEA-SM-321/61: 677(1991)
6. T.Matsuoka and M.Kobayashi., The Incorporation of Common Cause Failures into the GO-FLOW Methodology, Proc. of the International Topical Meeting on Probabilistic Safety Assessment PSA'93, Clearwater Beach, Florida, January 26-29, pp.811-817(1993).
7. K.N.Fleming et al., An Extension the Beta Factor Method to Systems with High Levels of Redundancy, PLG-0289(1993).
8. A.Mosleh et al., Procedures for Treating Common Cause Failures in Safety and Reliability Studies, EPRI-NP-5613, (February 1988).

MALFUNCTIONING EVALUATION OF PRESSURE REGULATING INSTALLATION BY INTEGRATED DYNAMIC DECISION ANALYSIS

R. Galvagni[1], I. Ciarambino[1] and N. Piccinini[2]

1 SYRECO, Via al Lido, 5 - 20126 Gavirate (VA) - ITALY
2 Politecnico di Torino -
Dipartimento di Scienza dei Materiali e Ingegneria Chimica,
C.so Duca degli Abruzzi, 24 - 10129 Torino - ITALY

INTRODUCTION

This paper describes a new computerised plant analysis method known as Integrated Dynamic Decision Analysis (IDDA). A full representation of the states of operation of a plant is provided by the method, as well as all the possibile modes of occurrence (description of events).

IDDA is:

"Integrated", because it automatically pairs the logical - event description with the phenomenological - deterministic description of the course of each alternative, which is thus fully defined in both logical-probabilistic and phenomenological terms, and hence with respect to its consequences,

"Dynamic", because it is based on a cause-consequence logic, and hence provides a causal description of each alternative and enables it to be interprete in a phenomenological-deterministic manner,

"Decision", because it supplies the full set of possibile alternatives, and defines each of them from the logic-event and probabilistic standpoint, and also with regard to its consequences.

The IDDA method, based on logical-probabilistic techniques using decision-tree modelling, is the end-product of a line of research on which Remo Galvagni has worked alone for a number of years (1-3).

DESCRIPTION OF THE PLANT

The example reported here to illustrate the application of the IDDA type of logical-probabilistic analysis to determination of the courses of possible alternative events, and hence to the definition and quantification of a Top Event (TE), relates to the Pressure Regulating Installation (PRI) installed on a city gas mains to reduce initial pressures of 0.5 to 5 bar to the less than 0.04 bar used in the feed pipes serving individual consumers. Branch distribution plants employ two structurally identical, automatically operating pressure reduction lines known as the "service line" and the "emergency line" (Fig. 1). A continuous supply is ensured by the automatic cut-in of the emergency line if the service line breaks down.

NOTES ON THE METHOD

An analyst who employs the widely used Fault Tree (FT) method concentrates his attention on a single TE and looks for all its possible causes. With IDDA, on the other hand, one is not restricted to following the path of failures or faulty operation alone, but must examine the system in its entirety. The analyst is thus required to describe the complete system. This description takes the form of questions regarding a series of random events related to the operation of the system itself. In other words, he asks a series of questions about the operation of the system (Table 1). Each question has only two possible answers, obviously with complementary probabilities of occurrence.

This means that each question represents a random event. The terms "questions" and "random events" will thus be used indifferently.

The question stated in capital letters (Nos.l, 16, 23, ...) are really "false questions", since their answers are tied to a pre-established outcome. The analyst uses them to create brief summaries representing sequences of answers, or "headings" of what he intends to examine. He has, as it were, obtained a bird's eye view of the situation at points where the analysis might otherwise have not have been very clear.

The program combines the answers to the analyst's questions in all possibile ways according to the constraints imposed so as to define a cluster of answers. Each sequence forming part of a cluster is thus immediately assigned its own probability of occurrence. Description by questions concerning the operation of a system is therefore open to interpretation by the program, whose task is to reconstruct all the series of events congruent with the logic contained in the description and also calculate their probability of occurrence.

Each sequence of events belonging to the cluster constitutes an occurrence "alternative" for the evolution of the system. When describing the system,. the analyst can impose constraints on the answers. For example, a given answer may render one or more subsequent questions meaningless, and it will therefore be necessary to alter the order of the sequence of questions. Alternatively, it may become evident that one of the subsequent questions must have only one of the two possible answers. In other cases, an answer may influence the probability in favour of a particular answer to the subsequent questions. It should be pointed out that these constraints may be either "logical" or "probabilistic". They are interpreted by the program as logical criteria to be followed in presentation of the cluster of events. It therefore supplies solely the combination of answers regarded as logically possible. Table 1 gives a sample of a list of 52 questions.

Only 27 are "free", i.e. either answer is possible, even if whit different probabilities.

RESULTS

Employment of the computerised IDDA method to analyse a PRI has made it possible to derive from the set of normal, disturbed and accidental operation alternatives identified not only the totality of possible events leading to accidental conditions (high or low pressure to consumers), as well as undesirable conditions (blow-off of gas, etc.), but also the gravity of their respective consequences.

Some outputs will be described below and some comments will be made on the results.

The analysis shows that autors using other techniques have themselves sometimes come to different conclusions owing to insufficient understanding of the operation of a PRI when the initial analyses were performed (4-6).

The IDDA method has now raised doubts concerning the information available, thanks to some incongruencies that have emerged from the analysis. The current technique, in fact, in addition to allowing account to be taken of the logical and probabilistic dependencies between events, enables a complete set of all mutually self-excluding alternatives (partition) that might occur to be constructed. This has led to identification and correction of gaps in knowledge of

the plant being examined, and the logical and probabilistic congruence of the alternatives supplied by the program.

Two important aspects of the question are not dealt with in this paper. No reference is made to the behaviour of the system in response to the gamut of possible manoeuvres that could be performed by those in charge of the plant. Furthermore, no examination has been made of the dynamic patterns of the physical quantities involved in function of the occurrence of the different events. It has not been possible, therefore, to integrate event analysis with the phenomenology and hence fully exploit the possibilities offered by the method.

Close examination of the outputs (obviously omitted here) has shown that the most likely TE resulting in "low pressure to the users" is faulty operation of the service or the Emergency line Monitor.

On descending a further degree of detail concerning the reasons for this event, one can deduce that its most probable cause will be closure of the monitor shutter.

The use of questions makes it easy to describe the system to any degree of detail required. If the analyst is not satisfied with the computer output, he can simply increase the number of questions addressed to the machine.

When a cut set of 10^{-10} events every two months was imposed on the probability of the alternative sequences of events considered, IDDA provvided 365 descriptions of alternative plant situation patterns (with a total probability of 0.99999953). The paths leading to the Top Event regarded as most significant were drawn from the complete set. These Top Events are illustrated in Table 2.

In Table 3 is given a description of the alternative most likely to occur.

CONCLUSION

IDDA is generally applicable for the decision analysis and solution of risk evaluation problems. It involves the formulation of a logical-probabilistic model providing a true, logical simulation of a plant and the set of its logically possible alternatives presented as sequences of events that are congruent in terms of both the internal logical and the probabilistic formulation. The degree of detail reached in the compilation of such sequences will be determined by the degree of detail in defining the events themselves required by the objectives of the analysis. Events, therefore, are the fundamental elements for application of the tools and rules of logic in the analysis.

Attribution of randomness to an event enables it to be correctly used in probability analysis.

The distinguishing feature of IDDA lies in its employment of logic tools to derive from events the full set of mutually self-excluding sequences, which are thus alternatives (constituents of a partition). Congruence of the probability evaluations is thus ensured, since this requires that the total probability in a complete set of alternatives should add up to one. A variation in the probability of even a single event alters the probability of the full set of alterantives, and congruency is thus automatically preserved. This assurance of logical completeness and respect for congruency in probabilistic evaluations cannot be supplied by any of the other analysis systems currently available.

Furthermore, this is far from being just a theoretical refinement. It is also a practical advantage insofar as it provides a greater amount of information and reduces the analysis time.

Availability of the full set of alternatives allows the complete spectrum of possible probability-consequence conditions to be kept constantly present. Information is obtained concerning critical events, and decision can be taken with full knowledge of the entire distribution of the risck, not just its mean value or the value of some particular and individual situation.

IDDA also solves the difficult question of transmission of the results of an analysis to those who need to use them. Written reports, in fact, are usually bulky and of little use,

especially when urgency is essential. Presentation on a monitor of anticipated sequences of events and their partial and final consequences, on the ohter hand, is both effective and timely. Experience shows that the method whereby logical sequences of events are arranged in both temporal and causal succession is particularly intelligible to experts, even those not specially acquainted with logical-probabilistic or realiability analysis.

ACKNOWLEDGEMENTS

A word of heartfelt thanks is also due to Claudia Ciarambino of SYRECO for assistance in using the software and in the data processing.

The cooperationg of the Pietro Fiorentini Co. (Vincenza), especially on the part of Paolo Calciolari, must also be placed on record. The indispensable informationg concerning the operation of the PRI thus supplied both made the research possible and enabled more results to be obtained than in the past.

REFERENCES

1. F. Felicetti, R. Galvagni and G. Zappellini, "Analisi di Sicurezza - Metodologia Semiprobabilstica e suo Sviluppo Applicativo", CNEN-RT/DISP, No. 78, 10, (1978).
2. R. Galvagni and S. Clementel, "Risk Analysis as an Instrument of Design", in "Safegy Design Criteria for Industrial Plants", M. Cumo and A. Naviglio (eds), CRC Press, Boca Ratom, (1989).
3. S. Senni, M.G. Semenza and R. Galvagni, "A.D.M.I.R.A. - An Analitycal Dynamic Methodology for Integrated Risk Assesment", Int. Conf. Probabilistic Safety Assessment and Management, Feb. 4-7, 1991, Beverly Hills, G. Apostolakis (ed.), Elsevier, New York, (1991).
4. N. Piccinini, M. Scarrone, E. Malinverni and P. Rosti, "Availability of a pressure regulating installation on a city mains", Reliability Eng. Syst. Safety, 20, 303-321, (1988).
5. I. Ciarambino, M. Scarrone and N. Piccinini, "Quantitative Operability Analysis: a study of a Pressure Regulating Installation on a city mains", proc. Int. Conf. Probabilistic Safety Assessment and Management, Feb. 4-7, 1991, Beverly Hills, p. 625, G. Apostolakis (ed.), Elsevier, New York, (1991).
6. N. Piccinini, M. Scarrone and I. Ciarambino, "Operability analysis devoted to the development of logic trees", to be published on Reliability Eng. Syst. Safety.

Table 1 - Sample of tipical question or statement

Component or event		Question		Item
- START				1
- Main filter	(is)	OK ?	Clogged ?	10
- Emergency line filter		OK ?	Clogged ?	14
- SERVICE LINE				16
- Erroneous opening of Service line		No ?	Yes ?	18
- Erroneous intervention of Slam-shut valve		Yes ?	No ?	22
- SERVICE LINE REGULATOR				23
- Down stream pressure		Stable ?	No-stable ?	24
- Low pressure to users		No ?	Yes ?	26
- High pressure to users		No ?	Yes ?	28

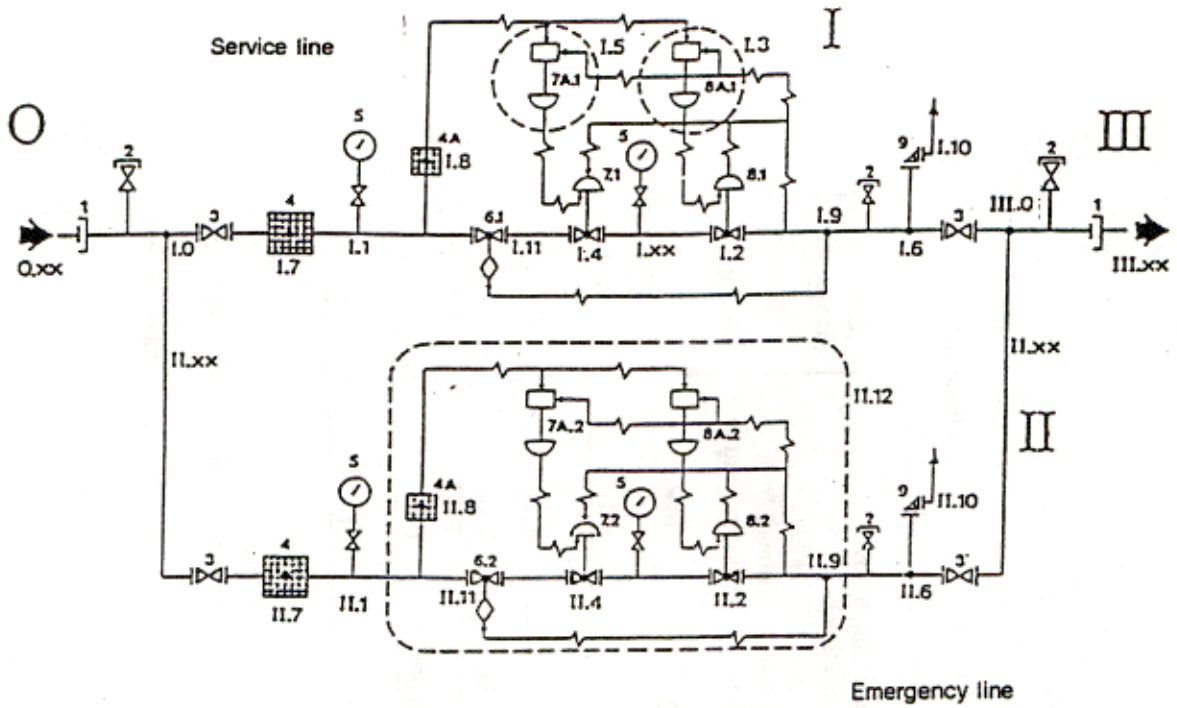


Figure 1 - Layout for a branch unit PRI and its division into sub-systems

1. Insulating joint; 2 Pressure inlet; 3 Cutt-off valve; 4 Main filter; 4A Pilot filter; 5 Pressure gauge; 6 Slma-shut valve; 7 Monitor; 7A Monitor regulator pilot; 8 Regulator; 8A Regulator pilot; 9 Vent valve

Table 3 - Description of the most probable alternative

	ITEM		PROBABILITY		FAILURE PROBABILITY
		(1)	(2)	(3)	(4)
ALTERNATIVE:	1 st				
START	1	+	B	1.000	
Main filter ok	10	+		0.954	$4.6 \cdot 10^{-2}$
Emergency line filter ok	14	+		0.950	$4.6 \cdot 10^{-3}$
SERVICE LINE	16	+	B	0.950	
Emergency line	18	+		0.950	$2.71 \cdot 10^{-5}$
Monitor open	20	+		0.937	$1.29 \cdot 10^{-2}$
Slam-shut valve	22	+		0.937	$3.5 \cdot 10^{-4}$
SERVICE LINE REGULATOR	23	+	B	0.937	
Regular operating of Regulator	24	+		0.936	$8.4 \cdot 10^{-4}$
Down stream pressure on the range	28	+		0.917	$1.3 \cdot 10^{-2}$
REGULAR PRESSURE TO USERS	990	+	B	0.917	
CUMULATED PROBABILITY				0.917	

NOTE:

1. The "+" signs indicate that an event announced on the left of the line has responded with a success.
2. The "B" shows that the elementary event concerned is bound to be sussessful or unsuccessful as the result of prior events occurring in the same alternative.
3. The probabilities shown for each elementary event indicate the probability accompanying the evolution of the alternative as far as the occurrence (included) of the event itself.
4. Values of the probability of "failure" of the elementary event present at that level. These values are referred to the entire mission time (= 2 months).

Table 2 - Events analysis of a branch type PRI

Probability cut: 10-10 Total n. of alternatives: 237 Cumulated probability: 0,99999953 Mission time = 2 months

TE	Description	N. of alterna-tives	Enthropy of examined alternatives (1)	Fair wager on verified alternative (2)	Probability per single TE [in mission time] Top limit x 10^{-4}	Mean x 10^{-4}	Botton limit x 10^{-5}	Estimate from point by point set x 10^{-5}	Expected frequency (Event/Y)
1	Very high pressure to users	38	1.39	162 / 100	1.73	0.74	2.08	5.27	1/3162
2	Low pressure to users	147	2.1221	335 / 100	8.29	5.20	29.60	45.90	1/363
3	Sudden blow-off of gas	71	1.0217	103 / 100	6.93	3.06	9.26	25.05	1/666
4	Continuous discharge of gas	31	0.476	39 / 100	1.76	5.99	0.90	3.94	1/4230
5	Pulsed discharge of gas	117	0.779	71 / 100	26.3	10.70	27.20	84.17	1/198

NOTE:

1. Indicates the degree of disorder of the possible alternatives, and hence the difficulty of identifying the alternative that has occurred. This indication provides the mean number of questions that need to be asked in order to identify such alternative.
2. Indicates the amount that could be wagered on the occurrence of the most probable alternative against 100, ending at par on a high number of wagers. It thus shows the extent to which the most probable alternative prevails over the others. It is derived from S (the entropy value) according to the relation: $(2^S-1)\cdot 100$.

033 Team Skills and Group Processes in Human Reliability

Chair: D. Orvis, Accident Prevention Group

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

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

THE SIGNIFICANCE OF OPERATOR TEAM INTERACTION SKILLS TO NUCLEAR POWER PLANT RISK

Michael S. Harris[1]

Risk & Safety Analysis Group
Pacific Northwest Laboratory
P.O. Box 999
Richland, WA 99352

INTRODUCTION

Historically, most accidents of large magnitude are caused by a combination of both human and mechanical failures. Two examples from the nuclear power industry that support this observation are the 1979 accident at Three Mile Island and the 1986 accident at Chernobyl. The Rogovin Commission, in it's analysis of the accident at Three Mile Island, reported that "...The persistent failure of the ... operating crew - and of the monitoring personnel in the control room - to recognize and react to these symptoms is one of the abiding mysteries of the first day of the accident." (Rogovin, 1980). Seven years later, and 10,000 miles away, the staff of the Chernobyl Unit 4 nuclear power plant began a test before the plant shut down for its annual maintenance. Twelve hours later, two explosions blew off the 1,000-ton concrete cap of the reactor, resulting in the worst accident in the history of commercial power generation.

Each of these accidents involved a combination of both human and mechanical failures. The accident at Chernobyl, in fact, was due almost entirely to human actions and decisions. It has been noted that at least six violations of procedures occurred during the hour before the explosions, and eight major operational errors and management control breakdowns contributed to the Chernobyl accident (NRC, 1987).

---

[1] This report was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability of responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights. The views expressed are those of the author and do not necessarily reflect the views of the Nuclear Regulatory Commission.

Although both of these accidents involved a combination of human and equipment failures, the consequences and circumstances associated with these two accidents were very different. In addition, the equipment used in these two plants was of radically different design, and was controlled by dissimilar work stations. However, despite these radical differences in design, a number of the human factors were alarmingly similar. Crew members at both plants did not provide adequate checks and balances for each other. In both cases, significant consequences resulted before the crew members shared their doubts with each other about what was going on and what should be done. These examples illustrate the potential importance of team interaction skills during events involving extreme stress or uncertainty. Specific examples of the types of team interaction skills that are required during operation of a nuclear power plant are given in Table 1.

Table 1. Examples of Operator Team Interaction Skills

Generic Team Skills	Task-Related Behaviors
Communications	Crew members are kept informed of plant status
Feedback	Crew members acknowledge receipt of information
Effective Influence	Crew members openly oppose decisions with which they do not agree
Conflict Resolution	Crew members discuss areas of disagreement
Leadership	Crew members take action when a crew member is overloaded with work

Deficiencies in the types of team interaction skills identified in Table 1 have been found during observation of control room team skills, during simulator training sessions, and during review of actual incidents (Montgomery, 1991). For purposes of this paper, it is assumed that these deficiencies could be minimized by implementing team skills improvement programs. These improvement programs would be designed to ensure that (1) each crew member's technical and diagnostic inputs are considered, (2) independent perspectives are provided on plant problems, (3) team members look out for each other and catch or prevent errors, and (4) in work overload situations, team members support each other.

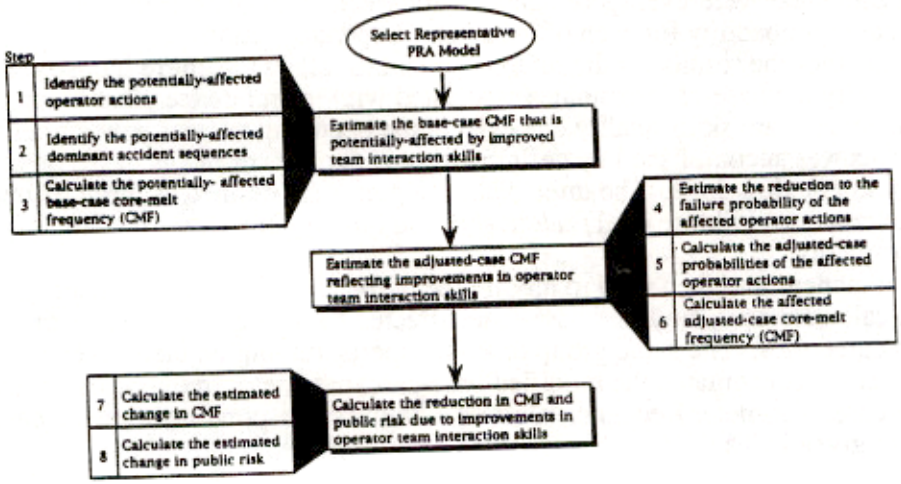
In this paper, the significance of operator team interaction skills to nuclear power plant risk is assessed. The objective of this assessment is to evaluate the reduction in public health risk that might be achieved by improving operator team interaction skills at nuclear power plants in the United States.

APPROACH

The approach used here is derived from *A Handbook for Value-Impact Assessment.* (Heaberlin, 1983). The significance of operator team interaction skills is measured by the potential reduction to core-melt frequency (CMF) and public health risks that could result from improving operator team interaction skills. Such improvements to operator performance are assumed to result from team skills improvement programs and subsequent changes to operator training and examination. The improvements in operator team skills are assumed to directly result in a reduction in the probabilities of specific operator errors.

The first step of the approach is to identify the specific operator actions that could be affected by improvements to team interaction skills. This was accomplished by reviewing the operator actions modeled in a representative Probabilistic Risk Assessment (Sugnet, 1984). The potential effect on each of the identified operator actions was then evaluated using a sensitivity technique. This sensitivity technique was used to: 1) estimate the reactor core-melt frequency that can be affected by improvements to operator team interaction skills (this is referred to as the "base-case" affected core-melt frequency), 2) using expert judgement, estimate the "adjusted-case" core-melt frequency assuming that the quality of operator team interaction skills is improved by specific measures, and 3) compare the "before" and "after" estimates of overall core-melt frequency to determine the potential reduction in core-melt frequency associated with the potential improvements to operator team interaction skills. Estimates of the core-melt frequency reduction were then extended to represent a reduction in public health risk.

Because the objective of this assessment is to evaluate the *relative* reduction in public risk due to improved team interaction skills, no attempt was made to reevaluate the baseline risk of nuclear power plant operation. The approach relies on the use of the reference Probabilistic Risk Assessment (PRA) to provide the quantitative framework for modeling the significance of operator team interaction skills. The reference PRA also provides the original risk equations for the plant, including the dominant accident sequences and their associated cut sets, along with the basic events that form the cut sets. Therefore, the reference PRA serves as the starting point for the approach, which can be characterized by an 8-step process illustrated in Figure 1.



Note to Plenum Publishing: 1) this illustration is Figure 1 of my paper (Michael S. Harris)
2) please reduce this figure to fit portrait style (not landscape)
3) the suggested location of this figure is shown in my paper

Figure 1. Overview of Approach

RESULTS

Based on a detailed review of the reference PRA, over one dozen operator actions were identified as being potentially-affected by improvements to operator team interaction skills. Descriptions of the potentially-affected operator actions, along with their event identification codes and base-case probabilities, are provided in Table 2.

Table 2. Potentially-Affected Operator Actions[2]

Event Identifier	Base-Case Probability	Description of Operator Action
YRBSH	0.5	Operator fails to terminate Reactor Building (RB) spray (given RB cooling available) to extend availability of suction for High Pressure Injection (HPI) during small-break Loss Of-Coolant Accident (LOCA)
XHPR2H	0.003	Operator fails to decide on and correctly implement High-Pressure Recirculation (HPR) within 2 hr after a small-break LOCA
REFDW2	0.3	Operator fails to recover feedwater given that two sources are available (main feedwater recovery or a suction supply from another unit) and given failure to initiate HPI cooling
REIA2/6	0.055	Failure of the operating staff to recover Instrument Air (IA) prior to depletion of the Upper Surge Tank (UST)

These potentially affected operator actions were then reviewed by a group of PNL experts. These experts, most of whom are certified as either a Senior Reactor Operator or Shift Technical Advisor, estimated the expected change to the base-case probability of each of these events assuming that operator team interaction skills are improved by specific measures. The highest and lowest estimates received from the experts were eliminated and the remaining estimated were averaged. The resulting estimates were then used to calculate the "adjusted-case" probability for each of the affected operator actions.

In order to tailor the results for the reference plant to reflect the entire industry, it was necessary to modify the base-case estimates associated with the reference plant to represent the variance in actual team skills quality that exist in the operating nuclear power plants across the country. This was accomplished by defining three categories of plants based on current quality of team interaction skills. The three plant categories are defined as those plants whose current team interaction skills are of: 1) *relatively good* quality, 2) *intermediate* quality, and 3) *relatively poor* quality.

Expert judgement was then used to modify the base-case, affected parameter frequencies to calculate new, modified base-case, affected parameter frequency estimates for the three plant categories. The same group of PNL experts, relying on their diverse operational experience, estimated the modified base-case, parameter frequencies. These modified base-case, parameter frequencies, along with the corresponding adjusted-case frequencies, are given in Table 3.

---

[2] For purposes of brevity, not all potentially-affected operator actions are shown in this Table.

Table 3. Probabilities of Affected Operator Actions

Event Identifier	Modified Base-Case Probability Current Quality of Team Interaction Skills			Adjusted-Case Probability
	Relatively Poor	Intermediate	Relatively Good	
YRBSH	0.7	0.5	0.1	0.04
XHPR2H	0.01	0.003	0.001	0.0008
REFDW2	0.6	0.3	0.03	0.003
REIA2/6	0.1	0.055	0.02	0.002

These modified parameter probabilities were then incorporated into the original PRA risk equations for the affected core-melt accident sequences. These affected core-melt sequences along with their estimated annual frequencies, are provided in Table 4.

Table 4. Affected Accident Sequences

Accident Sequence Identifier	Base-Case Frequency Current Quality of Team Interaction Skills			Adjusted-Case Frequency
	Relatively Poor	Intermediate	Relatively Good	
G, T12BU	4.4E-5	1.3E-5	2.8E-6	3.4E-7
A, SYSXS	2.1E-5	4.5E-6	3.0E-7	9.6E-8
E, T10BU	1.3E-5	4.7E-6	2.3E-7	3.7E-9
B, AXA	9.3E-6	4.7E-6	9.3E-7	8.4E-7
F, T6BU	6.5E-5	3.2E-6	4.7E-7	6.8E-8
A, AXA	9.3E-6	2.8E-6	1.9E-6	1.9E-6
A, T2BU	3.1E-6	7.7E-7	3.8E-9	7.7E-10
TOTAL	1.6E-4	3.4E-5	6.6E-6	3.2E-6

The reduction in public health risk is estimated by multiplying the core-melt frequency reduction estimates by a factor that represents the public dose associated with a core-melt accident. A conservative dose conversion factor of 4.8E+6 person-rem per core-melt event is used in this analysis[3]. Based on this dose conversion factor, the public risk reduction estimates for relatively poor, intermediate, and relative good plants are 750, 150, and 16 person-rem/year, respectively[4].

---

[3] This dose conversion factor is consistent with a severe (PWR-2) release category (NRC, 1975).

[4] To help put these results into perspective, consider that the overall core-melt frequency for the reference plant is 2.0E-4 accidents/year. Applying the above dose conversion factor, this represents a public health risk of approximately (2.0E-4)(4.8E+6) = 960 person-rem/year.

In conclusion, the results of this study indicate that the significance of operator team interaction skills to nuclear power plant risk can be quite large. Additionally, it appears that for those plants whose current quality of team interaction skills is relatively poor, the potential reduction in public risk achievable by improving operator team interaction skills is large. Even for those plants whose current quality of team interaction skills is intermediate, the potential reduction in public risk is significant. As expected, however, there is limited improvement potential for those plants whose current quality of team interaction skills is relatively good.

ACKNOWLEDGMENTS

This work was supported by the Office of Nuclear Regulatory Research of the U.S. Nuclear Regulatory Commission. The author, however, acknowledges sole responsibility for the content of this paper. The author wishes to acknowledge the time, effort, and valuable assistance provided by the various PNL staff members who provided their considered expert judgement. In addition, the author appreciates the contributions and guidance provided by Joel Kramer, the project technical monitor at the U.S. Nuclear Regulatory Commission.

REFERENCES

Heaberlin, S. W., et al. 1983. *A Handbook for Value-Impact Assessment.* NUREG/CR-3568, Pacific Northwest Laboratories, Richland, Washington.

Montgomery, J., C. D. Gaddy, J. Toquam. 1991. "Team Interaction Skills Evaluation Criteria for Nuclear Power Plant Control Room Operators." In *Proceedings of the Human Factors Society 35th Annual Meeting*, pp. 918-922.

Rogovin, M., et al. 1980. *Three Mile Island: A Report to the Commission and the Public.* NUREG/CR-1250, Vol. 1, U.S. Nuclear Regulatory Commission, Washington, D.C.

Sugnet, W. R., et al. 1984. *Oconee PRA, A Probabilistic Risk Assessment of Oconee Unit 3, Summary Report.* NSAC-60, prepared jointly by the Electric Power Research Institute, Palo Alto, California, and Duke Power Company, Charlotte, North Carolina.

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

U.S. Nuclear Regulatory Commission (NRC). 1987. *Report on the Accident at the Chernobyl Nuclear Power Station.* NUREG-1250, U.S. Nuclear Regulatory Commission, Washington, D.C.

ROOT CAUSE ANALYSIS METHODOLOGIES: TRENDS AND NEEDS

Giacomo Cojazzi, Licia Pinola

Commission of the European Communities, Joint Research Centre
Institute for Systems Engineering and Informatics, 21020, Ispra, Varese, Italy

INTRODUCTION

The technological advances in managing complex plants, by means of more and more powerful control and protection systems, has shifted the active role of the operator towards a supervisory task. In this sense, the human activities mainly "play the game" during critical situations, such as operational transients and emergencies caused by failures. Moreover, the increased reliability of the "hardware" of the plant, as a result of the design improvements, the use of advanced materials and the extensive application of reliability techniques has outlined the potential weakness of the human element.

The study of accidents such as those of Three Mile Island and Chernobyl has revealed the role of the operator errors in worsening the progression of the accident itself. On the other hand, excluding sabotages and terrorist actions, the human interventions are always aimed by good intentions, and eventual errors are the result of different concurring causes. This complexity and the great variability and unpredictability of human performances, with respect to system performance, has been recognized as one of the main difficulties of the human factor analysis since the work of Swain (1976).

Human errors have a clear impact on safety and economical aspects, it has been estimated that 30 % of the automatic scrams in nuclear power plants is due to human errors (in 1991; this value is obtained from the data of the Incident Reporting System, jointly operated by OECD-NEA and IAEA). This situation is also common to other domains: an analysis of the data for air carrier operations over a 24 years period shows that about two thirds of all accidents are attributable to the cockpit crew (Boeing, 1985). These statistics, although very important, must be properly interpreted since often human errors are not the real causes of the accident, but are the result of systems failures or inappropriate procedures, etc. Therefore, in order to introduce changes in the design of the socio-technical system capable of preventing the occurrence of future accidents, a "detailed" analysis of actual accidental/incidental sequences represents the primary source of information. To this aim the Institute of Nuclear Power Plant Operations (INPO, 1988) has promoted a Human Performance Evaluation System (HPES) which is largely adopted by American Utilities as a method for the assessment of human performances. The IAEA ASSET service (IAEA, 1991)

concentrates on hardware and software ameliorments on the basis of an assessment of plant operational performance involving plant anomalies and incidents/accidents. Analogous operational data are collected by airplane companies, chemical industries, etc.

Starting from an initiating event, e.g. a system failure or a human error, the evolution of an incident is the consequence of the subsequent interactions of the system, with the intervention of automatic and manual controls, the protection systems, and the adopted emergency procedures. Root Cause Analysis (RCA) methodologies are conceived for the retrospective analysis of the accidental sequence to analyze system failures and the involved human actions in order to identify which ones involved errors and why, i.e. the root causes. In general RCA approaches are conceived for both system failures and human errors (Paradies, 1991) (Cojazzi, 1993). In this paper the basic needs for a tool aiming at the assessment of the causes of human errors are presented and discussed with reference to the current existing tools and methodologies.

A RCA FRAMEWORK

A first-attempt schema for a general framework of Root Cause Analysis Methodology is proposed hereafter. Four main phases can be envisaged: 1) data acquisition, 2) representation of the incidental sequence, 3) identification of system failures and of human erroneous actions and, 4) causal analysis.

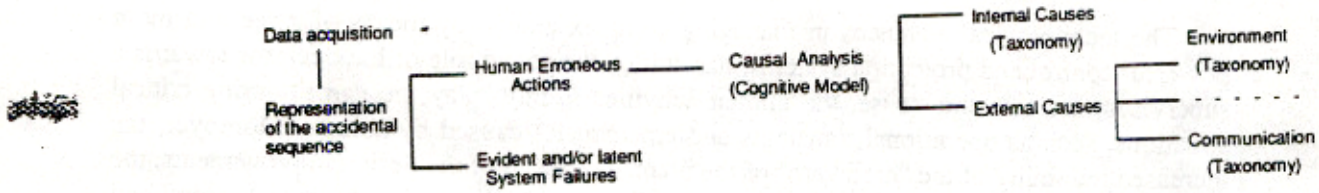


Figure 1. Framework for a root cause analysis of human erroneous actions.

The analysis of an accident with the aim of finding the causes of human errors raises the problem of the definition of human errors. Many authors have attempted a general definition of what is a human errors. Reason (1990) considers skill-based slips and lapses and rule and knowledge-based mistakes: the following definitions are given: " a) slips and lapses in which actions deviate from current intention due to execution failures and/or storage failures...and b) mistakes in which the actions may run according to the plan but where the plan is inadequate to achieve its desired outcome" (Reason, 1990 p.53).

The main problem with the term "human error" is that it is employed for indicating both the cause of an event and a special class of actions. For this reason Hollnagel (1991) introduced the term "erroneous action" in order to indicate an unwanted event without implying anything about its cause. " An erroneous action is an action which fails to produce the expected result and which therefore leads to an unwanted consequence" (Hollnagel, 1991). Erroneous actions are not observable by themselves, they are to be seen in the context and they can be identified only if their consequences can be predicted (Hollnagel, 1993). Hollnagel criticizes the Reason's definitions because "According to these expressions it is only possible to recognize a slip or a mistake if it is also known what the person's intentions are, which plan(s) he was trying to carry out, etc..... furthermore unequivocally identifying a person's intentions is clearly beyond the ability of most people" (Hollnagel, 1993, p. 70). The definition that Hollnagel gives concentrates on the consequences of an erroneous action, but

is also, in our opinion, not totally satisfying since to characterize an erroneous action Hollnagel introduces terms like "expected results" and "unwanted consequences" that answer to the question "by who" and are not so far from the "intentions" of Reason.

A more pragmatic approach to the definition of erroneous actions might be the following: "An erroneous action prevents the fulfillment of the mission and leads the system to an immediate or potential hazardous state". From the point of view of accident analysis, of highly proceduralized man-machine systems, it can reasonably be said that each deviation from the procedures, written or even tacit ones, is a "potential error". In the case that the operator deviates from the procedure, an expert of the domain should be able to explain if the alternative actions performed by the operator should be considered correct or not, in respect to their expectations, achievements and consequences on the system. This last definition implies that the procedures are the ideal sequence of events to be performed, erroneous actions are deviations from the procedures; errors in the procedures can be seen as latent failures in the system that can cause an hazard condition on the system itself.

In the accident analysis the operator should be considered as an information processor: in this sense he receives information from the system and then, after some cognitive processing of these information he produces, as output, actions on the system. Therefore, the analyst should recognize if system failures exist in input and/or output to the operator. In the former case the operator does not receive the correct input, in the latter case the system can not respond correctly to his actions. The identification of these system failures, at this level of the analysis, could result not always possible. In these cases the root cause analysis of the erroneous actions is performed and the cause, will result as external to the human being.

One fundamental task of the root cause methodology is to provide a guide for the punctual definition of the accident "details" which must be specified in order to perform the set goal of finding the basic causes of human errors. Hence, first of all, a suitable representation method of the incidental sequence must be accomplished, starting from the available data and information about the overall evolution of the accident. Typical sources of information are represented by interviews with people involved and walk through analysis, reporting forms and questionnaires to determine aspects such as the work activities etc.. The required data can be also extracted from a black box, videotapes and registrations, elicitation of operators and experts, and so on. It must also be stressed that multidisciplinary teams, combining human factor specialists and reliability experts are preferred for the analysis.

The second step to be accomplished is the transcription of the acquired and organized knowledge in an hyper space whose main dimensions will be the time, the system components, the involved operators, their actions and intentions, the information fluxes, and the ideal procedures written or tacit, which had to be pursued. In the analysis of the time-evolving accidental sequence, the third step to be accomplished is the distinction between human errors, in terms of error manifestations or modes, and system failures; finally the root causes must be ascertained.

While the data representation structure, the logical pattern tracing to causes, and the internal causes provided by the RCA methodology have to be of general validity, the external causes and also the communication-related errors are less general, since to be effective they must be related in a quite strong way to the particular domain of application. With respect to internal causes, the goal of the RCA is to find the cognitive levels involved in the process that lead to the error (Rasmussen, 1986; Hollnagel and Cacciabue, 1991), to identify at which one of these levels the error arose, and its root causes.

Operators and pilots are seldom isolated and they actually work in teams and, hence, the communication amongst the crew members has to be considered as a relevant source of mistakes (Lucas and Embrey, 1986). A communication-error taxonomy structure should be included, based on a communication schema which takes into account the emitting and the receiving nodes, the message, the transmission channel, the code, the feedback, the noise and

the redundancies of the information, the decoding process, the received message, the tacit knowledge, and the roles played by the humans in the communication procedure.

IMPLEMENTATION OF THE METHODOLOGY

In order to find the causes of human errors a possible implementation schema is presented in figure 2. Two main blocks refer to: 1) Event Sequence Analysis, with the aim of representing and analyzing the sequence of events and to identify the human erroneous actions for which 2) the Causal Analysis has to be performed.

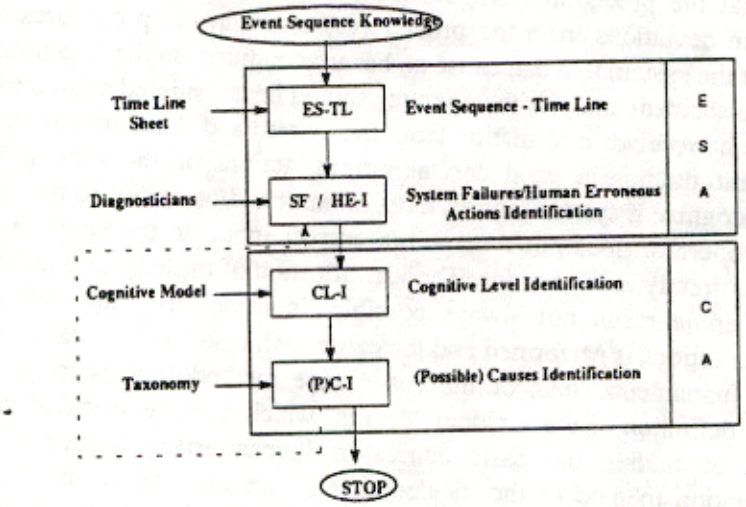


Figure 2. Schema for the implementation of a RCA methodology of human erroneous actions.

Event Sequence Analysis

Different methods and tools are available to the analysts in order to represent the sequence of events, both in term of human actions and plant changes of state, in a time ordered way. An event tree can give an idea of the progression of the incident; in principle a two-items description reporting separately the technical system state and the human system state gives the basic information on the incident progression.

The defense in depth concept, implemented in nuclear power plants, with multiple safety systems and recovery actions of the plant operator, is intrinsically modeled in some methods based on the concept of "barrier analysis". In the AEB method (Svenson, 1991) the basic assumption is that an incident in a plant should naturally stop due to the presence of safety barriers: it is the breaking of these safety barriers that causes the accident to occur. In this method the concept of root cause is not used, since the goal of the analysis is to find the breaks in the safety barriers in order to improve them. This concept is derived from the previous ideas of (Leplat and Rasmussen 1987) to represent the accident in terms of variations of human and system performances and to identify breaks that can stop the accident progression.

Another important concept relates to the safety criticality of the human actions and component failures. The criticality can be at, least partly, assessed with the use of "causal factors charting", in which the incident is seen as a succession on events for which an immediate cause, the causal factor, is reported. The idea is then to remove progressively the

causal factors, one after the other, in order to see if it is really necessary to the progression of the incident (Paradies and Bush, 1988). The root cause analysis should be performed only for these necessary factors. This idea, although powerful, has some intrinsic drawbacks since it assumes a sort of linearity in the accident evolution. In particular some factors that seem ineffective for the accident progression may act as a sort of latent failure conditions inducing other failures or other causes of failure.

A rather comprehensive description of the incident evolution can be achieved with the table proposed by Pew et al. (1981) in the frame of a project aiming at the evaluation of nuclear power plants control rooms. The "event time line" proposed by Pew et al. contains the following essential items:

- Information available to the operator and/or stimulus information. This column should report the objective information available to the operator regardless to the use that he has been done.
- Knowledge and/or belief state of the component on which operator's actions were based. This item is the basis for collecting hypothesis and strategies of the operator.
- Decision/actions performed by the operator.
- Sources for Decision/Actions, such as procedures, mental model of the system etc..
- Immediate feedback from the system.

Other items relate to intentions and expectations of the operator.

In our opinion this table constitutes the basic tool to report incident data with the aim to identify human errors and to find their causes. Barrier Analysis concepts can easily be filled in this table as additional information regarding automatic or manual interventions that could have been arrested the accident progression.

The comparison between the available information to the operator and the information actually employed, the belief and expectations, the feedback to the operator, the comparison of the actions performed vs. the procedures and the analysis of the communication constitute the basis for the identification and distinction between human errors and system failures. All these items could be named "diagnosticians" as reported in figure 2.

Causal Analysis

The analysis of the causes of human erroneous actions requires a suitable taxonomy. Different taxonomies have been proposed in order to classify human errors (Cojazzi et al., 1993). From the point of view of accident analysis, once the erroneous actions are identified, the causes must be ascertained. Therefore, a clear distinction between the causes and the manifestations is necessary. The phenotype-genotype taxonomy (Hollnagel, 1991) is founded on this concept. Errors can arise at different levels of cognition, and, once the erroneous actions are identified in terms of manifestations, i. e. as execution failures, the causes of the error can be found at the execution level itself or at inner cognitive categories such as planning, interpretation, etc.. It is clear that a taxonomy aimed at the causal analysis should be based on a model of cognition. The taxonomy proposed by Hollnagel and Cacciabue (1991) has this characteristic, in fact it is developed around the Simple Model of Cognition in which the following categories of operator functions are considered: Perception/Observation, Interpretation, Memory (Knowledge repository), Planning/choice and Action/Execution. The causes of erroneous actions are divided in external (System related causes) and internal (Person related causes). The person related causes have a direct effect on the erroneous behavior, while the system related causes act through the person related causes. Specific internal causes are listed for each of the operator functions of the SMoC. In addition, a set of tables is provided for each of the operator functions of the SMoC and can be used for a) prospective application, passing from error causes to error manifestations and for b)

retrospective application to find the causes of erroneous actions. The table for the execution contains the error manifestations: if a cause is not found at the execution level (in this case the planning should be correct) the analysis can continue at the level of planning. At the planning level, the analysis can stop if causes are found. Otherwise the analysis can go up to the level of perception/observation. In our opinion the structure and the features of this taxonomy fit well the need of a causal analysis of human erroneous actions (Pedrali, 1993). Some work should be done in order to meet the definition of the human erroneous action as deviation from the procedures.

If the source of the erroneous action results to be at the observation level, the cause might be related to the man-machine interface or even to a system failure. In this last case it means that such a system failure could not be identified during the third phase of the RCA framework. This case is represented by the dashed line of figure 2.

CONCLUSIONS

The analysis of the causes of an accident is a very powerful way for improving the safety of a complex installation. In this paper the needs for a root cause analysis of human erroneous actions have been discussed with reference to existing methods and theories. As a result of the discussion, a framework for RCA has been proposed, based on the definition of erroneous actions as deviation from a given procedure and attempting to distinguish, at first, human errors form general system failures. In particular, to represent fruitfully the accidental evolution, the Event Time Line by Pew et al. (19881) can be fruitfully employed. In the same way, the taxonomy proposed by Hollnagel and Cacciabue (1991) results to be quite suitable to perform causal analysis since it is properly constructed upon a cognitive model. It must be remarked that any application of the RCA to specific domains would require a tuning of the above mentioned tools to properly cover the specificity of the context (Hollnagel and Cacciabue, 1994).

Acknowledgments

This work was partially funded by ALENIA (contract No SD-TN-AI-353) in the frame of an ESA contract on Human Dependability. The authors wishes to thank P. Carlo Cacciabue and Mauro Pedrali for the many interesting and fruitful discussions.

REFERENCES

Boeing Commercial Airplane Company, 1985, Statistical summary of commercial jet aircraft accidents, worldwide operations, 1959-1984.

Cojazzi G., 1993, Root Cause Analysis Methodologies. Selection Criteria and Preliminary Evaluation, Commission of the European Communities, Tech. Note No. I.93.93.

Cojazzi, G., Pedrali, M., and Cacciabue, P.C., 1993, Human Performance Study. Paradigms of Human Behaviour and Error Taxonomies, Commission of the European Communities, Internal Report, ISEI/IE 2443/93.

Hollnagel, E., 1991, The phenotype of erroneous actions: implications for HCI design. In G. Weir & Alty (Eds.), "Human-computer interaction and complex systems", 73-12. London: Academic Press.

Hollnagel, E., 1993, "Human Reliability Analysis Context and Control", Academic Press, London.

Hollnagel, E. and Cacciabue P.C., 1991, Cognitive Modelling in System simulation. *Proc. of the Third European Conference on Cognitive Science Approaches to Process Control*, Cardiff, UK, September 2-6, 1991.

Hollnagel, E. and, Cacciabue, P.C., 1994, Reliability of Cognition, Context and Data for a Second Generation HRA, *Probabilistic Safety Assessment and Management II (PSAM-II)*. San Diego, Ca, 24-28 March, 1994.

IAEA, 1991, Asset Guidelines. Revised 1991 Edition. Reference Material Prepared by International Atomic Energy Agency for Assessment of Safety Significant Event Teams. IAEA-TECDOC-632. Vienna.

INPO, 1988, Human Performance Evaluation System. Inst. of Power Operations, INPO 87-007 Rev. 01.

Leplat, J., and Rasmussen, J., 1987, Analysis of human errors in industrial incidents and accidents for improvement of work safety, in Rasmussen et al. ed., "New Technology and Human Error", 1987, J. Wiley.

Lucas, D.A., and Embrey, D.E., 1986, Root Causes of Human Error Independent Failures, Human Reliability Associates.

Paradies, M., 1991, Root cause analysis and human factors. *Human Factors Society Bulletin*, **34**, 8, 1-4.

Paradies, M., and Busch, D., 1988, Root Cause Analysis at Savannah River Plant, *IEEE Record 4-th Conference on Human Factors and Power Plants*, 5-9 June 1988, Monterey, Ca, USA.

Pedrali, M., 1993, Modelli e tassonomie di errori umani per l' analisi di sicurezza nell' aviazione civile. Il caso studio dell' incidente di Zurigo: ricerca delle cause e indagine prospettica. Graduation Thesis in Aeronautical Engineering, Politecnico di Milano, April 1993.

Pew, R.W., Miller, P.C., and Feeher, C.E., 1981, Evaluation of Proposed Control Room Improvements through Analysis of Critical Operators Decision, EPRI-NP 1982, 891.

Rasmussen, J., 1986, "Information Processing and Human-Machine Interaction, an Approach to Cognitive Engineering". North-Holland.

Reason, J. T., 1990, "Human Error". Cambridge, UK: Cambridge University Press.

Svenson, O., 1991, The Accident Evolution and Barrier Function (AEB) Model applied to incident analysis in the processing Industries. *Risk analysis*, **11**, No. 3 499-507.

Swain, A.D., 1976, Sandia Human Factors Program for Weapon Development. Sandia Laboratories Albuquerque New Mexico, SAND 76.0326.

034 Reliability/Availability/Maintainability Improvement

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

Improving the Conditional Probability of the Emergency Feedwater System at Arkansas Nuclear One - Unit 2

D. Johnson, J. Miller, D. Nilius (Entergy); B. Christie (RAPA)

Emergency Diesel Generator Conditional Probability Analysis Arkansas Nuclear One - Unit 2

T. Ivy (Entergy); B. Christie (RAPA)

ESFAS Reliability Analysis to Justify Test Interval Extension

S.H. Levinson, R.S. Enzinna (B&W Nucl. Technol.)

IMPROVING THE CONDITIONAL PROBABILITY OF THE EMERGENCY FEEDWATER SYSTEM AT ARKANSAS NUCLEAR ONE -- UNIT 2

Dwight J. Johnson, Jay Miller, and Dan Nilius

Arkansas Nuclear One
Entergy Operations, Inc.
Rt. 3 Box 137G
Russellville, AR 72801

Bob Christie

Reliability and Performance Associates (RAPA)
P.O. Box 53102
Knoxville, TN 37950-3102

ABSTRACT

Problems with overspeed trips of the Train 'A' Emergency Feedwater (EFW) turbine/pump developed in the latter part of 1988. A program to improve the performance of Train 'A' EFW was initiated under the system engineer and resulted in an improved conditional probability of the Train 'A' EFW turbine/pump responding to a valid demand.

This paper documents the period of time from January 1, 1988 to September 30, 1993 for modes 1, 2, and 3 operation. The conditional probability of Train 'A' responding to a demand has been raised from approximately 87% to approximately 92% (Figure 1). There have been no overspeed trips of the turbine/pump since September 1991.

The Train 'B' motor/pump performance of the EFW system has been exemplary. The conditional probability of Train 'B' has not dropped below 99.7% (Figure 6).

The impact of the variations in the Train 'A' EFW conditional probability on the Unit 2 core damage frequency has been calculated and trended. The month of April 1989 showed the largest variation in the core damage frequency because there were two failures to start due to overspeed trips during the month; one of these failures followed an actual (non-test) demand following a reactor trip.

BACKGROUND

Arkansas Nuclear One is owned by Arkansas Power and Light Co. and operated by Entergy Operations Inc. both of which are part of Entergy Corporation. The facility is a two unit site. Unit 2 is a pressurized water reactor with the NSSS being manufactured by Combustion Engineering. The plant is rated at 912 net megawatts electrical and first went into commercial operation in March of 1980.

The EFW system is a standby system (i.e., it is not normally running during power operation). The EFW system is used when the Main Feedwater system is not operating and the water level in the steam generators drops to a low level automatically activating the EFW system. Manual actuation of the EFW system can also be performed by operators in anticipation of the need for feedwater to maintain steam generator levels.

The EFW system is a two train system. Each train consists of an identical multistage centrifugal pump that can draw water from one of three sources and deliver approximately 485 gpm of water to either of two steam generators through various combinations of valves and piping. Each pump has a different driver type. Train 'A' (2P-7A) is turbine driven. Train 'B' (2P-7B) is motor driven.

IDENTIFICATION OF PROBLEMS

Prior to and during the EFW system performance evaluation period used in this paper, the Train 'A' pump and associated driver (2P-7A/2K-3) routinely evidenced problems associated with start demands. Typically, these problems resulted in mechanical overspeed trips. Repeated attempts to correct the situation via design modifications involving the process logic and hardware associated with the start up portion of the turbine speed controls were nominally successful. However, by late 1988 and continuing into 1991 (included in the period evaluated in this paper) a pattern of repetitive problems concerning overspeed trips had developed.

A failure to start was experienced on Train 'A' EFW on April 5, 1989 during routine surveillance testing to prove operability following maintenance. This was almost immediately followed by a much more serious event on April 18, 1989 when the Train 'A' EFW turbine/pump failed to start on an actual demand. These events and the past operating history lead to close regulator scrutiny of the corrective action plans.

QUANTITATIVE MONITORING PROGRAM

Following a valid demand, the EFW system must start and run for a defined mission time. The model developed to monitor the performance of the system keeps track of three phases of operating history:

1. The EFW system must be in a condition where it is possible to start the equipment (Standby Availability).
2. The Train 'A' turbine/pump and/or the Train 'B' motor/pump must start (Probability of Start).

3. The Train 'A' turbine/pump and/or the Train 'B' motor/pump must run for 24 hours (Probability of Run).

The three phases can be multiplied together to determine the overall conditional probability of success following a valid demand.

Standby Availability

Trending of the Standby Availability of the Trains are shown in Figure 2 for Train 'A' and in Figure 7 for Train 'B'. The trend of the Standby Availability of Train 'A' shows a fairly steady increase in recent years and was 99.8% in September 1993 as measured by a 12 month sliding average. The Standby Availability of Train 'B' was essentially greater than 99.7% for the entire evaluation period.

The Standby Unavailability of Train 'A' can be broken down for forced maintenance and for planned maintenance as seen in Figure 5. The Train 'A' forced Standby Unavailability has been as high as 2.9% for a 12 month period ending in September 1991. The forced Standby Unavailability of Train 'A' has dropped down to 0.06% for the 12 month period ending in September 1993. The Train 'B' forced and planned Unavailabilities have been negligible for the entire evaluation period.

Probability of Start

During modes 1, 2, and 3, from January 1, 1988 to September 30, 1993, there were 310 starts of Train 'A' with 9 failures to start. The nine failures to start were all due to overspeed trips. In order to trend this statistic, a number of different evaluation techniques were used. The most easily understood was the cumulative number of successful starts divided by the number of total starts which provides a cumulative probability of start over the period considered. Additionally, the data was aggregated in 12, 24, and 36 month sliding averages. After consideration of the various trending methods, the most realistic and best estimate seemed to be the use of the cumulative probability of start taken over a 36 month time interval (sliding average). Such a combination provides for a large number of starts in the calculation but also allows old data representing pre-corrective action failures to be eliminated from the results. The trend of the Probability of Start for Train 'A' is shown in Figure 3.

For the same evaluation period and conditions, there were 260 starts of Train 'B' all of which were successful. The probability of start for Train 'B' was taken to be 100% over the entire evaluation period.

Probability of Run

During the 301 successful starts of Train 'A' described previously, 103 hours of run time were accumulated with one failure to run on May 6, 1989. Using statistical techniques from the Arkansas Nuclear One - Unit 2 Probabilistic Risk Assessment (PRA), a failure rate per hour was calculated for each month. A lognormal distribution with a mean value of 4.10E-4 per hour and a variance of 1.03E-6 was used as the prior. These statistical techniques and the values for the prior distribution are under review and may undergo revision in the future. Using this calculated failure rate with a 24 hour mission time as called for in the Unit 2 PRA yields a Probability of Run for each month

for Train 'A'. For example, in January of 1993, the failure rate per hour was calculated to be 2.38E-3 per hour resulting in a Probability of Run of:

$$\text{Probability of Run} = e^{-(2.38\ E\text{-}3)\ (24)} = 0.944$$

The Probability of Run for Train 'A' is shown in Figure 4.

During the 260 successful starts of Train 'B' described previously, 1044 hours of run time were accumulated with no failures to run. Using statistical techniques from the Arkansas Nuclear One - Unit 2 PRA, a failure rate per hour was calculated for each month. A lognormal distribution with a mean value of 2.62E-5 per hour and a variance of 3.87E-10 was used as the prior. Again, these statistical techniques and values for the prior distribution are under review at this time and may undergo revision in the future. Using this calculated failure rate with a 24 hour mission time results in a Probability of Run for each month for Train 'B'. For example, in January 1993 the failure rate per hour was calculated to be 2.58E-5 per hour resulting in a Probability of Run of:

$$\text{Probability of Run} = e^{-(2.58\ E\text{-}5)\ (24)} = 0.999$$

The calculated value of the Probability of Run for Train 'B' was always 0.999 or higher during this time period.

Conditional Probability

The probability of the three phases were multiplied together and the trend for Train 'A' is shown in Figure 1 and the trend for Train 'B' is seen in Figure 6. The minimum conditional probability for Train 'A' is 0.871 calculated for April 1989. The calculated value for Train 'A' in September 1993 is 0.917. The conditional probability of Train 'B' has always been 0.997 or higher.

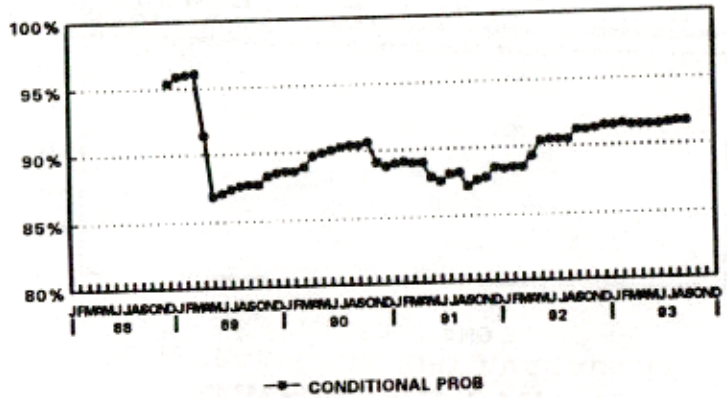
IMPACT ON CORE DAMAGE FREQUENCY

The Emergency Feedwater System is a very important system with respect to the core damage frequency for the Unit 2 Reactor. In fact, the EFW system has the highest Fussell-Vesely importance ranking of any system at ANO Unit 2. The change in core damage frequency resulting from EFW events occurring during the evaluation period can be seen in Figure 8. The core damage frequency values have been normalized in order to show the trend in the values rather than depict the absolute values. The largest core damage frequency change, using monthly values, occurred in April 1989 when the turbine/pump had two overspeed trips out of five demands including an overspeed trip during an actual reactor trip (valid demand). The core damage frequency using the sliding values has been a relatively flat curve.

CONCLUSIONS

The study of the conditional probability of ANO Unit 2 EFW system demonstrates that the corrective actions put in place during the evaluation period (January 1, 1988 - September 1993) have adequately addressed the root cause of degrading Train 'A' performance and maintained excellent performance for Train 'B'.

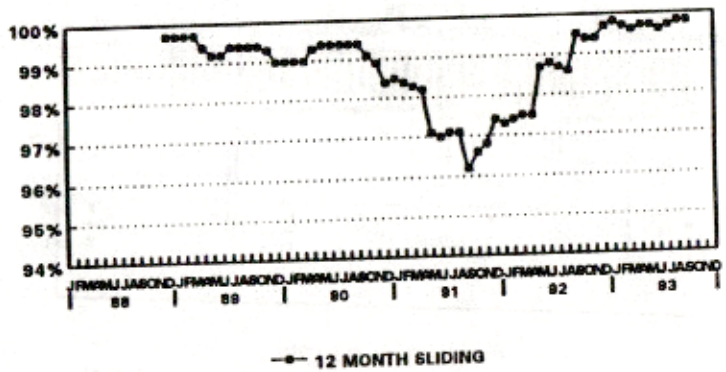
ARKANSAS UNIT 2
EFW TRAIN A CONDITIONAL PROBABILITY



PROBABILITY THAT THE TURBINE/PUMP AUTOMATICALLY STARTS AND RUNS FOR 24 HOURS WITHOUT OPERATOR ACTION

Figure 1

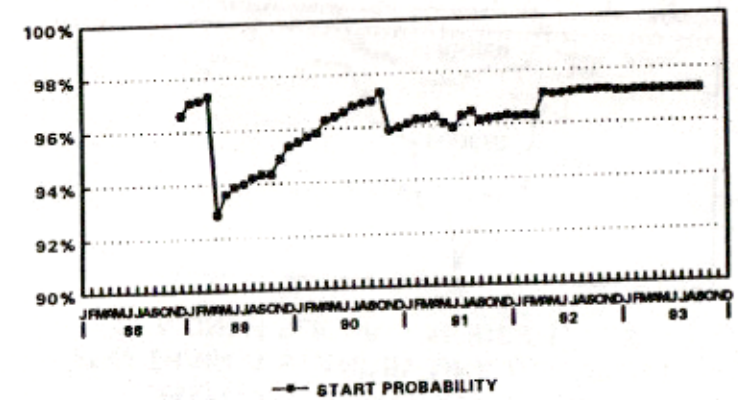
ARKANSAS UNIT 2
EFW TRAIN A STANDBY AVAILABILITY
MODES 1, 2, AND 3



CURVE REPRESENTS THE PROBABILITY OF EFW TRAIN A NOT BEING IN PLANNED OR FORCED MAINTENANCE - 12 MONTH SLIDING

Figure 2

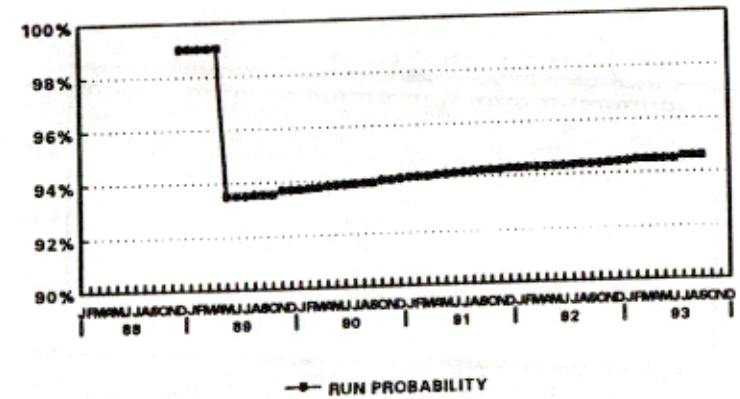
ARKANSAS UNIT 2
EFW TRAIN A START PROBABILITY



PROBABILITY THAT THE TURBINE/PUMP AUTOMATICALLY STARTS WITHOUT OPERATOR ACTION

Figure 3

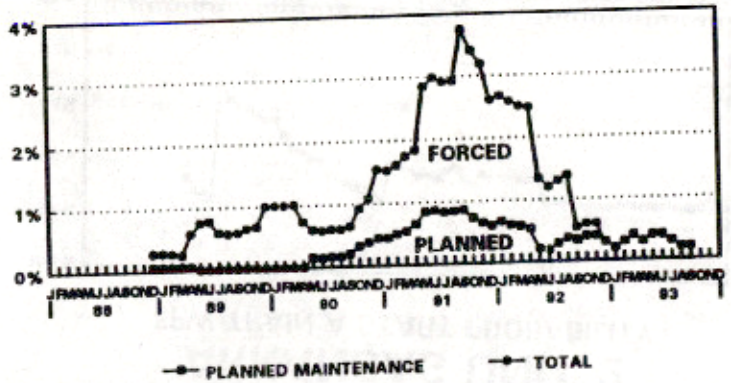
ARKANSAS UNIT 2
EFW TRAIN A RUN PROBABILITY



PROBABILITY THAT THE TURBINE/PUMP RUNS 24 HOURS WITHOUT OPERATOR ACTION

Figure 4

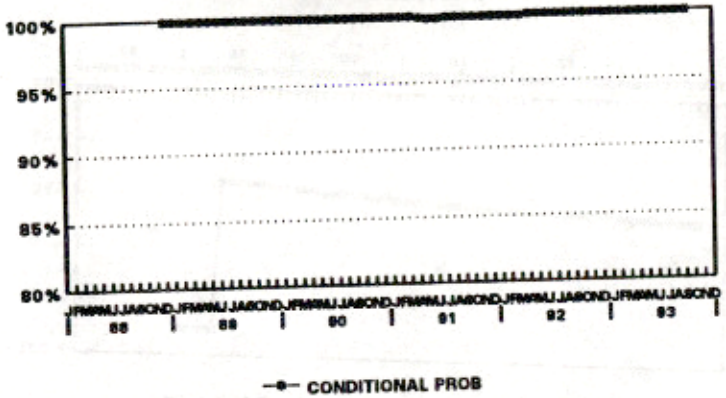
ARKANSAS UNIT 2
EFW TRAIN A STANDBY UNAVAILABILITY
12 MONTH SLIDING - MODES 1, 2, 3



TOTAL INCLUDES PLANNED AND FORCED MAINTENANCE HOURS

Figure 5

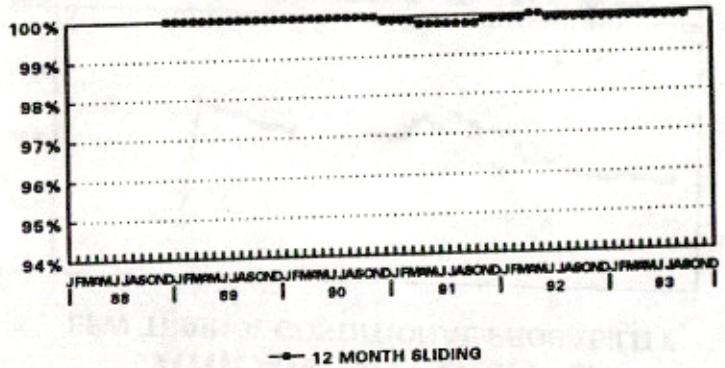
ARKANSAS UNIT 2
EFW TRAIN B CONDITIONAL PROBABILITY



PROBABILITY THAT THE MOTOR/PUMP AUTOMATICALLY STARTS AND RUNS FOR 24 HOURS WITHOUT OPERATOR ACTION

Figure 6

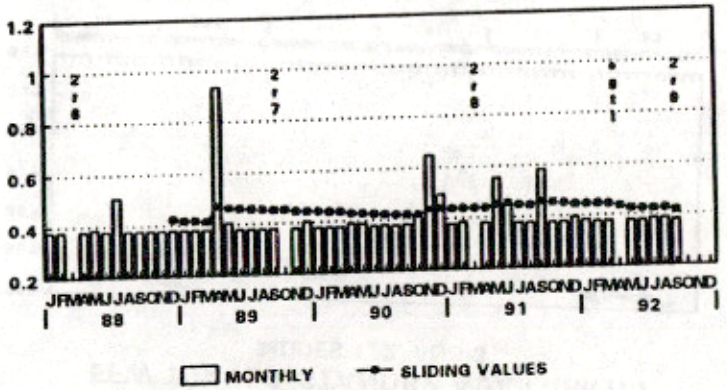
ARKANSAS UNIT 2
EFW TRAIN B STANDBY AVAILABILITY
MODES 1, 2, AND 3



CURVE REPRESENTS THE PROBABILITY OF EFW TRAIN B NOT BEING IN PLANNED OR FORCED MAINTENANCE - 12 MONTH SLIDING

Figure 7

ARKANSAS UNIT 2
NORMALIZED CORE DAMAGE FREQUENCY
MODES 1, 2, AND 3



BASED ON TIME VALUES FOR THE EFW TRAIN A - OTHER VALUES ARE NOMINAL

Figure 8

EMERGENCY DIESEL GENERATOR CONDITIONAL PROBABILITY ANALYSIS

ARKANSAS NUCLEAR ONE - UNIT 2

Ted Ivy, P. E.

System Engineer - Unit 2
Arkansas Nuclear One
Entergy
Russellville, Arkansas 72801

Bob Chrisite

Reliability Consultant
Reliability and Performance Associates (RAPA)
P. O. Box 53102
Knoxville, Tennessee 37950-3102

INTRODUCTION

Over the last few years a program to improve the performance of the Emergency Diesel Generators and to monitor their performance has been instituted at Arkansas Nuclear One - Unit 2. This program was initiated under the system engineer and resulted in an improved conditional probability of the emergency diesel generators responding to a valid demand. Continued improvement in the conditional probability through the use of this analysis is expected

This paper documents the period from January 1, 1988 to April 30, 1993 for Modes 1, 2, and 3. The operating histories of the emergency diesel generators during Modes 4, 5, and 6 are not covered in this analysis. The conditional probability of emergency diesel generator #1 (2K4A) has been raised from approximately 75% to approximately 88% (Figure 1). The conditional probability of emergency diesel generator #2 (2K4B) has been raised from approximately 63% (following the failure to run on January 3, 1989) to approximately 75% (Figure 5). There have been no failures to start or failures to run of the emergency diesel generators since January 1991.

These calculations are used in a monthly update of the Unit 2 core damage frequency as calculated in the Unit 2 Probabilistic Risk Assessment along with values from the Emergency Feedwater System. The impact of the Emergency Diesel Generators on the core damage frequency is not as high an impact as that of the Emergency Feedwater System.

I. BACKGROUND

Arkansas Nuclear One is part of ENTERGY and is located in Russellville, Arkansas. The facility is a two unit site. Unit 2 is a pressurized water reactor with the reactor being manufactured by Combustion Engineering. Unit 2 is rated at 912 net megawatt electric. Unit 2 first went critical in December 1978 and began commercial operation in March 1980.

The Emergency Diesel Generators are standby equipment: i.e., they are not normally running during

power operation. The diesel generators are provided for emergency situations when the voltage on the respective 4.16 kv bus falls below an acceptable level, especially from a loss of offsite power transient.

There are two emergency diesel generators:

Diesel Generator #1 (2K4A) supplies bus 2A3

Diesel Generator #2 (2K4B) supplies bus 2A4

Each diesel generator is separate from the other with its own set of subsystems (jacket cooling water, lubrication oil, fuel oil, etc.). There exists some redundancy in the subsystems for each diesel generator. No attempt was made to model the subsystems for the diesel generators; each diesel generator was treated as a single piece of equipment.

The diesel generator Conditional Probability model was formulated upon the premise that no operator action would be allowed in the calculation of the probability of successful start and load of a diesel generator. The model was based on a 24 hour mission time. This 24 hour mission time comes from the ANO Unit 2 Probabilistic Risk Assessment.

II. QUANTITATIVE MONITORING PROGRAM

Following a loss of voltage to its respective 4.16 kv bus, the diesel generator must start and run. The model keeps track of three phases of diesel generator operating history.

1.) The diesel generator must be in a condition where it is possible to start the diesel (Standby Availability).

2.) The diesel generator must start automatically (Probability of Start).

3.) The diesel generator must run for 24 hours (Probability of Run).

All three phases of operation must be successful in order for the Emergency Diesel Generators to perform their mission. The three phases can be multiplied together to determine the overall conditional probability of success following a valid demand.

A. Standby Availability

No maintenance that would make a Unit 2 diesel generator "inoperable" is routinely scheduled for modes 1, 2, or 3. Therefore, the standby availability of the Unit 2 diesel gener-ators should be 100% if all equipment were "perfect". Consequently all maintenance that makes a diesel generator unavailable during modes 1, 2, or 3 could be considered "forced". However, there was some discretion about the scheduling of certain maintenance tasks during the time period considered and the following rule was used to categorize maintenance. Forced maintenance was defined to be maintenance actually performed within 24 hours of the time the maintenance was initially identified and was performed while the diesel generator was "inoperable" or was performed to keep the diesel generator from being declared "inoperable."

The historical record of the diesel generators from January 1, 1988, through April 30, 1993, for operation in modes 1, 2, and 3 was analyzed to determine the times the diesel generators were in either planned or forced maintenance.

The Standby Availabilities of the diesel generators range from 98% to 100% over the period covered (Figures 2 and 6). Diesel Generator #2 has shown the largest variation in Standby Availability over the time period. At the end of April 1993, each diesel generator was at 99.9%.

Diesel Generator #2 has had substantially more forced maintenance time than Diesel Generator #1. Diesel Generator #1 has had only one forced maintenance occurrence of 3.0 hours on 7/3/90.

B. Probability of Start

During modes 1, 2, and 3 from January 1, 1988 to April 30, 1993, there have been 246 starts of the diesel generators with no failures to start. The breakdown was:

Diesel Generator #1	126 starts	no failures to start.
Diesel Generator #2	120 starts	no failures to start.

All starts except trouble shooting starts following a known problem were considered in the analysis. All

the starts except the start of both diesel generators on December 1, 1988, were test starts or operability starts. On December 1, 1988, both diesel generators started following a reactor trip. Diesel Generator #1 ran for 38 minutes and Diesel Generator #2 ran for 39 minutes before they were secured.

A number of different methods were tried to trend the probability of start of the diesel generators. After consideration of the various methods, it was believed that the best estimate to the probability of start for the diesel generators was a combination of cumulative probability and a 36 month sliding value. Such a combination allows for a large number of starts in the calculation but also allows old failures (if any) to be eliminated from the calculations.

Since there have been no failures to start while in modes 1, 2, and 3, the probability of start of both diesel generators has been 100%. See Figures 3 and 7.

C. Probability of Run

The two diesel generators accumulated 405.5 hours of run time during modes 1, 2, and 3 following the 246 starts considered in the analysis. The breakdown was:

Diesel Generator #1	213.5 hours	zero failures to run.
Diesel Generator #2	192.0 hours	two failures to run.

The two failures to run on Diesel Generator #2 occurred on January 3, 1989 and January 3, 1991. Details concerning the two failures to run are provided below.

January 3, 1989 - Diesel Generator # 2. Following maintenance on breakers for bus 2D24, the diesel was started at 1152 hours and secured at 1331 hours. During the run a gasket on the south exhaust header failed. The gasket failure allowed hot exhaust gases to discharge directly onto the governor. At 30 minutes into the run, the temperature of the south side of the governor was approximately 200 F. The temperature of the top of the governor was approximately 240 F. The temperature on the north side of the governor was greater than 600 F. Conversations with representatives of Woodward Governor Co. indicated operation when temperatures exceeded 180 F were not recommended. Details are provided in Condition Report CR-2-89-0005.

Based on the data taken during the event, a judgment was made that the diesel generator could not have continued to run for 24 hours. The event was considered a failure to run.

January 3, 1991 - Diesel Generator #2. The diesel was started at 0931 hours and secured at 0935 hours due to smoke rising off the air start header and the air start header jumper to the #8 cylinder failing.

The cause of the diesel failure was the spring retaining nut on the air start check valve for the #8 cylinder backing off to the point that it came in contact with the valve operating piston. This mechanical binding of the operating piston caused the check valve to remain slightly open all the time. When the diesel was started, the hot gases from the combustion chamber were forced backwards through the check valve and into the air start header. The resulting heat and pressure caused a soldered connection on the header jumper to the #8 cylinder to fail. Details are provided in Condition Report CR-2-91-0007. The diesel was returned to operation on January 5, 1991.

During the 126 successful starts of 2K4A described above, 213.5 hours of run time were accumulated with no failure to run. Using statistical techniques from the Arkansas Nuclear One Probabilistic Risk Assessment, a failure rate per hour was calculated for each month. A lognormal distribution with a mean value of 0.0147 failures per hour and a variance of 1.22E-4 was used as the prior. These statistical techniques and the values for the prior distribution are under review at this time and may undergo revision in the future. Using this calculated failure rate with a 24 hour mission time as called for in the Unit 2 Probabilistic Risk Assessment results in a Probability of Run for each month for 2K4A. For example: In April 1993, the failure rate per hour was calculated to be 5.31E-3 resulting in a Probability of Run of

$$\text{Probability} = e^{-(\text{failure rate})(\text{mission time})}$$

$$\text{Probability} = e^{-(.00531)(24)} = 0.88$$

During the 120 successful starts of 2K4B described above, 192 hours of run time were accumulated with

two failures to run. Using the same statistical techniques from the Arkansas Nuclear One Probabilistic Risk Assessment, a failure rate per hour was calculated for each month. For example: In April 1993, the failure rate per hour was calculated to be 1.21E-2 resulting in a Probability of Run of

$$\text{Probability} = e^{-(.0121)(24)} = 0.75$$

See Figures 4 and 8 for the trend of Probability of Run.

D. Conditional Probability

The probabilities from the three phases were multiplied together and trended in Figures 1 and 5. In April 1993, Diesel Generator #1 has a Conditional Probability value of approximately 88%. Diesel Generator #2 has a value of approximately 75%. The most important component of the Conditional Probability is the Probability of Run.

III. SUMMARY

A. Problems

An examination of the operating history of the diesel generators indicates a wide variety of problems. No one subsystem or component dominates the failure history of the diesel generators.

Diesel Generator #2 has had substantially more forced outage hours than diesel generator #1. Diesel Generator #2 also has had two failures to run, while Diesel Generator #1 has had no failures to run. In general Diesel Generator #1 is the more reliable diesel and this shows up in the calculation of the conditional probabilities of the respective diesel generator.

Both diesel generators have had problems with the air start compressors. These problems do not show up in the maintenance outage hours or the probability of start calculations for the diesels because of the use of the air receiver tanks and the redundancy of the air start compressors.

No problem appears to be reoccurring with either diesel generator during the last year.

B. Trends

The overall performance of the diesel generators is trended in Figures 1 and 5. The absolute value of the Conditional Probability is dominated by the Probability of Run of each respective diesel generator.

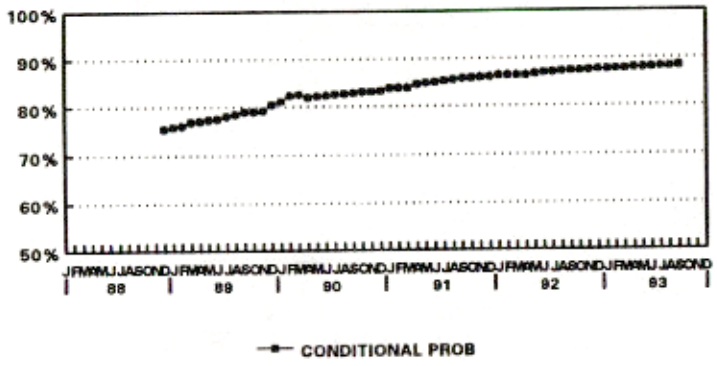
The Standby Availability of each diesel generator has reached essentially 100% over the past year. That is, little or no maintenance (either planned or forced) is being performed on the diesel generators during modes 1, 2, or 3 that makes the diesel generators unavailable for an automatic start, given a valid demand.

It has been almost two years since the last failure to run of a diesel generator. Consideration is being given to adopting a three year sliding value for the Probability of Run rather than using a cumulative value since January 1, 1988.

C. Uses

The calculations described in this paper are being used to monitor the performance of the emergency diesel generators. These calculations are also used in a monthly update of the Unit 2 core damage frequency as defined in the Unit 2 Probabilistic Risk Assessment.

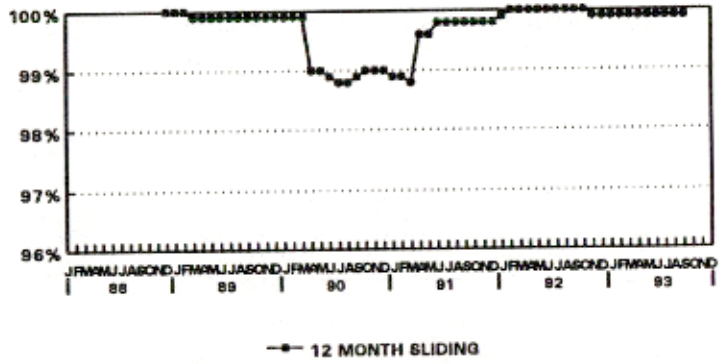
ARKANSAS UNIT 2
2K4A/DG1 CONDITIONAL PROBABILITY
MODES 1, 2, AND 3



PROBABILITY THAT DIESEL GENERATOR 1 AUTOMATICALLY STARTS AND RUNS FOR 24 HOURS WITHOUT OPERATOR ACTION

Figure 1

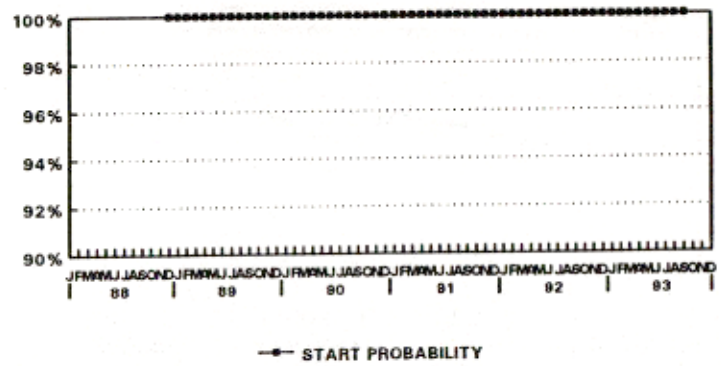
ARKANSAS UNIT 2
2K4A/DG1 STANDBY AVAILABILITY
MODES 1, 2, AND 3



CURVE REPRESENTS THE PROBABILITY OF 2K4A/DG1 NOT BEING IN PLANNED OR FORCED MAINTENANCE - 12 MONTH SLIDING

Figure 2

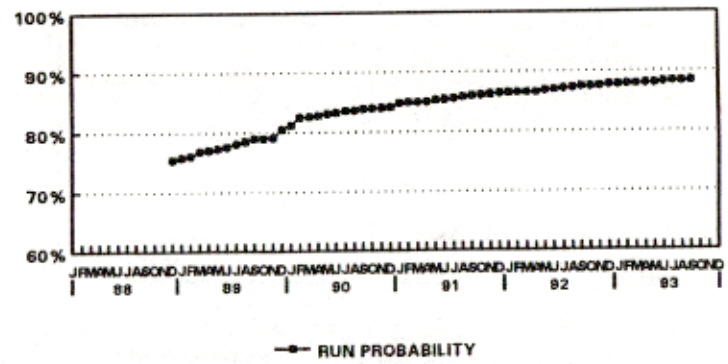
ARKANSAS UNIT 2
2K4A/DG1 START PROBABILITY
MODES 1, 2, AND 3



PROBABILITY THAT DIESEL GENERATOR 1 AUTOMATICALLY STARTS WITHOUT OPERATOR ACTION

Figure 3

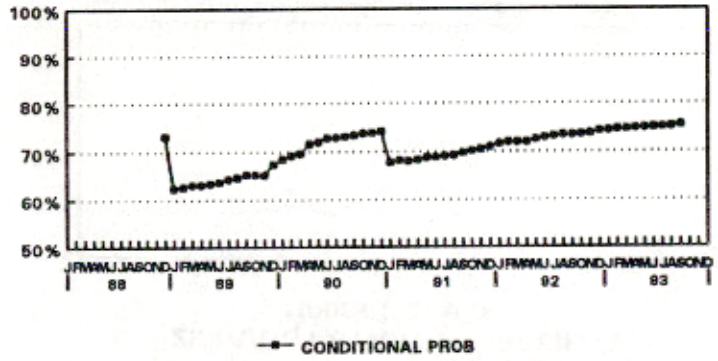
ARKANSAS UNIT 2
2K4A/DG1 RUN PROBABILITY
MODES 1, 2, AND 3



PROBABILITY THAT DIESEL GENERATOR 1 RUNS 24 HOURS WITHOUT OPERATOR ACTION

Figure 4

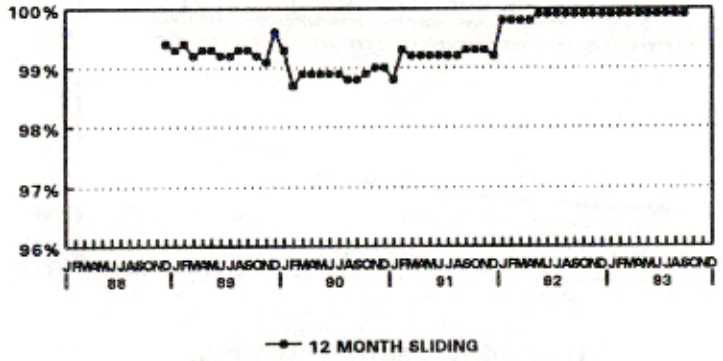
ARKANSAS UNIT 2
2K4B/DG2 CONDITIONAL PROBABILITY
MODES 1, 2, AND 3



PROBABILITY THAT DIESEL GENERATOR 2 AUTOMATICALLY STARTS AND RUNS FOR 24 HOURS WITHOUT OPERATOR ACTION

Figure 5

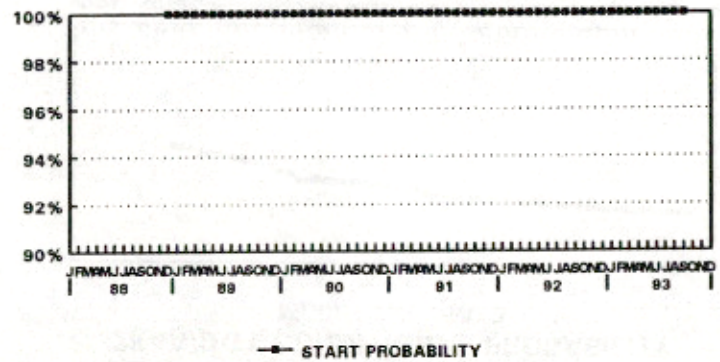
ARKANSAS UNIT 2
2K4B/DG2 STANDBY AVAILABILITY
MODES 1, 2, AND 3



CURVE REPRESENTS THE PROBABILITY OF 2K4B/DG2 NOT BEING IN PLANNED OR FORCED MAINTENANCE - 12 MONTH SLIDING

Figure 6

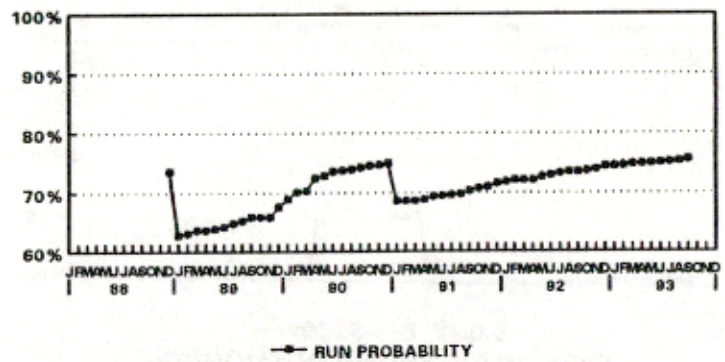
ARKANSAS UNIT 2
2K4B/DG2 START PROBABILITY
MODES 1, 2, AND 3



PROBABILITY THAT DIESEL GENERATOR 2 AUTOMATICALLY STARTS WITHOUT OPERATOR ACTION

Figure 7

ARKANSAS UNIT 2
2K4B/DG2 RUN PROBABILITY
MODES 1, 2, AND 3



PROBABILITY THAT DIESEL GENERATOR 2 RUNS 24 HOURS WITHOUT OPERATOR ACTION

Figure 8

ESFAS RELIABILITY ANALYSIS TO JUSTIFY TEST INTERVAL EXTENSION

Stanley H. Levinson and Robert S. Enzinna

B&W Nuclear Technologies
P.O. Box 10935
Lynchburg, Virginia 24506-0935

ABSTRACT

An analysis was performed to provide a technical basis to justify increasing the Engineered Safety Features Actuation System (ESFAS) on-line test intervals from one month to three months for three ESFAS designs. The methodology used is based on reliability block diagrams (RBDs) and contains the features that are important to the Nuclear Regulatory Commission for technical specification submittals, including: time-dependent modeling, emphasis on operating experience data, inclusion of common mode failures (mechanical and human-caused), and uncertainty analysis. Time-dependent results were integrated to obtain the average core melt risk due to ESFAS failure for both one-month and three-month test intervals, as well as the incremental difference in core melt frequency attributable to increasing the test interval from one to three months. The estimated mean incremental risk associated with extending the test interval to three months varied from 1.45×10^{-7} to 2.03×10^{-8} per reactor-year. The uncertainty analysis showed that, even with an order of magnitude uncertainty in the data, the incremental risk from extending the ESFAS test interval to three months is small.

INTRODUCTION/SCOPE

An analysis was performed to provide a technical basis to justify increasing the Engineered Safety Features Actuation System (ESFAS) on-line test intervals from one month to three months for three ESFAS designs. Extensions for actuated Engineered Safeguards (ES) devices, such as pumps and valves, were not investigated.

The investigation performed was generic and applicable to plants that have Babcock & Wilcox (B&W) Nuclear Steam Systems (NSSs). To account for three significantly different ESFAS design configurations, three separate models were developed. Although there are some differences in implementation, all of the ESFAS designs have three or four redundant analog subsystems that monitor pertinent plant parameters, generally reactor coolant (RC) and reactor building (RB) pressure, to actuate Engineered Safeguards (ES) devices that loosely translate into four functional groups: high pressure injection (HPI), low pressure injection (LPI), RB isolation and cooling, and RB spray. All three designs have two redundant actuation subsystems (i.e.,

digital subsystems) arranged in a one-out-of-two logic that is implemented by actuating one train of ES devices off of each ESFAS actuation subsystem.

METHODOLOGY/MODELS USED FOR EVALUATION

The methodology used to evaluate the test intervals for the ESFAS is the same as used for the B&WOG submittal on Reactor Trip System (RTS) test interval extension[1]. The methodology is based upon reliability block diagrams (RBDs) and contains the features that are important for technical specification submittals, including: time-dependent modeling, emphasis on operating experience data. inclusion of common mode failure and human error, and uncertainty analysis.

The RTS reliability and risk significance was evaluated for a representative (and bounding) event, namely, loss of feedwater. It also explicitly excluded manual recovery action (i.e., manual reactor trip) because it was considered a constant over all events and would unnecessarily complicate and mask the results. However, in the ESFAS analysis, it was not possible to choose a representative event because ESFAS actuates a wider selection of equipment than RTS. Therefore, ESFAS reliability was examined for a spectrum of different Loss of Coolant Accident (LOCA) events, each of which challenges different ESFAS parameters and requires different ESFAS response. Failure of ESFAS to respond by actuating the appropriate devices, in itself, does not disable the ES function(s), because the devices can be actuated manually independent of ESFAS. ESFAS has more functions than RTS. and the time available for appropriate operator recovery action is not constant over all ESFAS functions (e.g., failure of ESFAS to actuate HPI requires more urgent operator action than failure of ESFAS to actuate RB cooling). Thus, it was necessary to include ESFAS challenge rates and recovery through manual ES actuation to place the various event scenarios that challenge ESFAS, and the respective ESFAS failure modes, into common perspective with respect to impact on (core melt) risk.

The ESFAS analysis includes a common mode failure contribution for all components within the ESFAS system, even when the failure data did not support development of a rate. In the cases where common mode failure rates could not be obtained from the failure history, subjective (and conservative) β-factors were assigned.

For test-revealed failures, time-to-repair data could be obtained from historically-derived mean-time-to-repair (MTTR) data rather than technical specification-dictated allowed outage time (AOT) or ACTION times. The ESFAS analysis assumed that the system reliability will continue to be vulnerable to a test-revealed failure for the full length of the AOT/ACTION time dictated by technical specifications, even though the actual repair time may be shorter. Thus, the times used in the model are the full time allowed by technical specifications, from detection of the failure until the component or channel is in a "safe" state (generally tripped) or the reactor is shutdown to a "safe" state (i.e., a mode where the affected ESFAS function is no longer needed).

Reliability Block Diagram Modeling

The RBDs model each sensed parameter of the ESFAS trips. These include RC pressure (for low and low-low trips), and RB pressure (for high and high-high trips). In addition, some ESFAS designs include high RB radiation and low borated water storage tank (BWST) level trips. The RBD is arranged so that individual parameters or combinations of parameters can be called upon for evaluation of ESFAS response to a selected challenging event. The top logic of the RBDs reflect dependencies that are a function of ES equipment assignment to channels. Quantification runs were tailored to specific challenging events by detaching unchallenged or inapplicable functions. For example, for an interfacing systems LOCA, high RB pressure will not be challenged -- therefore, when evaluating that case, the unchallenged RB pressure parameter was analytically detached from the RBD.

The level of detail of the RBD basic events was chosen to correspond with the level of resolution of the data, with preference given to data derived from operating experience. For example, random and common mode failure data for instrumentation assemblies from NUREG/CR-3289[2] is available at the "sensor" and "signal conditioning system" level of resolution.

Common mode failures are treated explicitly in the RBDs. Dependent basic events are shown involving two or more redundant components. All RBD basic events involving ESFAS components have corresponding common mode failure basic events associated with them and their redundant counterparts. Human errors are not explicitly shown on the RBDs. Errors introduced during maintenance and test activities are incorporated into the common mode failure (and random) events, due to the difficulty in separating the human element from the common mode failure. In the interest of using operating experience data wherever possible, the human element and common mode failure contribution are integrated. The preference of operating-experience-based rather than theoretically-based estimates of human error probabilities provides more meaningful results.

The RBD model was constructed with the flexibility to examine alternative test intervals for the ESFAS analog and digital subsystems, and account for changes in the ESFAS configuration due to testing. All component failures that are not in the fail-safe mode contribute to system unavailability (i.e., to trip on demand) until they are detected (usually through testing). Some components are tripped either for testing or subsequent repairs and therefore do not contribute to system unavailability while they are in the safe state. Other components contribute to system unavailability because redundancy is reduced while they are bypassed during testing. Components that are not tripped upon detection of failure contribute to system unavailability further while they are inoperable awaiting repair or reactor shutdown.

The calculations performed are time-dependent. For example, the time-dependent availability is calculated as a system changes from 2-out-of-4 logic to 2-out-of-3 logic for the test, and back to 2-out-of-4 logic as the channel is returned to service, showing the effect of channel bypass during testing. Other time-dependent effects become evident using time-dependent analysis, e.g., after each test, there is a step improvement in system unavailability as the tested components are verified to be free of undetected failures. The time-dependent model confirms that temporary changes in system configuration do not result in brief periods of extremely poor reliability. This type of modeling is important when trying to demonstrate the effect of technical specification revisions.

Determining Risk Significance of ESFAS Reliability

Since the purpose of the analysis is to examine the risk-impact of ESFAS test intervals, it is necessary to isolate the impact of ES actuation failure on that risk. The method used was to build an ESFAS RBD model, and then modify it with generic challenge rates and recovery probabilities, for a spectrum of events. Assuming that the consequence of non-recovery is core melt, the result is the ESFAS contribution to core melt frequency.

Since ESFAS is a multi-functioned system that is designed to respond to a variety of postulated LOCA events, it was necessary to align the RBD model functionally to different challenging events. Each event has a different impact on ESFAS, with respect to parameters that are challenged and ESFAS functions that need to respond. In addition, for a given event, some ES functions (e.g., actuation of long-term RB cooling) have less urgency than others (e.g., actuation of HP safety injection); consequently, their actuation failures have different risk significance. These issues were addressed for each event that could challenge ESFAS and incorporated into the model to produce an "aggregate" ESFAS-induced risk model.

The risk analysis built upon the RBD model, with RBDs being generated to represent all ESFAS functions at each plant. Then the models were run for the specific events from the

spectrum of LOCAs and challenged ESFAS parameters. Given a specific ESFAS challenge scenario, the risk significance was addressed as a function of the ESFAS challenge rate and the consequence of non-recovery of ES actuation for that scenario. Thus, a perspective was given to the relative importance of various events and ESFAS functions.

SOURCES OF DATA FOR THE RELIABILITY EVALUATION

Emphasis was placed on the use of operating experience in the derivation of random and common mode failure rates. All failure rates were derived either directly or indirectly from experience collected in the Nuclear Plant Reliability Data System (NPRDS) and Licensee Event Reports (LERs) data bases.

For the digital subsystem components, such as the various logic modules and/or relays used in the ESFAS designs, B&WOG experience from the NPRDS data base (available through INPO) was used. Operating experience (including mechanical- and human-caused failures) was reviewed to quantify failure rates for digital subsystem components, including logic modules. Failure rates were obtained from the operating experience data for the ten years ending January, 1990.

NUREG/CR-3289[2] was used to develop the common mode and random failure rates for the analog channels. This includes the sensors and instrumentation strings, including signal conditioning components up to and including the bistables. The data base used in NUREG/CR-3289 coalesces industry-wide operating experience obtained from LERs.

The historical data bases largely represent components that have been tested monthly. As long as the modeled test frequency is monthly, a reliability analysis that assumes per-demand rates will yield the same results as one that assumes per-hour rates. This assumption is not true if the data is extrapolated to longer-than-one-month test intervals. Obviously, if failure rates are expressed per-demand, the component's probability of failure for a given challenge will remain constant regardless of how the test interval is varied. This would be optimistic and misleading. However, if failure rates are expressed per-hour, the component's probability of failure for a given challenge will be a function of the time elapsed since the last test, and would increase proportionally as the test interval increases. This would be pessimistic and may overestimate the sensitivity to test interval. An ideal model would separate the historical failure experience into cyclic and time-related contributions, and split the failure rates into per-demand and per-hour contributions.

The failure records supporting NUREG/CR-3289 (LERs) and NPRDS were not sufficient to meaningfully discriminate between time-related and cyclic failure mechanisms. The failure rate data used in this analysis were obtained from NUREG/CR-3289 and NPRDS, and are reported in terms of failures-per-hour. They are, therefore, conservative for examining ESFAS sensitivity to test interval. This conservatism applies to the human errors as well as mechanical failure modes that have cycle-dependent rather than time-in-service dependent failure mechanisms.

The ESFAS reliability models, in addition to failure rates, require data for time-to-repair of test-revealed failures. The time-to-repair is a function of the time taken-to-discover the failure. For test-revealed failures, this is a function of the surveillance test interval (STI). Both the existing one-month test intervals and the proposed three-month test intervals were used in the analysis to determine the sensitivity of ESFAS reliability to the STI. However, not all failures are test-revealed. Thus, unless the failure is catastrophic (in which case it will be detected at the shiftly channel check), it may not be apparent until the next refueling outage or an actual ESFAS demand. This was assumed to be the case for "reduced capability faults" of sensors. Due to the longer exposure time (i.e., the time that the failure is likely to go undetected), the degraded failure modes ("reduced capacity faults") dominate sensor unavailability.

Challenging event frequencies were obtained from a combination of B&WOG experience, and a B&W nuclear plant Probabilistic Risk Assessment (PRA). Conventional LOCA frequencies were obtained from the PRA, which were obtained from industry operating experience. Transient-induced LOCA frequencies were obtained from B&WOG operating experience. LOCAs induced from LOOP events, with and without coincident emergency diesel generator (EDG) failure, were included by combining B&WOG operating experience with generic EDG failure probabilities. The interfacing-systems LOCA frequency was extrapolated from a representative plant because the B&W NSS designs are similar and because ESFAS is not a significance risk contributor for interfacing systems LOCA. The potential interfacing systems LOCA pathways identified in the PRA were reviewed to determine which ones contained ESFAS-actuated isolation valves. The frequency was re-calculated by omitting credit for the ESFAS actuation in determining the significant pathways and the ESFAS challenge rate.

Given ESFAS failure, the time available to avert core damage depends on the severity of the LOCA and the ESFAS function that has failed. Estimates were made of the minimum time available for manual initiation of ES devices that have failed to actuate. Extrapolating from available accident analyses, conservative times were assumed for diagnosis and action to avert core melt given the specific event and failed ESFAS function. Operator recovery from ESFAS actuation failure requires both cognitive (diagnostic) and action tasks. The operator can initiate all of the ES equipment (independent of ESFAS) from the main control panel. Operator error probabilities for operating these controls were obtained from NUREG/CR-1278[3]. The diagnostic (cognitive) error probabilities were obtained from NUREG/CR-4834[4], which contains time-reliability correlations based on simulator experiments. Recovery times longer than an hour were not assigned (although in some cases, they may have been justified) because the failure probability for recovery times greater than one hour were equivalent to recovery times of one hour.

MODEL QUANTIFICATION/RESULTS

The quantification for each test interval included making separate runs for each of the three ESFAS designs for each challenging event, as well as an aggregate run where all the challenging events were accounted for in a single Boolean expression. The base cases, using the current one-month test interval, were quantified using best estimate (mean) failure rate data to determine the time-dependent and time-averaged core melt risk due to ESFAS failure. The one-month analyses were repeated using a three-month test interval to quantify the effect of extending the test interval. For the latter cases, the test interval for all of the ESFAS components was changed from one to three months, except for components outside the ESFAS system boundary, such as external power supplies.

Time-dependent plots were used to examine the dynamic effects of the STIs. They substantiate the validity of the RBDs, as well as the time-averaged results derived from integrating the time-dependent results. Most importantly, the time-dependent plots were used to confirm that temporary changes in system configuration do not result in brief periods of extremely poor reliability (i.e., risk vulnerabilities) that might result from changing test intervals (that may have been hidden if averaged over a month or a year).

The calculated mean contribution of ESFAS to core melt frequency (with one-month STI) ranges from 2.11×10^{-8} per reactor-year to 5.26×10^{-7} per reactor-year for the ESFAS designs analyzed. In this analysis, the risk of core melt due to ESFAS failure with a three-month test interval ranges from 4.1×10^{-8} per reactor-year to 6.1×10^{-7} per reactor-year. As a check, some previous PRA-based studies were examined to determine their consensus on the contribution of ESFAS to risk, and to see if the risk-significance compared favorably with the ESFAS risk significance calculated in this study. This compares favorably with the results expected in PRA studies for ESFAS contribution to core melt frequency.

The mean incremental core melt frequency associated with the extension of the STI from one to three months ranges from 2.03×10^{-8} per reactor-year to 1.45×10^{-7} per reactor-year. Thus, the impact of increasing the ESFAS test interval from one to three months is small; accordingly, the test interval extension is justified in light of the negligible increase in the overall core melt frequency. In addition, the time-dependent analysis shows that the change of STI from one to three months does not significantly change the conditional risk (i.e., vulnerability) due to testing.

UNCERTAINTY ANALYSIS AND RESULTS

For each of the three ESFAS designs, uncertainty analysis was performed on the time-averaged results. The purpose of the uncertainty analysis was to quantify the effect (on risk) of the uncertainty of the failure rate data as the ESFAS test interval was increased from one month to three months. The Boolean expressions derived from the RBDs were also used as input to the SAMPLE Monte Carlo code.

The point-estimate value and 95%/95% values of the incremental risk of core melt due to an increased ESFAS test interval were determined for each of the three ESFAS designs, and each of the challenging events and the challenging event aggregate. The mean incremental core melt frequencies calculated by SAMPLE agree with the mean incremental core melt frequencies calculated by integration of the time-dependent plots. The relative closeness of the means and 95%/95% values (upper bound) shows the robustness of the best estimate incremental risk even with considering an order of magnitude variation in all the basic event failure data.

The uncertainty analysis shows 95%/95% values for the incremental risk of core melt due to the extension of the STI from one month to three months to range between 9.57×10^{-8} per reactor-year to 4.94×10^{-7} per reactor-year. The small magnitude of the upper bounds reinforces the robustness of the conclusion that increasing the ESFAS test interval to three months does not significantly impact risk.

REFERENCES

1. "Optimization of Reactor Trip System Test Intervals", 1984 INTER-RAM Reliability Conference for the Electric Power Industry, Las Vegas, Nevada, April 1984. Reprinted in Nuclear Engineering International, September 1985.

2. T. R. Meachum and C. L. Atwood, Common Cause Fault Rates for Instrumentation and Control Assemblies, Estimates Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants, 1976-1981, prepared for the U.S. Nuclear Regulatory Commission by the Idaho National Engineering Laboratory (INEL), EGG-2258, NUREG/CR-3289, May 1983.

3. A. D. Swain and H. E. Guttman, Handbook of Human-Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Final Report, prepared for the U.S. Nuclear Regulatory Commission by Sandia National Laboratories, Albuquerque, New Mexico, SAND80-0200, NUREG/CR-1278, August 1983.

4. L. M. Weston, D. W. Whitehead, and N. L. Graves, Recovery Actions in PRA for the Risk Methods Integration and Evaluation Program (RMIEP), Volume 1: Development of the Data-Based Method, prepared for the U.S. Nuclear Regulatory Commission by Sandia National Lab., Albuquerque, New Mexico, SAND87-0179, NUREG/CR-4834/1 of 2, June 1987.

035 Regulation and Legal Issues

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

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

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

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

RELIABILITY CERTIFICATION OF ELECTRONIC SYSTEMS USED FOR PROTECTION

Paraskevas A. Stavrianidis[1], Dimitrios M. Karydas[1]

[1]Factory Mutual Research Corporation
1151 Boston-Providence Turnpike
Norwood, MA 02062

ABSTRACT

The petro-chemical industry today is relying on sophisticated electronic systems to perform many of the safety functions. The reliability of these systems, and their contribution to the achievement of process safety needs to be evaluated. This paper presents a methodology that can: a) evaluate the potential risks associated with an industrial process; b) identify existing safety systems and their contribution to process risk reduction; and c) propose new safety systems and evaluate their ability to reduce existing risks to an acceptable level. The methodology is applied to a chemical process which employs a programmable electronic system as one of the safety layers.

INTRODUCTION

Industry is continuously asked to produce a "high" quality product in a cost effective and efficient way under more stringent safety guidelines from industry sponsored organizations (ISA, 1993; IEC, 1993; CCPS, 1992), government agencies that have jurisdiction (OSHA, 1992) and the insurance industry. The primary focus of these guidelines/rules is to define an overall framework that allows the systematic identification and evaluation of risks and the development of risk reduction methodologies based on sound engineering principles. Plant management needs to have guidelines in place that may be used to define the plant or process "acceptable" risk level and the likelihood of safety system failure. Only then will they be able to make objective risk management decisions

based on risk and, the ability of a safety system or layers of safety systems to reduce that risk to an acceptable level.

The need to evaluate the safety of processes is being dictated by new government standards (OSHA, 1992). Industry sponsored organizations (ISA, 1993 and IEC, 1993), are developing standards and guidelines that identify safety system reliability or integrity levels. According to theses documents, safety systems must comply with or exceed the safety integrity level for a specific application. A methodology is proposed that employs risk analysis and reliability techniques to achieve three objectives: a) identify the total risk associated with a process using a "process safety lifecycle model"; b) identify all safety systems and the contribution of each system to the reduction of risk using a "Safety layer model" and; c) evaluate the performance of specific safety systems using system reliability analysis techniques so as to meet design and safety criteria.

The methodology is exercised on a specific system to emphasize the need to evaluate and certify the reliability of systems used for safety and evaluate their contribution to the total process risk reduction. In recent years, most of the process control and safety functions in the chemical industry are being performed by sophisticated micro-processor based systems either as independent units or in layers of control and safety systems. These systems allow the users to quickly identify and repair failed components or systems and to implement more extensive control or safety logic. They are often looked at as "black boxes" with very little information about their performance and reliability. As a result, their ability to function either as an independent safety system or as an intricate part of a safety system assembly that incorporates several independent safety layers is rarely investigated. These safety systems must be examined and their performance should be evaluated both as independent safety systems and as part of an assembly of safety systems.

PROCESS SAFETY LIFECYCLE MODEL

The lifecycle model given in Figure 1 is a modified version of the model given by ISA (1993). It focuses on an existing process with safety systems and examines the need of an additional safety layer which will be provided by a programmable electronic system (PES). The methodology to evaluate the performance of the PES is given in Figure 2. The lifecycle model is applicable to any process and covers the process from hazard assessment to the design, testing, installation, operation and final decommisioning of the process. This paper focuses on five specific areas: a) assessment of existing risks through formal quantitative risk analysis; b) contribution of all existing safety systems to overall process risk reduction through the use of accident sequence modeling; c) evaluation of the need for an additional safety system; d) reliability certification of proposed safety system; and e) process risk reduction due to a new safety system.

QUANTITATIVE RISK ASSESSMENT

The first step in an attempt to identify and quantify the risks associated with a process or industrial plant is to perform a Quantitative Risk Assessment (QRA). QRAs play an important role in risk analysis and risk management during the design, testing and operational phases of a process. The procedure identifies, quantifies and ranks the risks associated with specific process hazards and examines the adherence of the process design and operation to safety criteria and standards established by corporate policy, the industry and government agencies.

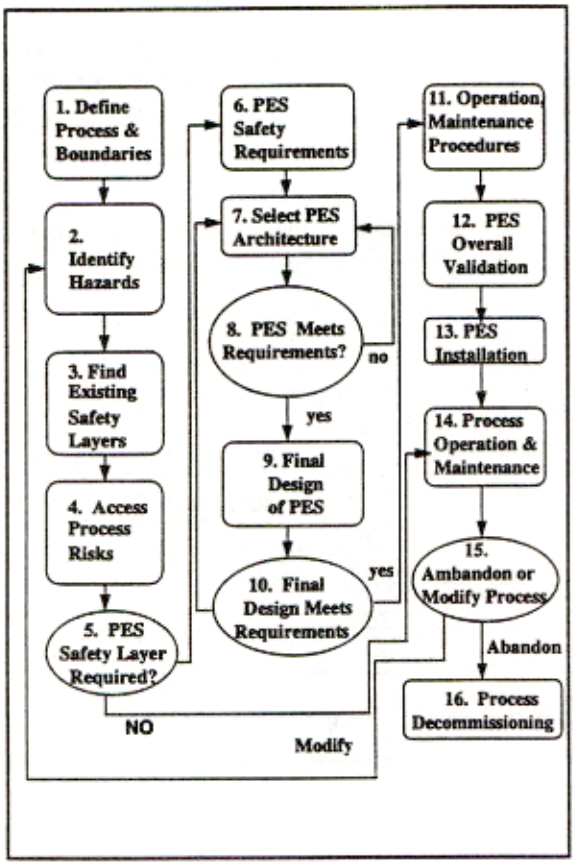


Figure 1. Process Safety Lifecycle Model

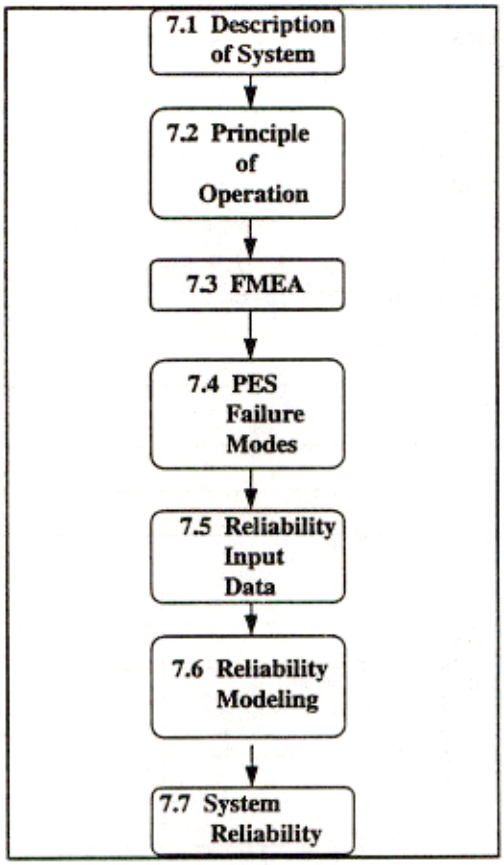


Figure 2. Select a PES Architecture

In Figure 1, stages one, two, three and four are the essential elements of a QRA. Specifically, the methodology and the procedures can be distinguished in the following seven major steps which are developed and discussed in detail in Contini (1992).

1. Hazard Identification using Hazards and Operability Analysis (HAZOP) or other suitable techniques to identify hazards of the process (i.e., initiating events) and classify existing safety systems.
2. Accident Sequence Modeling using Event Tree Analysis to develop accident scenarios for every initiating event.
3. Component/system performance data acquisition.
4. Fault tree analysis to determine the probability of occurrence of the initiating events and the reliability of safety systems.
5. Quantification and grouping of like accident scenarios using results from above steps.
6. Evaluation of the consequences of all accident scenarios.
7. Integration of the results (consequence and probability of an accident) into risk profiles.

Three outcomes of interest are produced from the above exercise. Namely, a better understanding of the process and therefore of the risks associated with it, the risk profile for the process and the contribution of existing safety systems to the overall risk reduction or conversely, safety level of the process.

The QRA methodology was exercised on a specific facility that uses a flammable gas, (Cranefield et al., 1993). Figure 3, solid line, provides the risk profile for the facility developed to graphically represent the overall risk associated with the process. All safety systems and their contribution to process risk reduction have been identified. Corporate and plant management must access whether or not the process complies with all safety criteria.

These are criteria established by relevant codes, standards and regulations, as well as safety goals set by corporate policy and insurance industry recommendations. An "acceptable risk level" is established by corporate or plant management through policy and engineering practice, past experience and use of standards and codes. If the risk is within acceptable limits, the existing safety systems (i.e. safety layer) are adequate and the process operates under existing operation and maintenance principles, (Figure 1, stage 14). If the risk is not acceptable, then a new safety system is added to the safety layer to either protect: a) the overall process; or b) a portion of the process judged to be a major contributor to the unacceptable risk level.

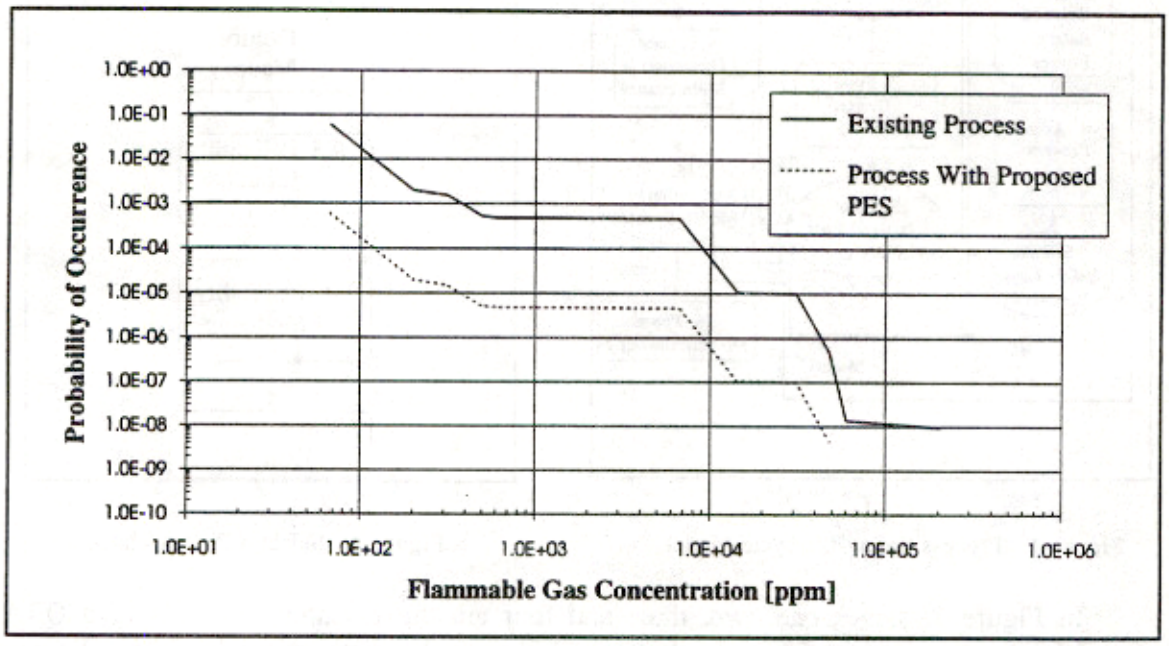


Figure 3. Risk Profile for Manufacturing Facility

SAFETY LAYER MODEL

The process QRA (Cranefield et al., 1993) identified the following existing safety systems: automatic detection and interlock systems, automatic sprinkler systems, and pressure relief valves. The safety layer concept shown in Figure 4, (ISA 1993), is applicable to this process. Not all of the existing safety systems will necessarily respond to a process disturbance. Often times, parts of the process rely on a sub-set of the safety layer for protection. The results of the accident sequence modeling allow the analyst to clearly identify initiating events, the safety systems available to respond, and the contribution to risk reduction from these safety systems.

Assuming that the risk profile shown in Figure 3 is not acceptable, management can either improve the reliability of existing safety systems in order to reach the desired process safety level or introduce a new safety layer (system). In either case, management must also consider the cost and benefits associated with either decision. This analysis assumes that management decided to introduce a new safety layer using a PES. The safety performance requirement(s) for the PES are established so that the new safety system reduces the overall process/facility risk to below the acceptable level. In other words, the PES probability of failure to respond to a process demand must be small enough that will reduce the overall

risk to below the acceptable level. This may be accomplished by carefully selecting the appropriate PES architecture using the methodology provided in Figure 2. Once a PES is selected and examined, its reliability must meet the safety performance requirements set at stage 6, Figure 1. This requires an iterative process where stages 7 through 10 in Figure 1 are followed until the final PES design does meet the prescribed safety requirements.

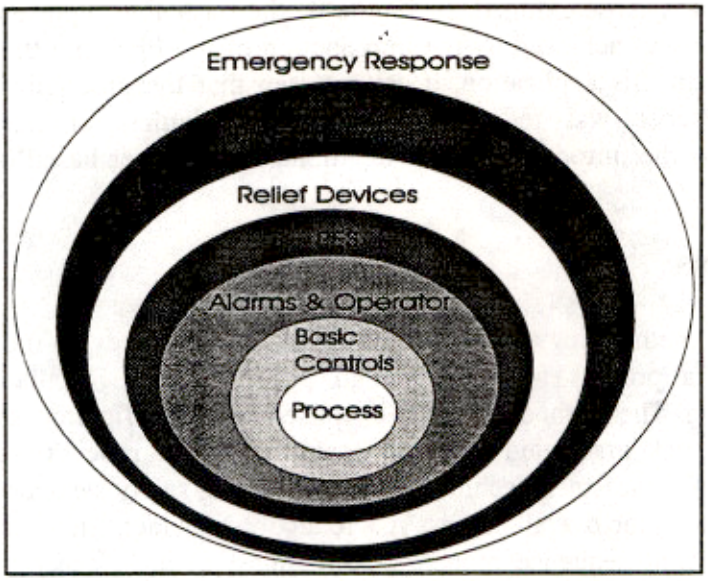


Figure 4. Safety Layer Concept with safety systems shown in order of activation.

RELIABILITY CERTIFICATION OF A NEW SAFETY SYSTEM

The certification or determination of a specific level of system reliability is accomplished through the use of Reliability analysis techniques. Reliability analysis employs systematic methodologies that decompose a complex system down to its basic components. Although the PES as a whole may be a new or custom designed, these components are used in other systems, and therefore sufficient performance data are available or may be collected. The performance and interactions of these basic components are merged into a reliability model to determine the overall system performance. The major steps of a reliability analysis are outlined in Figure 2. A general reliability methodology that can be applied to any system is discussed in detail by Stavrianidis (1993).

In the current application, it was decided to employ a new PES to reduce the risks of the process. Several PES architectures may be examined using the reliability methodology and the iterative procedure in Figure 1, stages 7 through 10. For every PES, an associated reliability value for specific system mission times is determined. Such an analysis for PESs is provided by Stavrianidis (1992).

A knowledge base expert system that employs the methodology discussed by Stavrianidis (1992) was developed by Yang (1993). This expert system facilitates the use of the reliability methodology on fourteen PES architectures using Markov modeling techniques and allowing for independent and common cause failures of the system.

PROCESS RISK ADJUSTMENT

The PES architecture that meets the safety performance requirements has been identified through the application of the reliability certification methodology, (Stavrianidis, 1992; Stavrianidis and Karydas, 1993). The PES is introduced into the accident modeling sequences (event tree analysis) for the process and the new risk associated with releases of the flammable gas is determined. In Figure 4, the dash line represents the reduction of process risk that was achieved by the introduction of the PES into the safety layer model of the process. In this application, it can be seen that the probability to have the same release consequence was reduced by almost two orders of magnitude. This was accomplished by the introduction of an additional safety layer based on PES technology.

CONCLUSIONS

An overall methodology based on a Process Safety Lifecycle model was introduced which follows a process from the design phase through installation, operation and decommissioning. The methodology was exercised on a specific process with the following results: a) the risk associated with the operation of the process was quantified using Quantitative Risk Assessment techniques; b) the existing safety systems were identified and their contribution to the overall process risk reduction was identified using the Safety Layer Model and accident sequence modeling techniques; c) an "acceptable safety level' is discussed and standards that attempt to set such levels are identified; d) a new safety system (PES) is introduced and its reliability is certified using Reliability Analysis techniques; and e) the contribution of the PES to the overall process risk reduction is quantified using accident sequence modeling techniques.

REFERENCES

1. "CCPS - Guidelines for Safe Automation of Chemical Processes", Center for Chemical Process Safety of the American Institute of Chemical Engineers, NY, 1993.
2. Contini, S., "Benchmark Exercise on Major Hazard Analysis", Commission of the European Communities, 1992.
3. Cranefield, J.T., Karydas, D.M. and P.A. Stavrianidis, FMRC Final Technical Report, Factory Mutual Research Corporation, Norwood, MA, 1993, (Proprietary).
4. "IEC - SC65A/WG10; Functional Safety of Electric/Electronic/Programmable Electronic Systems", International Electrotechnical Commission (pending).
4. "ISA - Programmable Electronic Systems used for Safety Applications", Instrument Society of America, SP84 Draft Report 13, 1993.
5. "OSHA - 29 CFR 1910, Process Safety Management of Highly Hazardous Chemicals", Occupational Safety and Health Administration, Washington, DC, 1992.
6. Stavrianidis, P.A, "Reliability and Uncertainty Analysis of Programmable Electronic Systems", Reliability Engineering and System Safety, Vol. 39, 1992.
7. Stavrianidis, P.A. and Karydas, D.M., "Methodology to Evaluate the Reliability of a Safety System", American Society of Mechanical Engineers, 1993 Winter Annual Meeting.
8. Yang, X.P. and Matthews, M., "Development of a Programmable Electronic System Reliability Assessment Expert System", Factory Mutual Research Corporation, Inter-company Communication, 1993, (Proprietary).

RISK ASSESSMENT: OVERVIEW OF LAND-BASED TORT LIABILITY

Joel L. Borrello and Mark J. Spansel

Adams and Reese
4500 One Shell Square
New Orleans, Louisiana 70139
Telephone (504) 581-3234

The law applicable to land-based tort liability varies widely from jurisdiction to jurisdiction. However, there are some basic principles of liability that are common to most if not all jurisdictions in the United States. This paper will present a brief explanation of some of those principles.

GENERAL TORT LIABILITY

General tort liability is imposed upon those who cause damage through their fault or negligence, that is, their failure to exercise ordinary care. Negligence is that conduct which falls below the standard established by law for the protection of others against unreasonable risk of harm. Underlying the concept of tort liability are the existence of a duty to the injured person, a breach of that duty and a causal relationship between the negligent act or omission and the resulting damage. The existence of a duty is generally a question of law, but a determination of whether the duty was breached and the extent of resulting damage is made by the finder of fact, that is, the court or jury.

The standard of conduct to which a party is held varies with the circumstances. The greater the potential harm, the higher the standard of care. Economics also has considerable influence on the applicable standard of care. For example, a compensated carrier owes a greater duty to a fare-paying passenger than does a host to a guest passenger and a compensated bailor a greater duty to a bailee than does a gratuitous one.

Individuals, of course, are responsible for the consequences of their negligent conduct. Corporations or other legal entities, which can act only through individuals, are considered to be vicariously liable for damages caused by the negligent acts or omissions of their employees acting within the course and scope of their employment. As a rule, a principal is not vicariously liable for the negligent acts of independent contractors which he hires to perform work on his behalf, unless the principal is engaged in ultra hazardous activity.

STRICT LIABILITY

In some instances, the law will impose a form of **strict liability** or liability without fault, which is a form of liability generally imposed by statute and founded on the public policy of the jurisdiction involved. Strict liability does not depend upon a showing of negligence, but is imposed by law when prescribed action or activity of a party causes damage. Some examples of those on whom strict liability is imposed are landowners who use their property to the detriment of their neighbors, owners or users of dangerous substances, machinery or instrumentalities and those involved in hazardous or ultra-hazardous operations. Ultra-hazardous activity is generally regarded as that activity which is unusual and poses a real risk of danger regardless of the care exercised in its performance.

PRODUCTS LIABILITY

Another form of strict liability is that of **products liability**. This body of law imposes upon manufacturer, or one who holds himself out as a manufacturer, liability for damages resulting not only from his negligence in producing the product but, even absent a showing of negligence, liability for damages resulting from a defect in the product which causes damage. To sustain recovery under the rule of products liability, the damaged party must show that the product was defective in that it created an unreasonable risk of harm when in normal use, that it was in normal use at the time of the accident and that the product was defective when it left the hands of the manufacturer. The duties imposed on a manufacturer include not only the duty to produce a product free of defects, but also to warn prospective users of those dangers which may be reasonably anticipated in connection with the use of the product.

NEGLIGENCE PER SE

One who breaches a duty specifically established by statute, ordinance or governmental regulation, may be strictly liable to those who are injured, if the statute, ordinance or regulation is designed to protect those who are injured against the risk involved. A breach of these legally-imposed duties will constitute **negligence per se**. Although the application of this doctrine raises a rebuttable presumption of liability, in some jurisdictions, the only defense to liability is proof not only that the act did not but could not have caused the damage.

LEGAL CAUSE

An essential element of any liability claim is proof of causation, that is, proof of a causal relationship between the offending act and damage. To support liability, the act must be a **legal or proximate cause** of the damage. There must be a natural and unbroken chain of causation between the act and the damage, unbroken by any intervening or superseding act or event.

The law recognizes that there may be more than one legal cause of damage. Two or more culpable acts may combine to cause damage. In this case, responsibility will normally be allocated to the offending parties in proportion to the extent that their respective acts contributed to the total damage. For example, if the finder of fact determines that A's negligence contributed 70% and B's negligence 30% to the total damage, they will bear responsibility for those proportions of the total damage. In the event that an injured party chooses to sue only one of two or more responsible parties, the party sued may claim against the other responsible parties for **contribution.**

Violation of industry standards or recommended practices normally do not constitute negligence per se, but rather may be used as an evidentiary standard against which to judge the culpability of the conduct.

RES IPSA LOQUITUR

Another evidentiary principle of tort law which affects liability is the doctrine of **res ipsa loquitur**, which, literally translated, means the thing speaks for itself. This doctrine is applied to situations in which the circumstances surrounding an incident are such as to raise a reasonable presumption that the act would not have occurred in the absence of some negligence or fault on the part of the party charged with responsibility. The facts themselves exclude other reasonable hypotheses of causation except negligence on the part of the party against whom the presumption is directed. When this doctrine is applied, a refutable inference of liability exists, and the party against whom it is raised must present proof sufficient to overcome the presumption.

DAMAGES

Normally, a liable party is responsible to pay to the injured party **compensatory damages**, that is, damages which will compensate the injured party for the pecuniary and non pecuniary losses resulting from the culpable act. In some cases, however, where the conduct of a party is particularly egregious, **punitive damages** may be awarded to punish the wrongdoer and to deter future similar conduct. Some examples of conduct giving rise to punitive damages are intentional or willful infliction of harm or damage, driving a motor vehicle while intoxicated, or acting with a wanton or reckless disregard for the public safety in the handling, storage or transportation of hazardous or toxic substances.

There has been a notable increase in claims for punitive damages, primarily because of the amount of potential recovery and the vague standards governing the conduct which may give rise to punitive damage awards. Appellate courts have sustained punitive damage awards hundreds of times greater than the amount of proven damages, often based in large part on the financial condition of the defendant. To date, a divided United States Supreme Court has upheld the constitutionality of punitive damage awards and has refused to establish definitive guidelines regulating the exercise of discretion in making such awards.

PROOF REQUIREMENTS

Unlike criminal cases in which the governing entity bringing the action must prove guilt beyond a reasonable doubt, plaintiffs in civil cases are required to establish the essential elements of their claims by a **preponderance of the evidence**. This means simply that considering the credible evidence as a whole, including all inferences and presumptions, the existence of a contested fact is more probable than its nonexistence. Proof of a fact may be by direct or circumstantial evidence or by a combination of both. **Direct evidence** is that which if believed, resolves a matter in issue. **Circumstantial evidence,** on the other hand, does not resolve the issue but permits the judge or jury to conclude from the evidence the existence or nonexistence of a contested fact. Circumstantial evidence has probative value if it excludes all reasonable hypotheses except that which is sought to be established.

CLASS ACTION

When numerous persons are damaged as a result of a common occurrence or condition, courts may permit the filing of a **class action.** These are suits filed by persons not only on behalf of themselves, but also on behalf of those persons similarly situated who also sustained damage as a result of the occurrence or condition. In the event that the court finds that there is a sufficient number of persons who sustained similar damage as a result of the occurrence or condition, the court may certify the action as a class action on behalf of all persons within the defined class who may have been damaged. Under class action procedure, once a court determines that a class is certifiable, a public notice is issued under the auspices of the court informing all potential claimants of their right to file claims within the proceeding. Class actions are common in cases involving major catastrophes such as fires, explosions, environmental emissions and other incidents in which numerous persons are damaged or exposed to damaging influences.

COST-RISK FACTOR DEVELOPMENT USING THE MAXWELL RISK CRITERIA MATRIX (MRCM) & THE ANALYTICAL HIERARCHY PROCESS (AHP)

David R. Graham

Chief, Communications Satellites Costing
SMC/FMCC
2430 E. El Segundo Blvd., Suite 2010
El Segundo, CA 90245-4687

INTRODUCTION

A briefing presented to the 24th Annual DoD Cost Symposium, entitled "A Quantification Structure For Assessing Risk-Impact Drivers" by R.L Abramson and S. A. Book, from the Resource Analysis Directorate of the Aerospace Corporation, outlined a procedure for developing a cost estimate of a subsystem that incorporated the influence of risk on cost. The briefing was based upon previous work done by F. D. Maxwell, also of the Aerospace corporation, who developed a risk-driver matrix that is known at the Space and Missile Systems Center as the Maxwell Risk Criteria Matrix (MRCM).

The Maxwell Risk Criteria Matrix (MRCM), as developed by Dr. Maxwell, is very useful in locating where a subsystem being evaluated for risk is relative to the criteria qualitatively (Fig. 1). However, as Dr. Maxwell points out in his paper, a shortcoming becomes evident as soon as one tries to quantify this location. The problem is that a numerical scale must be developed along each criterion's location continua in order to measure the magnitude of riskiness. Too much arbitrariness and not enough precision is allowed to enter into the risk evaluation. In this paper I will present an alternative application of the MRCM. I will demonstrate that embedding the MRCM within an Analytical Hierarchy Process (AHP) model eliminates arbitrary scaling

problems and allows for the refinment of the MRCM by making it easy to weight not only all the Maxwell Criteria but also easy to scale each of the individual criterion's location continua. The creation of a cost-risk factor developed as a result of this approach will be described.

RISK DRIVER CATEGORY	RISK LEVEL				
	LOW	MED-LOW	MEDIUM	MED-HIGH	HIGH
1. Required Technical Advancement	Nothing New	Minor Mods Only	Maj Mods	State of the Art	Past State of the Art
2. Technology Status	In Use	Proto Exists	Under Develop	In Design	Concept Stage
3. Complexity	Simple	Somewhat Complex	Moderate Complex	Highly Complex	Hi Complex & Uncertain
4. Interaction/ Dependencies	Ind of Other Risk Drivers	Dep on One Add'l Risk Drivers	Dep on Two Add'l Risk Drivers	Dep on Three Add'l Risk Drivers	Dep on > Three Add'l Risk Drivers
5. Process Controls	SPC	No SPC	Limited Controls	Inadeq Controls	No Known Controls
6. Manufacturing Precision	High	Adeq	Limited Margins	Known but Inadequate	Unknown
7. Reliability	High	Avg	Known Limited Problems	Serious Probs of Unknown Scope	In-Feasible
8. Producibility	Estab	Demo	Feasible	Known Difficulties	In-Feasible
9. Criticality To Mission	Non-Essential	Min Implact	Known Alts Avail	Possible Alts Exist	"Show Stopper"

FIGURE 1

COST-RISK DERIVATION

The cost-estimation process often assigns "low", "best", and "high" cost estimates to each subsystem. The low cost estimate generally specifies subsystem cost under the most optimistic assumptions concerning development and production capabilities. The best-estimate cost is typically derived from the output of a cost model or other appropriate estimating procedure such as analogy or engineering buildup. The MRCM was developed to determine a realistic and credible high-end cost that encompasses the impacts of all technical risks faced in developing and producing the subsystem. It does this by producing a 'risk factor' to apply to the best-estimate cost to determine a high-end cost. The low, best-estimate, and high costs then define a triangular probability distribution of cost for each subsystem. Monte-Carlo random sampling from each subsystem's triangular distribution produces a sequence of realizations of total-system cost that combine to define the cumulative distribution of total-system cost. Percentiles of total-system cost can then be read off the cumulative distribution.

The numerical value of the risk factor is determined by evaluating risk levels of the subsystem under study with respect to the 9 risk-driver categories (Fig. 1). A number, called a "risk value", is selected from an appropriate "risk-driver scale" and assigned to each of these categories. In accordance with engineering judgment concerning the specific nature and application of the subsystem under study, one particular risk-driver scale may be more appropriate than others. Scales that have been used in the past include the linear, logarithmic, and exponential scales. The risk factor for the subsystem as a whole is then calculated by averaging the risk values for the 9 risk-driver categories. Depending on the circumstances, a mean, median, or weighted average may be appropriate.[1]

This paper will suggest answers to F.D. Maxwell's three open questions presented at the end of his paper, (1) How the risk-driver numerical scale should be selected to realistically reflect a subsystem's high-end cost; (2) How risk values should be weighted among the various risk categories in compiling the subsystem risk factor; and (3) Whether or not different risk scales should be used for different risk categories.

THE ANALYTICAL HIERARCHY PROCESS (AHP)

The Analytical Hierarchy Process (AHP) allows for the modeling of criteria involved in influencing the outcome of any decision. Most often it is used in differentiating among alternative selections, for example, automobiles to buy, locations to build a retail store, personnel to hire, etc., based on criteria that are relevant to each decision.

The form of the criteria modeling is a 'tree' structure, the overall 'goal' of the modeled structure identified at the top of the tree with criteria and sub-criteria filling out the lower 'branches'. At the bottom of the tree are the 'leaves' or selections the decision maker is trying to choose among. Thus, AHP allows the factors that bear on the decision to be broken down into their separate pieces so that the decision maker can evaluate his or her factors individually.

Once so modeled, the criteria can be weighted relative to the goal, and sub-criteria can be weighted relative to their criteria, providing the decision maker with the flexibility of building-in his or her relative measures of importance to the criterion and sub-criteria. As I shall describe, this ability addresses F.D. Maxwell's three open questions mentioned above. The technique utilized for the weighting procedure is the 'pairwise' method. In this method for the criteria, each criterion is compared to each other criterion relative to the goal, a matrix of these ratings is tabulated by application of AHP mathematics, and a vector of values, called an eigenvector, is produced for the criteria so rated. The values calculated for each criterion in the eigenvector are the weights assigned to each criterion.

Once all the criteria are weighted by the decision maker to his or her satisfaction, each of the selections is rated relative to intensities (i.e. high, medium, low; simple, somewhat complex, moderately complex, highly complex; etc.) developed for each of the criteria or sub-criteria and the selection rated relative to the intensity scale. 'Scores' are accumulated for each selection by summing the products of the criterion's weight and the selection's intensity weight values across all criteria in a spreadsheet-like format. The rows are the selections and the columns are the criteria and sub-criteria. An intensity

rating is input to each cell where a row and column intersect. The selection with the largest overall 'score' is generally the preferred selection, however, in this application of the AHP, the scores of each selection are used to generate a ratio that represents the relative risk between the baseline and the alternative. In my example only two selections are compared, "Alternative A" and "Baseline". (See top half of Figure 2)

INTEGRATING THE MRCM AND THE AHP

Since the MRCM is a set of criteria it can, therefore, be modeled in AHP. Once so modeled it is quite straightforward to utilize the features of AHP described above to weight the risk-driver categories (i.e. criteria) and derive an eigenvector that represents the cost estimator's or engineer's judgements about the relative importance of each criteria and intensity influencing the program's subsystem under evaluation.

In the application of AHP to risk analysis we are concerned with just two selections. The first is the new program's subsystem we are trying to cost estimate (in this illustration case, 'Alternative A'), and the second is the technological reference point program(s) (i.e. 'Baseline'), for the subsystem as it exists in today's level of technology.

Since each criterion has a range of intensity levels associated with it, for example, the intensities 'Nothing New', 'Minor Mods Only', 'Maj Mods', 'State of the Art', 'Past State of the Art', for Required Technology Advancement, etc., each intensity weight can be determined the same way that the main criterion's weights were determined, i.e. by pairwise comparison. This allows for the explicit scaling of risk driver range values (i.e. intensities) not only independent of the other criteria but also without having to make an arbitrary determination of whether this range is a linear, logarithmic, exponential, etc., scale. The subsystem expert's own judgements determine the 'function' type.

Once the hierarchy is developed all that remains is the ratings of the selections. We rate both program's subsystems against each risk driver category with respect to where each program's subsystem falls within the risk driver category's risk levels. A summing is then completed for each program's subsystem across all risk-driver categories and a weight or a 'score' developed for each program's subsystem. The new program's subsystem score is divided by the reference point program's subsystem score and a ratio developed which is the risk factor to apply to the best estimate to determine a high-end estimate. (See Figure 2)

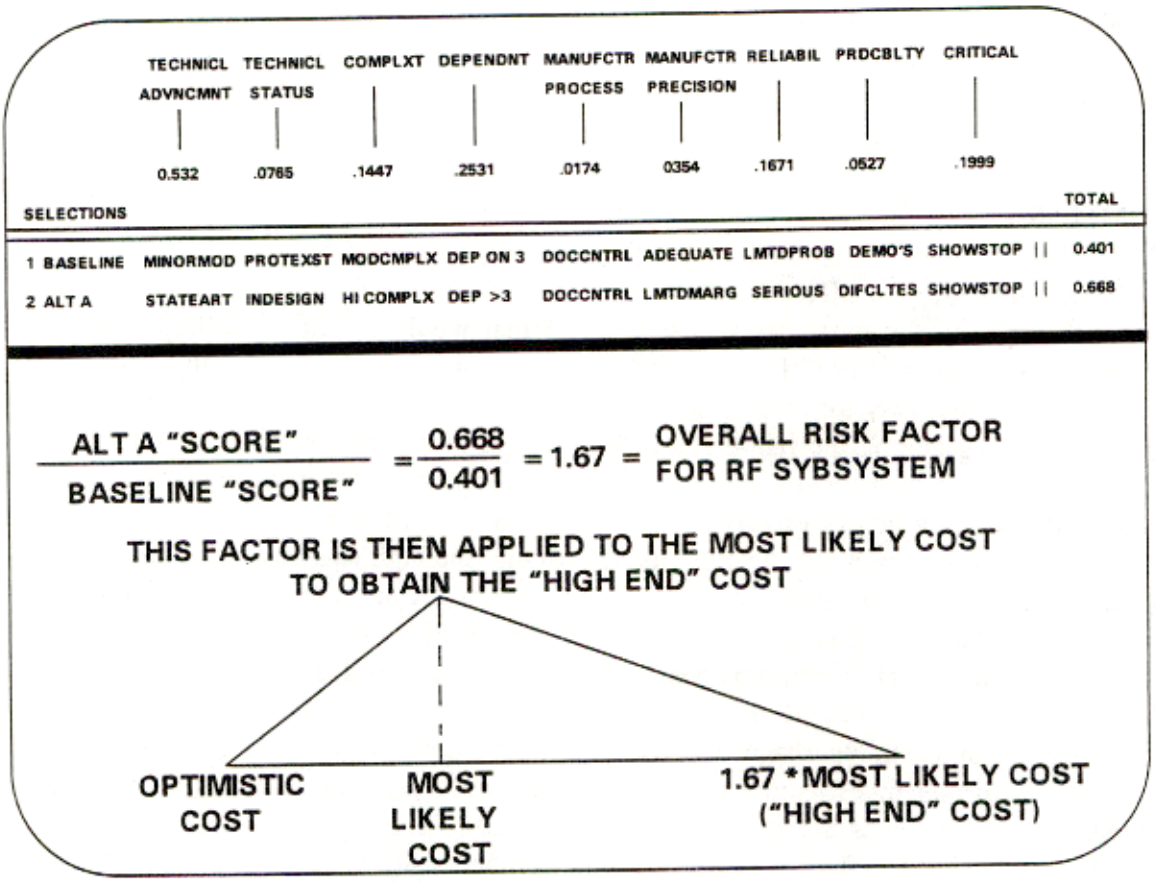


FIGURE 2

ANSWERS TO F.D. MAXWELL'S QUESTIONS

At this point I would like to return to F.D. Maxwell's three open questions presented at the conclusion of his paper and present answers to each.

(1) How the risk-driver numerical scale should be selected to realistically reflect a subsystem's high-end cost? (Dr. Maxwell is referring to what I have termed 'intensities'.) There should be no 'selection' at all! The weighting of the intensities is handled within the pairwise comparison exercise. There is no need to 'decide' ahead of time how they should be weighted, that is, in some arbitrary fashion, when the weighting becomes the natural result of the pairwise comparison process.

(2) How risk values should be weighted among the various risk categories in compiling the subsystem risk factor? Using the AHP there need only be the subsystem expert's judgements entered when deciding the relative importance of either the risk-driver categories or the intensities within each risk-driver category.

(3) Whether or not different risk scales should be used for different risk categories? The answer to this question is simply a moot point. Again, there is no need to think about whether or not different scales should be used because different risk scales are the by-product of the AHP weighting process. If the subsystem expert believes that all intensities are of equal influence then each intensity will be assigned an equal weight.

If he or she believes that they are not of equal influence, the subsystem expert is free to weight them accordingly, unconstrained by having to decide ahead of time which type of function to attribute to their relationship. The resulting function will be a natural fallout from the AHP.

SUMMARY

By utilizing the MRCM and the AHP a methodology was developed to derive a factor to apply to the most likely cost estimate that would generate the high-end of a triangular distribution useful for probabalistic cost-risk analysis. Using the AHP eliminates the necessity for arbitrarily setting numerical scales for the MRCM and assists in the weighting among the risk-driver categories. One question remains for the author and that is simply that once a risk factor has been derived, why should we use it as a direct multiplier on the most likely cost? I am not convinced that, a priori, we know that the true relationship between the most likely cost and the high end cost is represented by the factor we have developed. Even though much thought has gone into developing the criteria, sub-criteria, intensities, and ratings of the selections against the intensities, the assumption that the relationship between this factor and the 'best estimate' is linear is just that, an assumption. Through the application of the MRCM and AHP a great stride has been made to avoid the 'garbage in, garbage out' situation for generating endpoints to a distribution, further investigation is warranted. It is quite possible that during the actual development of the subsystem the honestly perceived risk, before beginning the project, would be managed to affect the cost outcome in manner not exactly like we postulated with our risk factor. Perhaps, after the subsystem has been developed, the cost impact turned out to be less by a quarter the risk factor we developed. Perhaps if we had taken the square root of our derived factor we would be closer to the true relationship between the most likely cost and the high end cost. We do not have a satisfactory anwer to this question now. However, we have begun a research project to attempt to determine the true relationship. We feel the answer lies in examining actual data. We, at SMC/FMC, will develop a strategy for tracking the risk-driven cost growth, using Cost Performance Reports, risk management reports, technical status reports, etc., for programs at SMC that are fairly early in their acquisition cycle, and that have an a priori risk dollar impact already developed as part of a program office estimate or an independent cost estimate. By monitoring the cost growth, identifying what part of the growth was risk-driven, and comparing the final costs with the estmates we will have a better idea as to the true relationship between the MRCM-AHP derived risk factor and the true relationship between the most likely cost and the high end cost.

1 "A Quantification Structure for Assessing Risk-Impact Drivers" Executive Summary; R.L. Abramson and S.A. Book; Based on the "Risk-Driver Scales" of F.D. Maxwell; Engineering Group, The Aerospace Corporation, 1990

036 Risk Management in DOE (II)

Chair: T. Eng, USDOE

Environment, Safety and Health Decision Process at a DOE Multipurpose Research Laboratory

W.R. Casey, M.S. Davis, J.B. Deitz, O. White (BNL)

Risk Management at Argonne National Laboratory

D.J. Hill, R.D. Hislop (ANL)

Probabilistic Risk Assessment of Manufacturing Activities Within the U.S.Department of Energy

P. Prassinos, P.D. Dilley (USDOE); P. Carrara (Advanced Sciences)

ENVIRONMENT, SAFETY AND HEALTH DECISION PROCESS AT A DOE MULTIPURPOSE RESEARCH LABORATORY

W.R. CASEY, M.S. DAVIS, J.B. DEITZ AND O. WHITE

Brookhaven National Laboratory
Upton, NY 11973

INTRODUCTION

The primary goal of Environment, Safety and Health (ESH) management at Brookhaven National Laboratory (BNL) is to maintain a strong base program and to achieve a reasonable balance between the new environmental, safety and health demands and the research mission of the Laboratory. This balancing of potentially conflicting demands requires a consistent approach to assessing the risk of operations and facilities and the costs associated with meeting or exceeding new or changing ESH objectives. While "systems" have been and continue to be developed for the assessment of the risk of operations and facilities, the decision process for assuring the efficient and cost-effective allocation of resources for addressing both ESH requirements and mission requirements remains highly subjective. This is particularly true of Department of Energy (DOE) facilities where activities vary from site to site, and the risks associated with these activities can range from those of high hazard operations to those with the potential for little or no major risk.

In an era of concerns over cost control, the efficient, effective use of staff and resources in the pursuit of excellence in ESH play a significant role in management decisions. Each site must develop a consistent method for establishing an acceptable trade-off between excellence in ESH and excellence in mission. Brookhaven National Laboratory's vision is to strive for the same level of excellence in ESH that it has achieved in its research mission. Limitations in the human and financial resources to achieve these goals require an approach that provides management a decision-making tool for issue resolution that is consistent and defensible.

BNL has been evolving a systematic process for issue resolution and risk management that is responsive to the Laboratory's unique operations and which strives to integrate the principles of quality management into its ESH program.

ESH ISSUES AND RISK MANAGEMENT AT BNL

As a multi-program facility, BNL is a site characterized by extensive ESH diversity. The facilities and activities at BNL may present radiation, industrial or chemical

hazards, with the potential for workplace and environmental impacts. In addition to many common facilities, there are unique, one-of-a-kind facilities with large user communities and, environmentally, BNL is situated over a sole-source drinking water aquifer.

A hazard classification is performed at the site using a DOE system[1] which ranks facilities from high to low depending upon the potential impacts of an accident offsite, onsite or within the facility. The High Flux Beam Reactor (HFBR), which operates at 30 MW and produces neutrons for research, is classified as a high hazard facility. The BNL accelerators and most of its other research programs involve low hazard activities. There are "industrial" operations at the Central Steam Facility, Water Treatment Plant, Chilled Water Facility and Sewage Treatment Facility. While BNL does not dispose of hazardous or radioactive waste on site, we do conduct waste management operations that include storage, packaging and shipment of hazardous and radioactive wastes for off-site disposal. In addition, hazardous and low-level radioactive materials are transported on site as well as offsite. BNL is a Comprehensive Environmental Response Compensation and Liability Act (CERCLA) site and will engage in extensive remedial activities, although the types and extent of contamination should not result in major risk to remedial workers, BNL staff or the public.

BNL has developed comprehensive ESH programs to address the primary risks associated with the operation of the site. Increasing costs for ESH are generally associated with costs for improvements to older facilities or costs associated with new ESH requirements. The decision to incur an increased cost for the ESH program has to be continually assessed against the risk associated with all site activities. Resource limitations demand that the relative risk of any operation be viewed in the context of the whole. When significant reduction in risk is possible or when the cost for risk reduction does not result in a significant enhancement in safety or environmental protection, the decision may be clear-cut. However, activities which represent overall quality improvements but do not necessarily reduce risk substantially may still be desirable for operational efficiency and may, in the long term, result in cost savings. Community relations and the desire for the Laboratory to be an accepted and welcomed member of the community can also influence management decisions, even if the risk associated with no action is low. Compliance with legal requirements, even for low-risk activities, will influence the relative priorities assigned in planning for new ESH program elements.

Risk management at BNL is only one facet of the overall integrated ESH program that is designed to achieve the Laboratory's vision of improved performance and future vision of the Laboratory. Risk evaluation and management is a part of an overall system for planning, self evaluation and effective change. Figure 1 schematically illustrates the major elements of BNL's program. The base or existing program is defined by current standards that are outlined in BNL's policies and standards. Requirements, improvements and non-compliance issues which result from BNL's multi-tiered self-assessment program or which are generated from external sources are evaluated through the issues management program. This involves a multi-step process (Figure 2) where risk and costs for risk reduction are estimated. Not every issue requires a complete analysis and the first step of the process is an initial determination of whether a more detailed analysis is required. Once it is determined that further analysis is warranted, the risks associated with not addressing the issue are estimated, activities that can reduce the risks are defined and the net reductions in risk are estimated. The net risk reduction value is used to establish an initial priority within all outstanding ESH issues that require additional, significant resources and/or staff commitment.

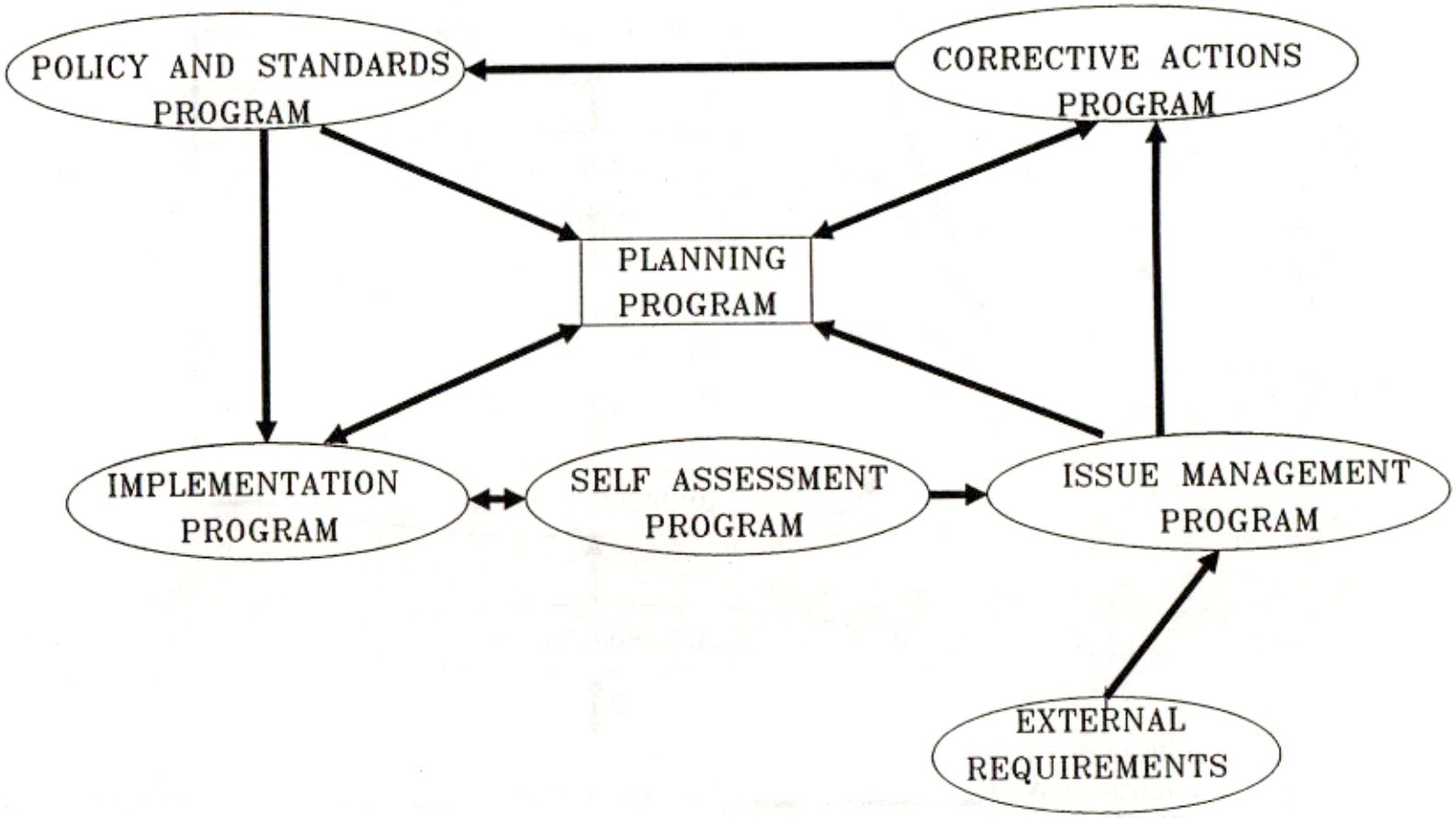


FIG. 1 BNL ESH MANAGEMENT PROGRAM

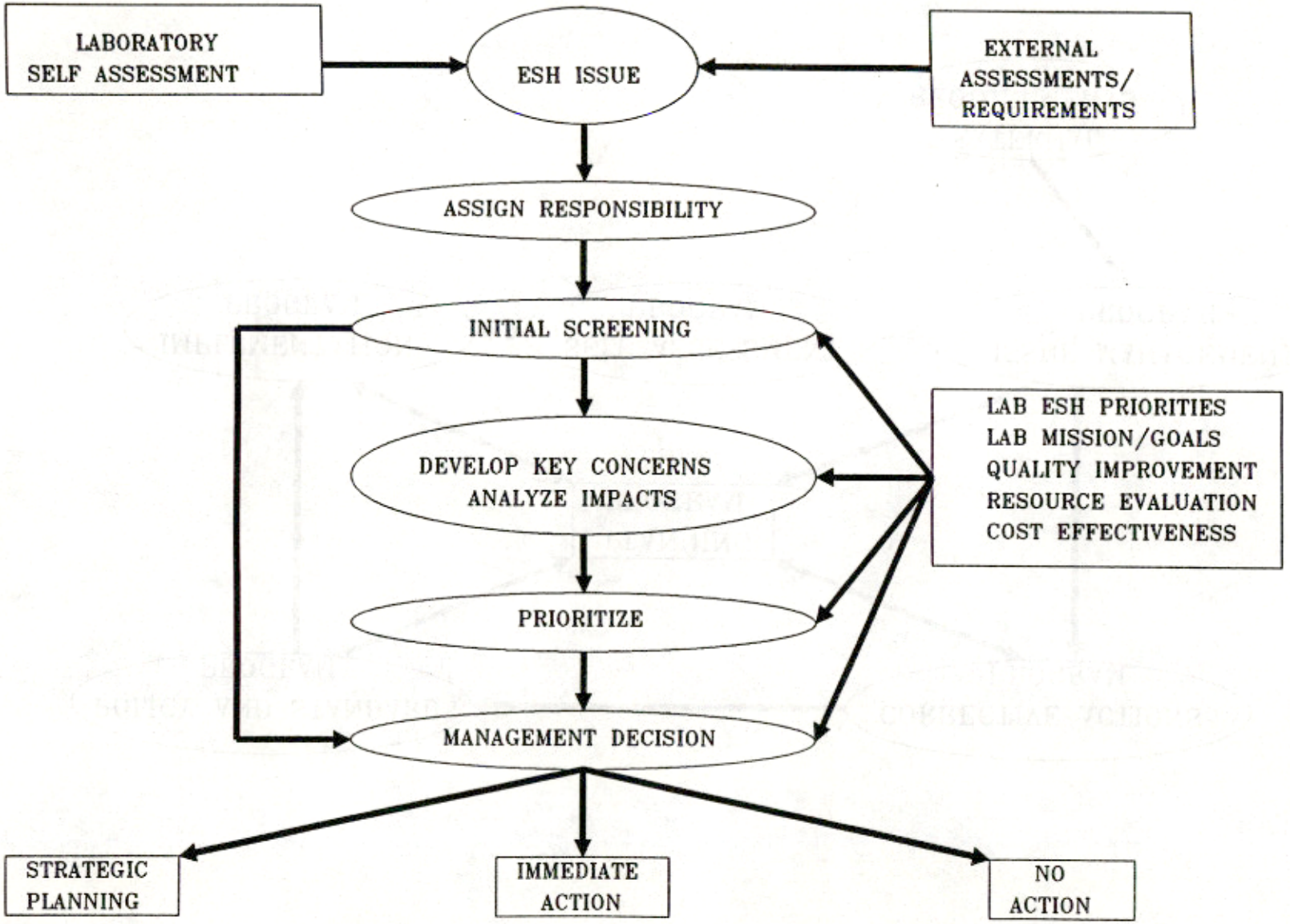


FIG. 2 ESH ISSUE MANAGEMENT PROCESS

Currently, BNL uses a "risk" evaluation system developed by DOE[2]. This model uses several modules for evaluating risk, including public safety, worker/site personnel safety, environmental compliance and mission impacts. Each module consists of possible consequences. Based primarily on professional judgment, the user determines the likelihood of a consequence and a weighing factor is assigned.

While this approach is not rigorous, it does provide a site such as BNL with an overview of the current ESH issues or demands and their relative priority. The risk prioritization model is not sufficient in itself for decision making. There are problems with the model, its application and the way in which it is used by those not directly associated with the site. It is equally important to develop a comprehensive analysis that encompasses not only the risk assessment, but which also documents other factors, including a knowledge of the operations of facilities, any unique factors (public concern, enforceable agreements) which may not be in effect at other DOE sites and sound professional judgment of the potential trade-offs between safety systems and administrative procedures for controlling operational risks. It is the complete analysis that must be communicated effectively and concisely to management.

Once the issues have been analyzed, the risks assessed, management informed and decisions made, implementation requires planning, scheduling and a commitment to proceed. These activities have to be an integral part of an overall program to manage the ESH programs at the site and viewed in the context of assisting the Laboratory in organizing and committing staff and resources in a cost effective and efficient manner.

ISSUES ASSOCIATED WITH THE DECISION PROCESS

Any decision process must be as defensible and as objective as possible. Clear lines of communication and definitions of roles, responsibilities and authorities are needed to assure a consistent approach. Resources must be available to implement decisions and the consequences of delay or no action must be understood. Above all, the process should assist the Laboratory in attaining the long-range ESH vision.

Risk management, as an integral part of the overall decision process at a site such as BNL, must therefore encompass the following elements:

- it can be applied with relative ease by a large number of people to a significant number of diverse ESH activities,
- it should include and balance the factors used to assess risk, including mission, management and business impacts that provide a site-specific approach which can be used to plan, schedule and budget ESH activities, and
- it must effectively communicate to management the major elements and impacts that should be considered in making a final decision.

The risk assessment process currently in use at BNL does not yet satisfy these criteria. The risk evaluation process employs a structured consensus method for use by knowledgeable professionals and is not easily adapted to wide-spread application by others. The factors involved in determining a risk "value" are subject to variations in interpretation and, to achieve consistency, a small group working together must be used to rank a large number of issues. The weighing factors assigned to each consequence do not have a proper balance between safety, environmental and mission/business factors. The base or ongoing program efforts are not ranked. Consequently, efforts that may enhance or provide value added to the base programs may not be properly weighed.

Even with a consistent assessment of risk and assignment of priorities, risk reduction

of addressing an issue or financial constraints may affect the schedules with which the Laboratory can respond. In addition, BNL is but one of a large number of DOE facilities, and the priority with which DOE addresses the site does depend on the perception of BNL's needs versus other DOE facilities' needs.

These issues are being addressed by BNL for its ongoing activities and for planning and budgeting future ESH initiatives. Trigger levels are being developed to help staff determine when a detailed risk assessment needs to be conducted. Simpler systems for assessing risk are being explored for use by the individual departments and divisions on site. The weighing factors currently in use are being revised to better reflect site-specific factors, including management concerns, to better address the mission and cost impacts. Procedures for documenting the assessments are being developed so that management can focus on the factors driving the assigned priority of the ESH activity.

All of the efforts that the Laboratory will undertake within the next year, while aimed at building a consistent approach to risk assessment and issue resolution, are not meant to eliminate the need for management involvement or attention; rather, they are to focus that attention on priority issues and to help in the long-range planning for activities at the site. It is the intent of the Laboratory to maintain ownership of the programs, to be active in any decisions that affect the operations of the site and to assure that DOE is fully cognizant of the needs and priorities of the site and how we propose addressing them.

While the initial decision and planning process can proceed at the local (Laboratory) level, the final decision at times may rest with DOE. DOE must also be organized to assure effective lines of communication and the vesting of authority at an appropriate level or the systems and processes established by the Laboratory will not be fully effective. If the process is to work efficiently, there must be a level of confidence that resources will be committed by the Laboratory or be made available by DOE. For the Laboratory, this requires appropriate planning and the inclusion of cost-intensive activities in the budget requests. For DOE, this requires a nationwide assessment of where funds are needed on a priority basis. The very nature of the current budget process and the complexity of DOE sites and their needs has resulted in an inefficient process for addressing ESH issues. At sites such as BNL where we are addressing low risk issues, this means that the Laboratory must pursue its own path to excellence, assure that we understand the risks involved in operating the site, understand the options that are available to us for minimizing risks where practical and institute the processes which will keep us focused on the continuing need to balance ESH demands while maintaining the mission of the Laboratory.

CONCLUSION

DOE laboratories such as BNL have longed recognized the need to balance the demands of program objectives with those of environment, safety and health requirements. At sites such as BNL, where the risks from operations are low, there needs to be a consistent approach to establish the priorities, define the level of "excellence" that is achievable with available resources and staff and to continually assess the effectiveness by measuring progress toward excellence in ESH.

[1] DOE Order 5481.1B, Safety Analysis and Review System, September 23, 1986.

[2] Department of Energy Guidance Manual to Support Development of the FY 1995-1999 Safety & Health Five-Year Plan, November 1992 and the U.S. Department of Energy Safety and Health Five-Year Plan Assistance Manual, November 20, 1992.

RISK MANAGEMENT AT ARGONNE NATIONAL LABORATORY

D. J. Hill[a] and R. D. Hislop[b]

Reactor Analysis Division[a]
Advanced Photon Source[b]
Argonne National Laboratory
Argonne, IL 60439

INTRODUCTION

Argonne National Laboratory (ANL) is a DOE multipurpose Laboratory with primary sites in Illinois (ANL-East) and Idaho (ANL-West). At ANL-East there are a number of inactive facilities as well as one active nuclear facility, Intense Pulse Neutron Source (IPNS), and many hot cells, caves, etc. associated with fuel behavior and actinide recycle programs. In addition, a major user facility, the Advanced Photon Source (APS), is under construction. At ANL-West there are several nuclear facilities including a small but complete Liquid Metal Reactor, the Experimental Breeder Reactor-II (EBR-II), and the associated fuel processing facility, Fuel Cycle Facility (FCF). These two facilities form the centerpiece of ANL's Integral Fast Reactor Program. Other facilities include TREAT, a transient test reactor, Fuel Manufacturing Facility (FMF), Hot Fuel Examination Facility (HFEF), and Zero Power Physics Reactor (ZPPR).

The only facility at Argonne National Laboratory which is classified as high hazard is EBR-II. A Level I Probabilistic Risk Assessment (PRA), including external events, has been completed for EBR-II. There were several objectives for this project; to provide a quantitative estimate of the risk associated with the operation of EBR-II, to provide a framework for managerial decision-making for the management of risk at the facility, and to provide insights into the nature of the risk of EBR-II that can be applied in the design of future LMRs. Other ANL facilities do not have complete probabilistic assessments. Despite this fact, Risk Management is an essential part of ANL's approach to safety and operations.

Risk management at Argonne National Laboratory is not limited to accelerator or nuclear facilities. It is also an integral part of construction activities. The Advanced Photon Source, a major construction project at the Laboratory, utilizes a variety of risk assessment techniques to identify potential construction loss exposures and to develop measures to eliminate them. Over the past 15 years, in excess of 15,000 pages of regulatory requirements pertaining to environment, safety and health have been printed in the Federal Register. Not all of these are applicable to Argonne National Laboratory all of the time, but as a highly-visible, nationally-funded facility, compliance with those that are applicable must be above reproach. Therefore, risk management is also a very

important part of construction activities at ANL.

This paper will give examples of these activities, such as, the EBR-II PRA, risk-based analyses of Fuel Cycle Facility Safety Systems, reliability studies of the Access Control Interlock System for the Advanced Photon Source and management approaches for controlling risk during the construction activities at APS.

EBR-II PROBABILISTIC RISK ASSESSMENT

The Experimental Breeder Reactor II (EBR-II) is a US Department of Energy (DOE) Category A research reactor located at Argonne National Laboratory (ANL-West) in Idaho. EBR-II is a 62.5 MW-thermal Liquid Metal Reactor (LMR) that began operation in 1964 and is currently being used as a testbed in the Integral Fast Reactor (IFR) Program.[1] ANL has completed a Level 1 Probabilistic Risk Assessment (PRA) for EBR-II. The Level 1 PRA for internal events and most external events was completed in June 1991[2]. The seismic PRA for EBR-II has recently been completed and is described in a separate paper[3]. EBR-II PRA results are being used in many aspects of risk management for EBR-II. Specific examples of the risk management are given below.

Every 24 hours (at midnight) the EBR-II operating crew "exercise" the control rods. The exercise involves moving two rods simultaneously in opposite directions without perturbing reactor power, thus ensuring their freedom to move and scram if necessary. This exercise was instituted over twenty years ago after a mechanical failure released debris into the primary tank which led to a concern that the debris could lead to the sticking of control rods. In the EBR-II PRA the daily exercise appeared in two separate ways: it provided the mission time for testing of the operability of the scram function and thus was a key factor in determining scram reliability, however, the number of demands on the control drive mechanism was an important factor in determining the frequency of the reactivity insertion initiating event.

Following an incident at EBR-II in which two rods of unequal worth were moved simultaneously, resulting in a very minor overpower event there was a review of the procedure. EBR-II operations felt that the potential for error in performing this procedure was too great and wished to reduce the frequency of testing, and the nature of the motions. The EBR-II PRA was used to determine acceptable frequencies and ranges of motion without significantly altering the risk of operation of EBR-II. As a result of the analysis, the procedure is still carried out daily but the range of motion is restricted to reduce the likelihood of operator error whilst preserving the procedure as a test of the functionality of the scram system.

Another example of this type of risk management arose with proposed installation of a wet-pipe fire protection system in the cable routing room to replace the existing halon system. In this case the concern was for inadvertent actuation-induced transients. It was determined from the EBR-II PRA that this cable routing room was not a significant location for reactor safety, primarily because of EBR-II's passive safety features[4]. Data on inadvertent acuation rates in the DOE complex and industry was collected and a cost-benefit analysis conducted. The key unknown in this case was the fraction of the safety-related electronic equipment that could be salvaged following an inadvertent actuation of the wet-pipe sprinkler system. As a result of this analysis, the wet-pipe system will only be installed when two conditions are met. The two conditions are: a) the removal of steam-fed heating from the room, because it was determined that failures of steam heating systems were both a source of moisture which could damage equipment and an important cause of inadvertent actuations, and b) the separation of power supplies to the primary pump clutches, removing the only possible water-induced initiating event of any consequence.

FUEL CYCLE FACILITY

Fuel Cycle Facility is currently under refurbishment and will again be the fuel manufacturing and reprocessing facility for EBR-II. The FCF facility is provided with a Safety Exhaust System (SES) designed for high reliability. The system consists of an active train with an operating fan and a closed damper, and a standby train with a fan at rest and an open damper. The Sense and Command subsystem that controls the operations of the dampers and fans actuates on pressure sensors in some of the cells of the facility. Because the system is designed for high reliability, the sensitivity results in a relatively high rate of inadvertent actuations. Inadvertent actuation is undesirable because of the possibility of drawing air into the Argon cell.

A study of inadvertent actuations of the SES due to malfunctions of the sense and command system was completed. The results of the study showed that the expected mean rate of spurious actuation was 0.56 times per year. The study was extended at the request of the design review committee to determine if a number of suggested alternatives could be implemented to reduce the calculated number of inadvertent actuations. These alteratives included redundant power supplies for the SES Sense and Command instrument racks, a conversion to two-of-three trip logic, and replacement of components which are the major contributors to inadvertent actuations with components having increased reliability.

The basic conclusion of the study is that the rate of inadvertent actuations is a consequence of the design philosophy (i.e., fail safe) and not the implementation of the SES Sense and Command design. The suggested changes offered by the design review committee would provide only a marginal reduction in the inadvertent actuation rate.

Another example relating to Fuel Cycle Facility and the whole of the ANL-West site concerns the water tanks used to supply water for fire fighting. One ANL-West water tank is not seismically qualified, and a seismically-qualified replacement is to be constructed and ready for use in two years. The issue to be resolved is: Should the nonseismically-qualified tank be decommissioned in the interim? The resulting analysis determined that it should not to be decommissioned, i.e., the risk of not having adequate water supplied for fire fighting outweighed the risk of seismic-induced failure leading to local flooding. However an alternate operating method was proposed to reduce the likelihood of seismic failures whilst still maintaining adequate fire-fighting capability.

ADVANCED PHOTON SOURCE RELIABILITY STUDY

The APS facility includes several stages: LINAC/PAR,SYNCHROTRON, and STORAGE RING. Each of the three parts of the accelerator will have an Access Control and Interlock System (ACIS) for personnel protection. At the time of the reliability study, the LINAC was being prepared for commissioning and the reliability study concentrated only on that ACIS.

In the reliability study, the different scenarios leading to potential personnel exposure were analyzed. The failure modes of the ACIS system were defined as those failures that would permit a person to be in the LINAC tunnel with no further interlocks preventing the actuation of some of the beam equipment, in such a way that exposure to radiation would be possible. The final set of failure modes analyzed included the inadvertent or premature actuation of the beam permissive by the ACIS, and the failure to trip under different conditions (door open, crash button pushed, and radiation alarm) when the beam is operational. The ACIS system fault tree models included programmable logic controllers (PLC) failures, as well as failures of the components involved in monitoring the interlocks (door switches and lockout keys), and equipment controlled by the ACIS to

provide the beam permissive.

The analysis, at this stage, was mainly qualitative than quantitative, given that the assessment of the reliability of the PLC equipment, in particular the user software, is the object of an extension of the study. Nevertheless, upper bounds were estimated for the probability of failure of the ACIS under the different situations. Qualitatively, the system was found to be well designed, with redundancy and diversity included as preventions against common cause failures. No single failures were identified by the fault tree analysis that would cause the failure of the ACIS to perform its personnel protection function.

An alternative which included a redundant, simple, hardwired system in parallel with the PLC of the ACIS was also analyzed. The analysis compared the reliability of the system with and without the parallel hardwired system and showed that only marginal gains would be achieved with this alternative. The reliability study was used in support of the reviews for the commissioning of the LINAC.

Future work will address the PLC reliability and will be extended to cover the other components of the APS facility. The fault tree models will also be used in analyzing the impact of the protection systems on the availability of the APS facility.

ADVANCED PHOTON SOURCE CONSTRUCTION ACTIVITIES

Preconstruction site evaluations are one of a variety of risk assessment techniques used to identify potential loss exposures which could adversely affect construction progress from either a programmatic or regulatory perspective. Failure to conduct these types of evaluations exposes construction projects to the potential for serious delays. Environmental compliance, cultural and historic concerns, and the physical constructability of the APS facility were all evaluated before the first construction contractor set foot on the project. Once it had been determined that there were no lurking "show stoppers," such as historic sites or insurmountable environmental issues, the feasibility of building the facility as designed by the architects was evaluated. The assembly of the buildings, their operating components, and the manner in which the completed facility will be operated were evaluated. This evaluation extended to the work practices of the contractors engaged to assemble the facility.

Environmental and Cultural Assessments

An assessment, conducted to determine the impact the proposed facility might have on the environment, revealed that three areas containing vegetation common to intermittent prairie wetlands lay under the proposed footprint of the facility. To minimize the effect on the wetlands, the facility footprint was moved out of the way of the larger wetland, and a new 1.8 acre wetland was designed and built according to U.S. Corps of Engineers' criteria to compensate for the loss of the two smaller areas.

A cultural assessment revealed evidence of prehistoric native Indian activity in the proposed construction area. A number of primitive Indian artifacts were unearthed, classified and sent to the Illinois State Museum for preservation and future study by archaeologists. A number of other artifacts dating from the early 1800's were also identified on the site, including clay smoking pipes, marbles, medicine bottles, and a family pet cemetery. This activity satisfied the requirements of the Illinois State Historic Preservation office requirements.

When site clearing activities finally began for the APS, an earth-moving contractor uncovered several tombstones. The contractor was concerned that he had unearthed a cemetery. This had the potential of shutting down his activities for some time if human remains had to be transferred to another location. However, review of the cultural

assessment of the site revealed that a former resident of the area had been the custodian for a nearby cemetery and had used damaged headstones as bulk material in the foundation of his home. Had this information not been available, construction activities would have been delayed for an appreciable time. In this case, the contractor was delayed for only one-half hour.

Constructability Review

Constructability of a project is the determination of whether a facility proposed by architects and their structural engineers can be erected as designed. Evaluation of the constructability of a facility is important to the project construction management team in order to understand and manage the risks present during construction. The material to be erected, the sequence of erection, and the manner in which they are to be erected are all important considerations. By working with the architects and their engineers, risk managers are able to make recommendations to reduce identified risks. For example, the Advanced Photon Source design called for handrails along the edge of a mezzanine. The fabrication and delivery of the handrails was scheduled for one year after completion of the mezzanine construction. This left the area without fall protection for a lengthy period of time. A schedule change was recommended in order to have the handrails delivered and installed shortly after the mezzanine construction was completed, thus eliminating a potential risk.

Construction Accidents

Contractors and their employees also present a major risk exposure to construction projects. Not all contractors employ safe work practices. These entities present a loss risk to themselves and other individuals working on site. The evaluation of contractors who bid on ANL construction work includes their past safety performance. The rational for including safety performance requirements is that contractors with unsafe work practices have a higher than average accident experience, and thus present a higher potential risk to the project schedule and budget. Accidents have the potential of not only delaying the affected contractor, but also the work of other involved contractors. Accidents consume project management and administrative time for investigations, analysis, reporting, and the rescheduling of work.

The frequency of accidental losses on a construction site are a reflection of the level of safety being practiced. One way of controlling this risk exposure is to understand root and casual factors of the accidental losses. All such losses at APS are analyzed and the resulting information is subsequently evaluated for trends and program weaknesses. However, a sound safety program can present a problem in that there tends to be few accidents and therefore, little data are available. The Advanced Photon Source project has experienced only six lost time cases in the past four years of construction. Accident experience is measured by the work hours of exposure. The project's current lost time accident index rate is .9, which is equivalent to saying that the safety program is such that one can expect one person in every work crew of 100 laborers to experience a lost-time accident once each year. The industry average for heavy construction, excluding highways, is 6.3/100.[5]

Other data, such as near-miss reports and facility inspections, are collected in order to identify and classify the source of risk during construction. However, near misses are difficult to identify, and frequently, are not reported. Inspections provide a more reliable source of information for the evaluation and management of risk. A formal program of inspections, identifying potential risk scenarios, has been established for the APS which includes personnel representation from all facets of the project. The information collected

during inspections is used to evaluate and identify the need for training and corrective actions.

SUMMARY

Argonne National Laboratory is making increasing use of quantitative risk management techniques to improve operation of facilities, make decisions on plant upgrades, improve safety system design and minimize the workers accident rates and lost time in major construction activities. The examples given in this paper are only some of the current applications.

These different, but complementary, aspects of risk management serve to demonstrate Argonne National Laboratory's commitment to using quantitative aspects of risk management to enhance worker safety, control construction costs and schedule and provide for more reliable and safe operation of its facilities.

REFERENCES

1. C. E. Till and Y. I. Chang, Integrating the Fuel Cycle at IFR, *Nucl. Eng. Intl.*, 33-34, (November 1992).
2. D.J. Hill, W.A. Ragland, J. Roglans, EBR-II Probabilistic Risk Assessment: Summary and Insights, *in:* Proceedings of the International Topical Meeting on Probabilistic Safety Assessment, Clearwater Beach, FL, January 1993, G. Apostolakis, ed., American Nuclear, Society, Lagrange Park, IL (1993).
3. J. Roglans and D. J. Hill, The Experimental Breeder Reactor II Seismic Probabilistic Risk Assessment, *in:* PSAM-II An International Conference Devoted to the Advancement of System-based Methods for the Design and Operation of Technological Systems and Processes, March 20-24, 1994, San Diego, California.
4. H.P. Planchon, et al., Implications of the EBR-II Inherent Safety Demonstration Test, *Nucl. Engrg. Des.* 101:75 (1987).
5. Accident Facts, National Safety Council, 1989.

PROBABILISTIC RISK ASSESSMENT OF MANUFACTURING ACTIVITIES WITHIN THE U.S. DEPARTMENT OF ENERGY

P. Prassinos,[1] P.D. Dilley,[1] P. Carrara[2]

[1]U.S. Department Of Energy
Albuquerque Operations Office
P.O. Box 5400
Albuquerque, New Mexico 87185-5400
[2]Advanced Sciences, Inc.
6739 Academy Road N.E.
Albuquerque, New Mexico 87109-6829

INTRODUCTION

The U.S. Department of Energy (DOE), Office of Defense Programs (DP), has embarked on using Probabilistic Risk Assessment (PRA) techniques to evaluate and improve the safety of its hazardous manufacturing operations. The primary purpose of this effort is to employ a systematic and comprehensive methodology to gain engineering insights into the potential accident behavior of operations within DOE, to identify positive measures to prevent accidents and to mitigate their consequences. The hazardous operations being analyzed are associated with explosives, propellants, electrically initiated devices, and radioactive material that include: assembly and disassembly, on-site and off-site transportation, storage and staging, and operations associated with field testing.

DOE Defense Programs is applying risk assessment methodology developed from the commercial reactor industry to manufacturing processes to better understand how the risk may be controlled or reduced. This application of risk techniques can be extended to other hazardous operations outside of DOE.

BACKGROUND

The content, and the results, of the risk assessment are mandated by applicable DOE/DP Orders. Although all the requirements of these orders will not be repeated here, it is useful to mention that risk assessment will be used to evaluate accidents that could disperse radioactive material to the public and environment. The risk assessment shall include identification of potential accidents to include as a minimum and as appropriate, accidents which could result in impact, puncture, crush, fire, immersion, chemical hazards, and electrical hazards or credible combinations of the above hazards associated with on-site operation and off-site transportation. The scope of the risk assessments is, therefore, pre-defined. It is hoped that the development and application of a standard methodology for the analysis will drive results that are comparable.

DISCUSSION

Application of Probabilistic Risk Assessment to hazardous manufacturing operations differs from its application in the nuclear power industry. The operations being evaluated are made up of sequential steps performed primarily by trained personnel and do not depend heavily on the function of automated system and equipment but rather adherence to procedures.

This DOE program will perform two types of risk assessments based on both the type and the similarity of operations. First, operational risk assessments will be performed for those systems/subsystems that will undergo operations which are similar. This type of risk assessment will be performed to evaluate initiating events, accident sequences, and accident environments postulated to occur from the operations being evaluated. The response of the system/subsystem will then be evaluated against the accident environment to identify probable consequences. Second, system specific risk assessments will be conducted for those systems/subsystems that undergo unique operations. These risk assessments will require system specific evaluations and will use the results of the operational risk assessments. The evaluation of each specific system/subsystem will also include its response to the accident environments identified in the operational studies.

For each operation, subsequent risk assessment can be performed using the upper level models of the overall process flow. Lower level models can then be developed to capture the unique nature of the component undergoing the operation.

The initial risk assessment will be performed by teams made up of DOE personnel, DOE contractors and personnel from the national laboratories. Along with performing several assessments, these teams will be developing a consistent approach and guidelines that will be used to perform future analyses and provide a means of reviewing and evaluating risk comparisons among operations. Ultimately, the organization responsible for performing these activities will have the responsibility to perform the assessment and conduct reviews, as well.

METHODOLOGY

The methodology uses a probabilistic risk assessment approach applied to operations made up of sub-operations or steps. The overall methodology consists of: 1) description of the system/subsystem and operation, 2) identification of potential accident sequences, 3) identification and description of credible accident sequences, 4) description of the system/subsystem response and consequences, 5) identification of relative risk, with uncertainties, of dominant risk contributors, and, 6) identification of positive measures and relative values.

This flow is depicted in Figure 1. In the context of the risk assessment, the accident environment characterization will bring forth the characteristics of the environment impinging on the system/subsystem as a consequence of the initiating event.

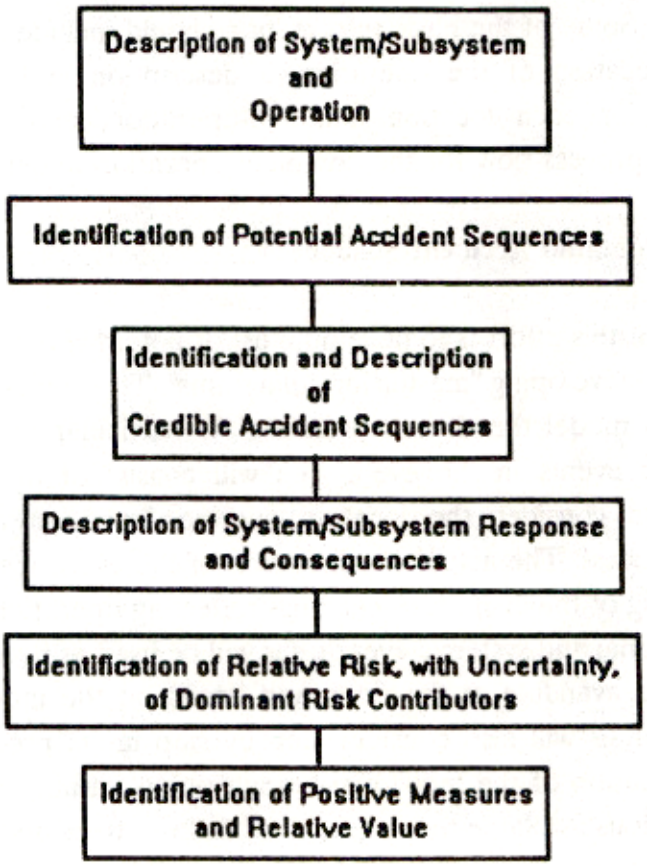


Figure 1. Risk Assessment Process

A short synopsis of the activities occurring in each of the six efforts delineated in Figure 1 follows.

Description of Operation

The objective of this task is to initially gain an understanding and overall familiarity with the operation, to establish the foundation for subsequent modeling activities by identifying the initiating events to be considered, the systems to be modeled, and the dependencies among systems and their support systems, if any. Investigation of initiating events is generally limited to those events associated with internal equipment, although external initiating events could be considered, based on the information available. The majority of the truly "external" events will already have been analyzed in the facility Safety Analysis Report. For the purpose of this effort, the identification of initiating events will lead to the identification of hazards and activities associated with the particular operation. It is important to realize that these risk assessments will interact closely with other safety documents that may already exist. Source information on a particular system will include; Safety Analysis Reports, operating procedures, system descriptions, etc. These sources of information can be of great value to this early stage of the assessment. Some of the basic information should include a brief description of the facility and location of the operation, a description and configuration of the system/subsystem for each location and sub-operation, and most importantly, a description of the process flow for the complete operation under consideration.

Identification of Potential Accident Sequences

The purpose of this effort is to develop a list of potential accident sequences. This is accomplished by developing "master logic diagrams". The envisioned application is to use event trees to model the overall process flow particular to the operation being analyzed. The top events in the event tree will consist of the individual steps or sub-operations and consider the location and configuration of the component undergoing the process. The actual configuration of the event tree will be dictated by the time sequencing of the event tree headings reflecting operational interdependence. To this end, functional and systemic event trees will be used as necessary, limited by the level of knowledge available at the time, and based on the individual system being analyzed. The analysis will also consider step by step faults propagated through the process. The evaluation of the individual branch points within the event tree can be modeled using various available techniques such as fault trees and/or human reliability models. These sub-operation models will focus on possible accident sequences that lead to severe consequences taking into account external events (events external to the sub-operation being performed) and the impact of facility systems to assure protection to the worker, public and environment.

Identification and Description of Credible Accident Sequences

Screening criteria will now be applied to the accident sequences identified in the prior step and screening will be performed both on a qualitative and a quantitative basis, depending on the hard data available. Those accident sequences identified earlier will be screened to identify "credible" accident sequences. Although the actual numerical values for the screening criteria have yet to be formalized, the accident scenario ranking will be based on qualitative weighing of the expected frequency of occurrence, the severity of the effects, the implicit limitations due to the scarcity and limitations of knowledge, and perhaps some early estimation of the value of prevention or mitigation. This task should also produce a complete listing of accident sequences which takes into consideration the accident environments particular to that location and system. The so called "accident environment" actually forms the basis for later development of the relative risk and the conceptualization of positive measures. The accident environment is a composite of operational and environmental factors.

Description of System Response and Consequences

This portion of the analysis deals with the identification and quantification, if possible, of the responses of the systems/subsystems to the accident environments which were characterized in the previous task. The accident sequences can be organized into groups based on their accident environments, as defined by accident and environment characteristics. Sequences that cause similar physical environments are grouped into "bins", which in turn can be subsequently screened for those that do not contribute significantly to the total frequency of the bin. In addition, accident sequences along with their environments that have no effect on the system/subsystem can be screened out of further evaluation. The system/subsystem responses to the characterized accident environment bins lead to consequences severities ranging from the violent reaction of explosives to the mechanical dispersal of radioactive material.

Identification of Relative Risk with Uncertainty of Dominant Risk Contributors

The sequences identified in the previous step are now used to develop an expression for determining which events dominate the frequency or severity. This evaluation is performed by analyzing the qualitative/quantitative expressions of failure combinations and severity contributing most to the accident sequences in order to isolate those particular aspects of the operation contributing significantly to the outcome of unwanted consequences. Insight into the operational features contributing mostly to risk, coupled with the respective adverse environments and system/subsystem response, should give rise to the identification of accident scenario patterns or classes of failures, based on the relative contributions of human errors, test and maintenance availabilities, and hardware failures. Importance calculations will be performed to rank all events that

have been shown to contribute to the system failure likelihood and response. Different measures of importance can be calculated, for example, risk reduction ratios, and risk increase ratios.

Identification of Positive Measures and Relative Values

All of the foregoing efforts result in an understanding of the systems, the potential hazards that may impinge on the system/subsystem, the initiating events that can give rise to an accident, the response of the system, and in general culminate with an identification of the weaknesses or vulnerabilities of the operation. The potential measures emplaced for obviation of the analyzed risks will be identified and analyzed from a benefit/risk reduction viewpoint. Some measures are expected to be easily implemented by merely fixing procedural shortcomings that make the operation susceptible to accidents, while others may be costly and much more difficult to fix. Sensitivity analyses could be performed to study the potential effects of decreases or increases in occurrence frequencies of damaging events. This in turn may lead to identification of enhancements to the operation or the facility that could lead to reductions in risk. Since it is expected that human error may be a large contributor to the overall risk, it is possible that additional administrative controls, annunciators or similar measures could lower the estimates for those sequences by orders of magnitude.

CONCLUSIONS

The initial application of risk assessment to hazardous operations within DOE will be of a qualitative nature. Initiating events, hazards, and accident sequences will be identified, developed and evaluated to gain insights into the possible failure behavior of each operation. The resulting accident sequences will be ranked based on a qualitative weighing considering such factors as expected frequency of occurrence, severity of the accident environments and consequences, knowledge limitations, and the value and ease of implementing positive measures. Initially, the identification of positive measures will be performed by examining the minimal cut sets and by application of engineering judgement, to the extent applicable, in the event of absence of hard data. As the risk assessments mature and more data for quantification become available, more stringent approaches will be applied.

Subsequently, the models developed in the qualitative risk assessment will be used to identify the data and information needed for quantification. These data are not easily obtained. Operations within the DOE are unique, and performed by well trained and supervised personnel. It is envisioned that the establishment of a centralized data base that will support these risk assessment as well as other potential applications, may be necessary to achieve the desired results. Failure rate data will eventually be needed in the quantification stage of the risk assessments, both for the basic events depicted in the logic models and for human errors.