MS 0619 Review & Approval (2) JUL 6 1998
Desk, 12690 For DOE/OSTI

SANDIA REPORT

SAND98-1083/1
Unlimited Release
Printed May 1998

SAND--98-1083/1

Committee to Evaluate Sandia's Risk Expertise: Final Report Volume 1: Presentations

RECEIVED
JUL 09 1998
OSTI

Evan C. Dudley

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of
Energy under Contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Prices available from (615) 576-8401, FTS 626-8401

Available to the public from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Rd
Springfield, VA 22161

NTIS price codes
Printed copy: A11
Microfiche copy: A01

SAND--98-1083/1

SAND98-1083/1
Unlimited Release
Printed May 1998

Committee to Evaluate Sandia's Risk Expertise: Final Report
Volume 1: Presentations

Evan C. Dudley
Environmental Systems
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0716

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

Abstract

On July 1-2, 1997, Sandia National Laboratories hosted the External Committee to Evaluate Sandia's Risk Expertise. Under the auspices of SIISRS (Sandia's International Institute for Systematic Risk Studies), Sandia assembled a blue-ribbon panel of experts in the field of risk management to assess our risk programs labs-wide. Panelists were chosen not only for their own expertise, but also for their ability to add balance to the panel as a whole. Presentations were made to the committee on the risk activities at Sandia. In addition, a tour of Sandia's research and development programs in support of the U.S. Nuclear Regulatory Commission was arranged. The panel attended a poster session featuring eight presentations and demonstrations for selected projects. Overviews and viewgraphs from the presentations are included in Volume 1 of this report.

Table of Contents

Committee to Evaluate Sandia's Risk Expertise
Sandia National Laboratories
July 1-2, 1997

Meeting Background and Overview

The FY97 Risk Initiative was a program-development activity in the Energy and Environment sector of Sandia National Laboratories. The Risk Initiative included six primary efforts:

- an external panel to evaluate Sandia's risk-related programs,
- the primary risk-related conference in the High Consequence Engineering Conference Series,
- an expanded and updated edition of *Risk Management at Sandia National Laboratories*,
- maintenance and strengthening of Sandia's International Institute for Systematic Risk Studies (SIISRS),
- a new effort on architectural surety, and
- a new effort on electric grid reliabilty.

On July 1-2, 1997, the Risk Initiative convened a panel of risk experts from around the country to review Sandia's existing programs and future directions and to make suggestions for improvement or disinvestment. This is one of a number of similar panels arising from Executive Vice President John Crawford's initiative to bring in external assessment groups to evaluate a wide variety of technical and administrative programs. The External Risk Committee was chartered under the auspices of Sandia's International Institute for Systematic Risk Studies (SIISRS) to evaluate Sandia's existing risk programs against the following measures:

- fundamental scientific and technical soundness,
- appropriateness at a national laboratory,
- potential to advance the state of the art, and
- relevance to current and emerging national-security issues.

In addition, the Committee recommended specific areas for continuation, enhanced investment, or disinvestment.

Presentations were made to the committee on the risk activities at Sandia. In addition, a tour of selected Sandia research and development (R&D) programs in support of the U.S. Nuclear Regulatory Commission was arranged. The panel attended a poster session featuring eight presentations and demonstrations for selected projects. Overviews and viewgraphs from the presentations are included in Volume 1 of this report.

Selected Presentation Abstracts

Overview of Risk Programs — Nestor Ortiz

The risk-related studies at Sandia National Laboratories entail almost $40M worth of work annually. The scope of the risk-related activities is broad, encompassing eight primary areas: weapons, nuclear reactors, transportation, nuclear waste management, environment and environmental restoration, decision support, architectural surety, and information systems. We primarily do risk research and development as it applies to real problems, and in consequence, the depth of our programs is important. For many risk-related problems, we do basic phenomenological research, data collection, engineering design and analysis, consequence analysis, fundamental research on risk methods, and code development in support of the risk analysis *per se*. We also support the U.S. Department of Energy (DOE), U.S. Nuclear Regulatory Commission (NRC), and other agencies in certification and licensing proceedings. Sandia has advanced the state of the art in several aspects of risk analysis during the past three decades as a result of our work for specific customers (e.g. uncertainty analysis, expert opinions); our current work utilizes and develops past work to solve new problems. New applications of old methods sometimes raise new problems that illuminate the need for fundamentally new risk methods; more often, they require new phenomenological models or data which in and of themselves represent advances on the state of the art.

Because of our project orientation, risk analysts at Sandia have never been collocated in a single organization. Instead, analysts are part of project organizations. To enhance internal coordination of our risk programs and to provide a convenient point of entry for external contacts and customers, we created Sandia's International Institute for Systematic Risk Studies (SIISRS), a virtual center for the risk programs at Sandia. One of our first tasks was to assemble a summary of all the risk activities and the responsible staff. Sandia also assigned a Risk and Reliability research area to be funded as part of the laboratory directed research and development (LDRD) effort. We see risk assessment and management as a key approach in applying our concept of surety to complex systems with potential high consequence impacts.

Weapons **Todd Jones**

Most of the system analysis work accomplished at Sandia has been with high risk, high consequence systems. The genesis of this work began in the nuclear reactor field, and expanded over the years to include risk analyses of robotics systems, nuclear weapons operations, transportation, and dismantlement, as well as terrorist attacks. The emphasis in these analyses has been on comprehensive assessments with a thorough treatment of all of the uncertainties involved. The key to the recent success of Sandia's work relating to nuclear weapons has been the integration of nuclear weapon system physical-response models into the risk analysis using event trees and fault trees in conjunction with first principles. This technique has allowed Sandia to conduct searches for specific abnormal environments in which the safety of the weapon may be compromised, and once these environments have been identified, to make a quantitative estimate of how likely these environments are and how probable it is that the pathways to nuclear detonation or loss of assured safety (LOAS) are achieved. Event trees are used to determine the environments, fault trees to determine the probability of the pathways, and the physical response models to determine the boundary conditions that will cause the system to exceed its physical thresholds.

An increased level of detail has been achieved by developing the physical response models of the system thermally, structurally, and electrically, and generating boundary conditions for the models based on the accident scenario likelihood (e.g., event tree results). These 3-dimensional finite element models are then used to develop temperature and acceleration histories, or electrical threshold levels, which are in turn integrated into the fault trees and event trees to estimate accident likelihoods and probability of occurrence. By applying this detailed level of evaluation to the system, an integrated understanding of the system performance in abnormal conditions, with identification of the major contributors to risk and a full characterization of the key assumptions and the uncertainties in the results can be achieved. This can provide a substantiated basis for making decisions and judgments in managing the risk associated with nuclear weapons.

Nuclear Power Plant PRA **Allen Camp**

Sandia National Laboratories has performed nuclear reactor risk assessments since the mid 1970s, when we participated in the initial Reactor Safety Study. Following that study, Sandia served as lead laboratory for most of the landmark risk assessments performed for the NRC. These studies included several large, full-scope, multiplant risk assessments that advanced the state of the art during their performance. More recent major studies include the 5-plant NUREG-1150 studies and the BWR (boiling water reactor) low power/shutdown studies. A large number of smaller, special purpose studies have been performed along the way to address particular safety issues. In the process of performing these studies, Sandia has developed most of what now represents the state of the art in reactor risk assessment.

Following the Reactor Safety Study, Sandia led the evolution of many Level 1 PRA (probabilistic risk assessment) methods, including treatment of dependent failures, integration of external events on a consistent basis, human reliability analysis, uncertainty analysis, and accompanying software. During the 1980s, Sandia developed a complete set of methods for Level 2 and 3 PRAs, including accident progression event trees, source term models, consequence codes, and processes for integrating the parts of a PRA, including an uncertainty analysis. Software to support these activities has been developed. The advanced methods have been applied to commercial reactor problems for the NRC and also to DOE and space reactor problems.

From the mid 1970s to the late 1980s, work sponsored by the NRC included a balance of methods research and applications. Most application programs included some component of methods development. However, in the early 1990s, there began to be more belief that risk assessment methods were relatively mature, and the focus has shifted much more to applications. There are some notable exceptions to this situation. We are developing a new human reliability approach to treat human errors of commission. We are investigating ways to improve fire PRA methods and are looking at better ways to evaluate the impact of digital instrumentation and control (I&C) systems. However, the larger programs are drawing insights from industry individual plant exams (IPEs) and supporting the development of risk-informed regulation. It is expected that future NRC research programs will be smaller in size and primarily application oriented. Some activities supporting space reactors and other nuclear facilities continue to allow development of improved methods, most notably, development of improved methods to support the Cassini space mission. However, major cutting edge PRA research now tends to come from programs in other fields, such as telecommunications and weapons risk assessment. Much of that development is benefiting from staff with experience at performing reactor PRAs.

Transportation **Sieglinde Neuhauser**

Sandia National Laboratories has been a pioneer in the field of transportation risk assessment since the mid 1970s, when the NRC sponsored the establishment of a transportation program at Sandia. Among the early results of that program were publication of the landmark report, NUREG-0170, "Final Environmental Statement on the Transportation of Radioactive Materials by Air and Other Modes," and concomitant development of the RADTRAN I computer code. NUREG-0170 provided broad coverage for most radioactive materials shipments within the United States for over ten years. Court challenges to the effect that the shipment information was out of date finally removed this umbrella coverage in the late 1980s. Since then, environmental impact statements (EISs) and environmental assessments (EAs) have had to include detailed transportation studies. Sandia is currently doing a NUREG-0170 update and re-validation study for the NRC, using the latest techniques and software.

The DOE took over as sponsor of Sandia's transportation risk program in 1980. Today Sandia (1) produces and maintains state-of]-the-art calculational tools, (2) performs numerous transportation consequence and risk analyses for EISs, EAs, and other studies, (3) validates input parameter values by various means from direct data collection to complex event-tree construction, and (4) provides support to DOE/GC (General Counsel) during litigation of transportation-related lawsuits. The fifth release of the RADTRAN computer code, RADTRAN 5, was made public in beta-test version this spring. The code remains parallel, to the extent possible, with the MACCS (MELCOR Accident Consequence Computational System) code in order to facilitate comparisons of fixed-facility and transportation risks. For example, RADTRAN 5 now contains the same COMIDA2 ingestion model as the latest release of MACCS (MACCS2). An example of an application of RADTRAN is the calculation of risks associated with maritime transport of research-reactor spent fuel for several shipping campaigns; SNL also prepared expert testimony on this subject during litigation concerning certain of these shipments. Related validation studies included collection of time-and-motion data during actual offloading of twelve casks of the research-reactor spent fuel.

Architectural Surety **Dennis Miyoshi**

Architectural surety is a *risk management* approach to providing confidence that structures and facilities will perform in acceptable ways when subjected to normal, abnormal, and malevolent threat environments. The as-built infrastructure is continually at risk because of weathering and aging, infrequent natural hazards such as wind storms, floods and earthquakes, and terrorist or saboteur acts. The risk methods used for our DOE and Nuclear Regulatory Commission customers play a key role in architectural surety for balancing the concerns of reliability, safety, and security in a cost-effective utilization of resources for risk management.

The entire construction life cycle from design through disposal is considered in the architectural surety process. Modeling and simulation techniques are used to form a foundation of knowledge so that the consequences of the threat environments can be fully understood. Security, safety, and reliability principles are developed for the as-built infrastructure so that engineers and architects can develop products where failure mechanisms are understood, predictable, and preventable.

Environmental Risk Analysis **Paul Davis**
Mert Fewell
Ken Sorenson

Sandia's foundation in NRC reactor risk analysis has served as the basis for extending risk analysis methods into the arena of environmental risk analysis. In the 1980's, the NRC, having established a strong reactor risk analysis capability at Sandia, asked us to develop methods for applying risk analysis to the assessment of the performance of geologic nuclear waste repositories. The result was the development of the performance assessment (PA) method that has been applied to various NRC and DOE geologic repository programs. Sandia's PA capabilities, combined with its competencies in geology, hydrology, and geochemistry as applied to the areas of energy technology and environmental impact analyses, have led to an expansion of environmental risk capabilities that have been applied to programs involving decontamination and decommissioning, low-level waste repository PA, National Envivonmental Policy Act risk analyses, and environmental restoration.

Sandia has performed risk assessments for several major NRC and DOE waste repository programs, including the System Prioritization Method (SPM), Yucca Mountain Program, Greater Confinement Disposal, Waste Isolation Pilot Plant, and the Idaho National Engineering & Environmental Laboratory PA. As the funding environment for risk related analysis becomes restricted and uncertain, Sandia has used its experience gained from past programs to implement new, cheaper, and smarter approaches to performing risk analyses. These new approaches can be applied to problems confronting new customers who face difficult decision problems without the budget resources required to undertake major risk programs. Sandia has developed several risk-based decision support tools that can be applied to a range of customers faced with difficult regulatory compliance issues.

Information Systems **Sharon Chapa**

When risk is carried out on a physical system, risk is typically associated with failures under normal, abnormal, and malevolent environments. The risks equate more or less to reliability in a very physical sense, and system reliability can be viewed as the sum-of-the-parts of its physical components. But what is an information system failure, and what are its consequences? For software systems, we view risk very broadly to mean anything that makes the system misbehave, which includes errors in the software logic, unexpected inputs, hardware or network failures, execution glitches, damaged code, bad patches or fixes, sabotage, and all sorts of ill-controlled interactions among parts of the system. In other words, failures stem from a myriad of causes, most of which are poorly characterized. Analysis of failures is complicated by the fact that software is typically complex, both in its internal structure and its sensitivity to its environment. It is important to recognize the model of failure space that is implicit in any risk analysis technique, and to consider whether the problem at hand aligns with that model. In a software-based information system, small changes can produce catastrophically different results, a failure here can have a delayed effect there, and so on. We seek a useful model of the failure space which identifies representative features of systems that can be measured and that have some predictive value for risk. Hand in hand with modeling the failure space is development of math or logic which enables traversal of the space and reasoning about risk.

At the present time, there is no formal Information System Risk Program across Sandia. However, Sandia has long been concerned with such risk, because of the role software plays in many Sandia programs. Sandia-built software analyzes weapons, controls robots, performs 24-hour-per-day situation awareness monitoring, and supports environmental decisions. In addition, Sandia participates in assessments of various software-driven control systems and infrastructures. Information system risk can arise as either project risk or technical risk. Project risk is addressed with such tools as the Software Engineering Institute's assessments, as well as cost and schedule estimators, project management tools, and reviews. Technical risk encompasses the surety elements of the system: reliability, safety, and security. We strive to reduce technical risk by improving best practices and by developing analytic techniques to assess failure probabilities. The latter involves modeling relevant aspects of the software and network failure spaces. This challenging work is currently minimally funded. The bulk of our efforts right now are on improving best practices. Some of the areas currently targeted for improvement are: testing, usability, safety, security, code synthesis, and self-monitoring.

Committee to Evaluate Sandia's Risk Expertise
Agenda
July 1 - 2, 1997
Sandia National Laboratories
Bldg. 823, Rm. 2279

Tuesday, July 1

7:30-8:00 a.m.	Continental Breakfast	
8:00-8:15 a.m.	Welcome and Overview of Sandia National Laboratories' Mission	Dan Hartley, VP, Laboratory Development Division
8:15-8:20 a.m.	Agenda and Logistics	Regina Hunter, Environ. Systems Assessment Dept.; SIISRS
8:20-9:00 a.m.	Announcements • NRC's International Risk Center at Sandia • High Consequence Engineering Conference Series Overview of Risk Programs	Nestor Ortiz, Director, Nuclear Energy Technology Center and SIISRS
9:00-9:15 a.m.	Break	
9:15-11:30 a.m.	Tour of Sandia's R&D Programs in Support of the U.S. Nuclear Regulatory Commission	Mike Hessheimer, International Nuclear Safety Dept.; Ken Reil, Reactor Safety Experiments Dept.
11:30 a.m. - 1:00 p.m.	Lunch Posters and Demos for Selected Projects • High Consequence Engineering • WinR™ (Reliability Analysis Software) • Reactor Risk Assessment at Sandia • Risk and Reliability Assessment for Telecommunications Networks • ARRAMIS (Integrated Risk & Reliability Software) • Cassini Fireball Safety Analysis • Microelectromechanical Systems • KBERT/CONTAIN (Integrated Tool for Facility Safety Hazard Analysis)	823 Breezeway
1:00-1:45 p.m.	Weapons	Todd Jones, Assessment Technologies Dept.
1:45-2:25 p.m.	Nuclear Power Plant PRA	Allen Camp, Risk Assessment & Systems Modeling Dept.
2:25-2:45 p.m.	Uncertainty of Consequence Analysis	Fred Harper, High Consequence Assessment and Technology Dept.
2:45-3:00 p.m.	Break	
3:00-3:45 p.m.	Transportation	Sieglinde Neuhauser, Transportation Systems Analysis Dept.
3:45-4:30 p.m.	Architectural Surety	Dennis Miyoshi, Director, Security Systems And Technology
4:30-5:00 p.m.	Caucus of the Committee	
6:30 p.m.	Dinner	Stephens restaurant

Wednesday, July 2

7:30-8:00 a.m.	Continental Breakfast	
8:00-10:00 a.m.	Environmental Programs: Nuclear Waste Management (WIPP, Yucca Mountain, and GCD); Environment and Environmental Restoration; and Decision Support	
	Risk Methods and Supporting Activities; Decision Support	Paul Davis, Manager, Environmental Risk And Decision Analysis Dept.
	Current Applications	Mert Fewell, WIPP Performance Assessment Code Development Dept.
	Future Applications	Ken Sorenson, Manager, Environmental Risk Assessment & Regulatory Analysis Dept.
10:00-10:15 a.m.	Break	
10:15-11:00 a.m.	Information Systems	Sharon Chapa, Manager, Decision Support Systems Software Engineering Dept.
11:00-11:20 a.m.	Some Future Research Directions	Greg Wyss, Risk Assessment & Systems Modeling Dept.
11:20-11:30 a.m.	Summary	Nestor Ortiz
11:30 a.m.	Leave for Coronado Club	
11:30 a.m.- 1:15 p.m.	Lunch with John Crawford, Executive VP	Coronado Club
1:15-5:00 p.m.	Committee prepares findings	

Panelists and Guests

Panelists:

Dr. B. John Garrick, PLG Inc.
Prof. George Apostolakis, MIT
Dr. Frank Parker, Vanderbilt University
Dr. A. Alan Moghissi, *Technology*
Dr. John Ahearne, Sigma Xi Center
Dr. Rush Inlow, U.S. DOE Albuquerque Operations Office

Guest Observers:

Steven Hamp, National Transportation Program/Albuquerque, DOE/AL
Sam Morris, BNL, representing the DOE Center for Risk Excellence
Mohamed El-Genk, UNM

Guests Representing Affiliates (under MOUs) of SIISRS (Sandia's International Institute for Systematic Risk Studies):

Ahmed Hasan, SNL, representing the Egyptian Atomic Energy Administration
Tito Bonano, BETA Corp. International

Tour of Sandia's R&D Programs in Support of the U.S. Nuclear Regulatory Commission

International Nuclear Safety Department

Mike Hessheimer

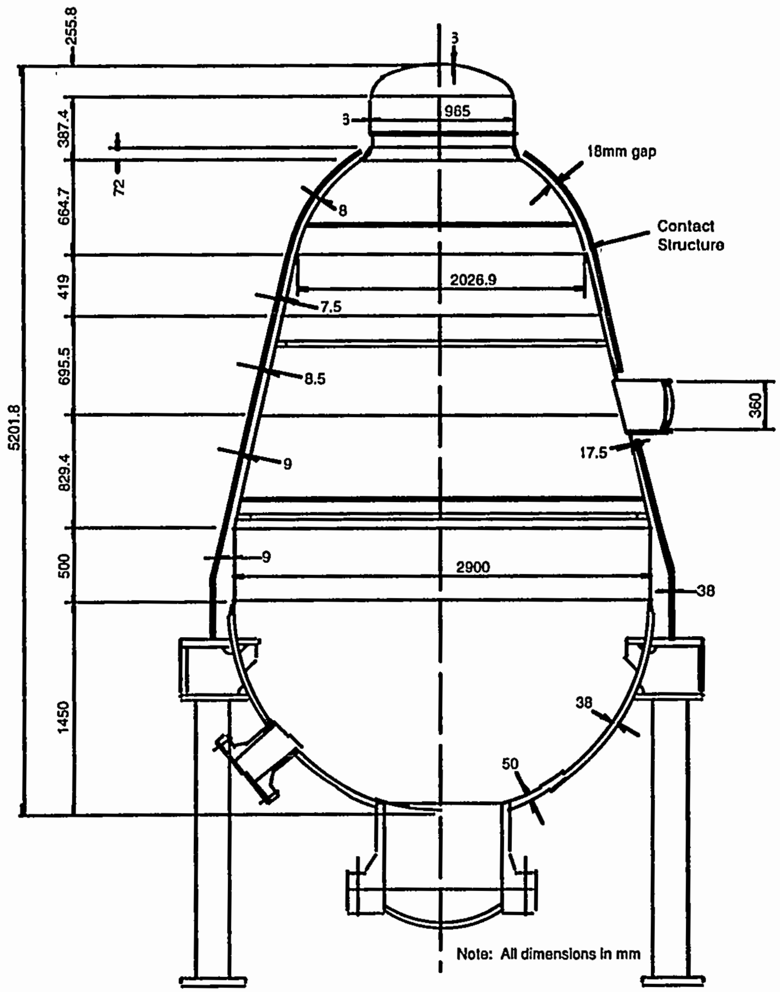
Cooperative Containment Research Program

This program is co-sponsored and jointly funded by the Nuclear Power Engineering Corporation (NUPEC) of Japan and the US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research. The purpose of the program is to investigate the response of representative models of nuclear containment structures to pressure loading beyond the design basis accident and to compare analytical predictions to measured behavior. This will be accomplished by conducting static, pneumatic overpressurization tests of scale models at ambient temperature. The models will be constructed by NUPEC. NUPEC is funding Sandia for planning and site preparation, review of the model design and design support, instrumentation and data collection, and reporting. NUPEC P.o.C .: Dr. Hideo Ogasawara, Director & General Manager, Systems Safety Dept. The NRC is funding Sandia National Laboratories to perform analyses of the models and conduct the tests. NRC P.o.C.: Dr. James F. Costello, RES/DET, Structural and Geological Engineering Branch.

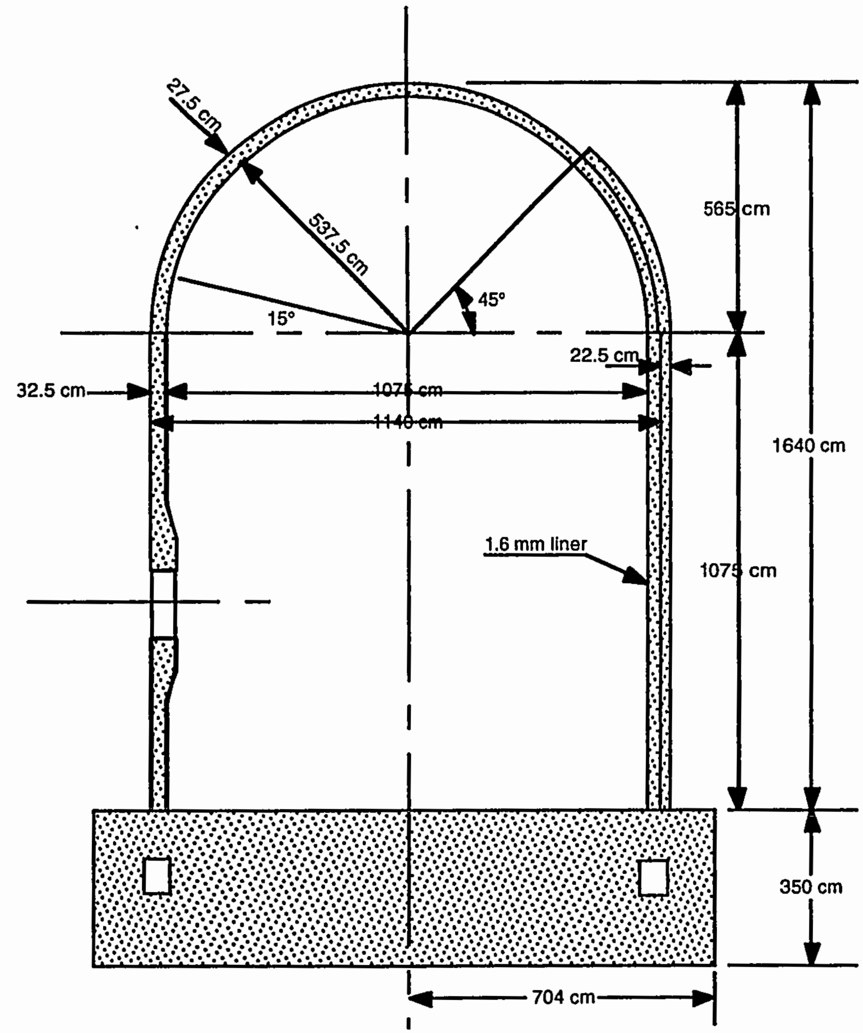
The first test in this program consisted of pressure testing a mixed scale model of a Steel Containment Vessel (SCV). The model is representative of the steel containment for an Improved Mark II Boiling Water Reactor plant. The geometric scale is 1:10. Since the same materials are being used for the model as for the actual plant, the scale on the wall thickness was set at 1:4. The model was fabricated at the Hitachi Works, Japan and transported to Sandia via cargo vessel and truck. The model arrived at Sandia on March 8, 1995 and was installed in the 'Fragment Barrier' structure on March 22, 1995. The Fragment Barrier houses the SCV model during instrumentation and is designed, along with its reinforced roof (which has not been placed), to contain the fragments and safely vent the overpressure from a catastrophic failure of the model at a maximum pressure of 2000 psig. Instrumentation of the model consisted of over 800 channels of data, including strain gages, displacement transducers, temperature sensors as well as visual monitoring. A steel 'Contact Structure' (CS) was placed over the SCV model prior to testing to represent some features of the reactor shield building in the actual plant. The model was expected to come into contact with the CS at approximately 4 to 6 times the design pressure (P_d=113 psig, scaled), resulting in deformation and failure modes which would be more representative of the actual plant. The High Pressure test of the SCV model was conducted on Dec 11 & 12, 1996. The model failed by developing a large tear adjacent to the Equipment Hatch insert at a maximum pressure of 674 psig.

The second test in this program will consist of pressure testing a uniform 1:4-scale model of a Prestressed Concrete Containment Vessel (PCCV). This model is representative of the containment structure of an actual Pressurized Water Reactor plant in Japan. The model will include functional representations of an Equipment Hatch and a Personnel Air Lock as well as smaller penetrations. The model has been designed by Mitsubishi Heavy Industries (MHI) and Obayashi Corporation. The 1.6mm liner was fabricated by MHI in Japan and was shipped to Sandia in segments. On-site construction of the model commenced in early 1997 under the general supervision of Taisei America Corporation and will be completed in 1998. Concurrently, Sandia is installing over 2000 channels of instrumentation on the model consisting of strain gages on the reinforcing steel, prestressing tendons and steel liner, displacement transducers, temperature sensors, pressure sensors, concrete crack transducers as well as visual monitoring. Current plans are for model testing to commence in late 1999 with a series of tests including low pressure tests, design pressure (P_d=57 psig) tests, an Integrated Leak Rate Test (ILRT) at 0.9 P_d, a Structural Integrity Test (SIT) at 1.125 P_d, and, finally, a test to failure to a maximum pressure of approximately 250 psig.

A third test of a uniform 1:4-scale model of a Reinforced Concrete Containment Vessel (RCCV), representative of an Advanced Boiling Water Reactor containment structure, has been discussed with NUPEC. Plans for this test are, however, currently on hold.



Steel Containment Vessel (SCV) Model



Prestressed Concrete Containment Vessel(PCCV) Model

Reactor Safety Experiments Department

Ken Reil

Severe Accident Phenomena/Analyses

Experiment Facilities

Sandia National Laboratories
Albuquerque, New Mexico

14

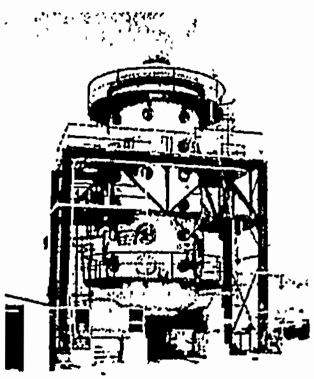
For further information, contact:
Kenneth O. Reil
Sandia National Laboratories, MS-1139
Albuquerque, NM 87185-1139
Phone: (505 845-3050
e-mail: koreil@sandia.gov

Sandia National Laboratories

Severe Accident Phenomena/Analyses

Many Years of Reactor Safety Research For USNRC

15 Annular Core Research Reactor (ACRR)



Surtsey Test Facility

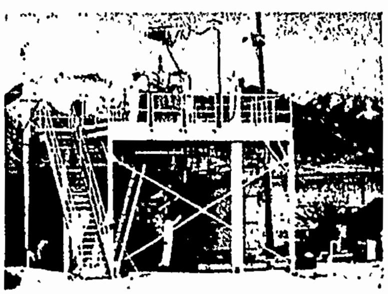
- SNL Severe Accident Research for NRC Started in 1974
- Work Has Evolved to Meet Needs
  - LMFBR
  - LWR
  - ALWR
- Activities Include
  - Experiments (In-Pile and Out-of-Pile)
  - Model Development
  - Code Development
  - Analyses
  - Issue Resolution

Severe Accident Phenomena/Analyses

Experimental Studies Coupled to Analytical Modeling and Code Development. Main Project Areas:


0.20 s

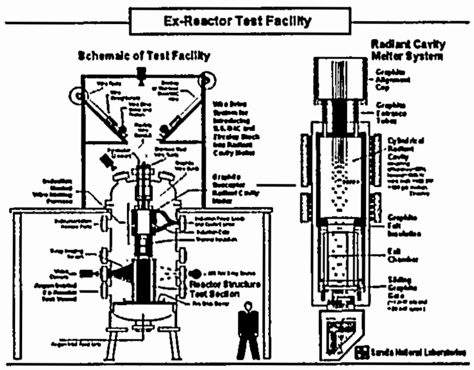
Steam Explosion


Large Melt Facility (LMF)

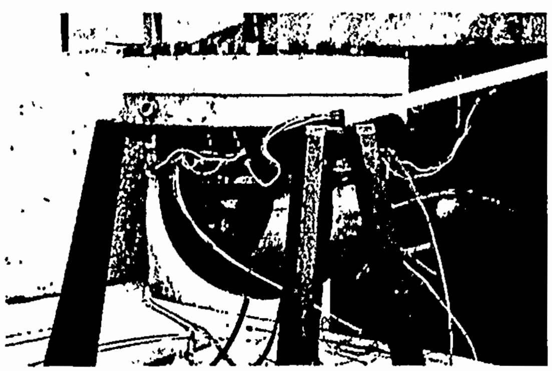
- Irradiated Fuel Behavior
- Accident Energetics (LMFBR)
- Debris Coolability
- Fuel Coolant Interactions (Steam Explosions)
- Hydrogen Combustion and Detonation
- Sodium Concrete Interactions
- Core Concrete Interactions
- Aerosol Behavior
- Fission Product Release
- Core Melt Progression
- Ex-Vessel Cooling

Severe Accident Phenomena/Analyses

Integrate Experiments, Analyses, and Codes in a Probabilistic Framework to Provide a Basis for Risk Informed Regulatory Actions



Ex-Reactor (XR) Experiment



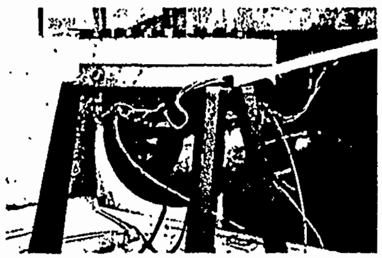
Lower Head Failure Test

- Direct Containment Heating
  - Testing in NPP Geometries
  - Issue Resolution Process
- Hydrogen Mitigation
  - Hydrogen Ignitors
  - Passive Autocatalytic Recombiners
- Lower Head Failure
  - Tests to Failure of Scaled Vessels
  - Model Assessment
- In-vessel Melt Progression
  - Ex-Reactor Experiments (BWRs)
  - PHEBUS Experiment Program
- Fission Product Source Term
  - PHEBUS Experiment Program

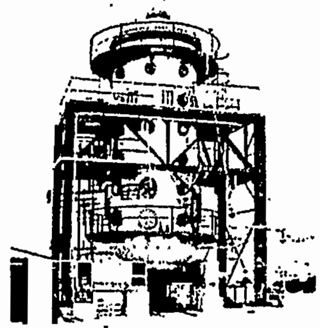
Severe Accident Phenomena/Analyses

SNL Has Utilized, Adapted, and Constructed a Variety of Facilities for Severe Accident Phenomenological Research. Some are Currently Active; Others are Idle.

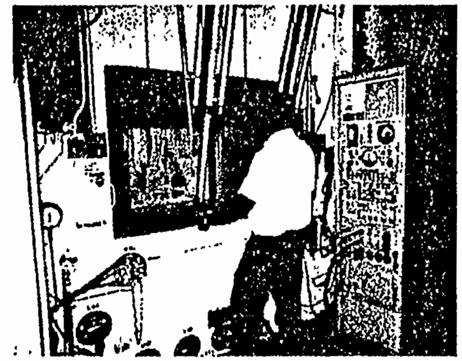
Annular Core Research Reactor (ACRR)



Lower Head Failure Test at Explosive Dynamics Laboratory

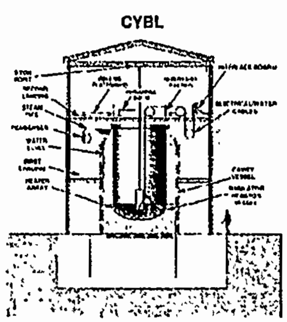


Surtsey Test Facility

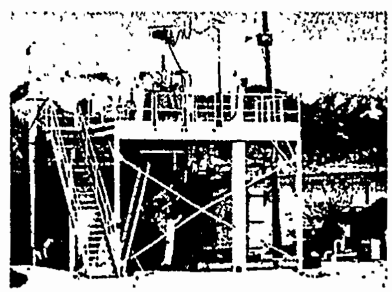


Hot Cell Facility

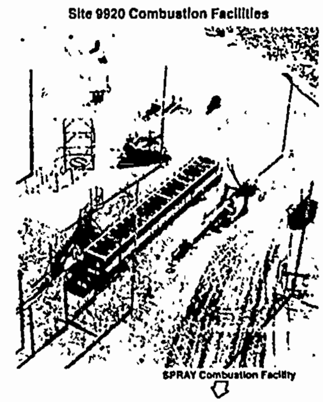
Containment Technology Test Facility (CTTF)



CYBL Facility



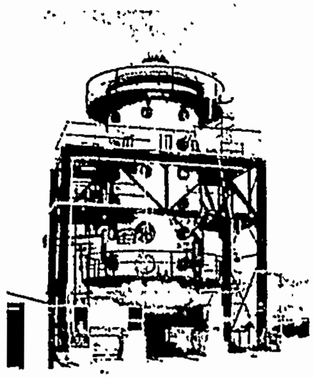
Large Melt Facility (LMF)



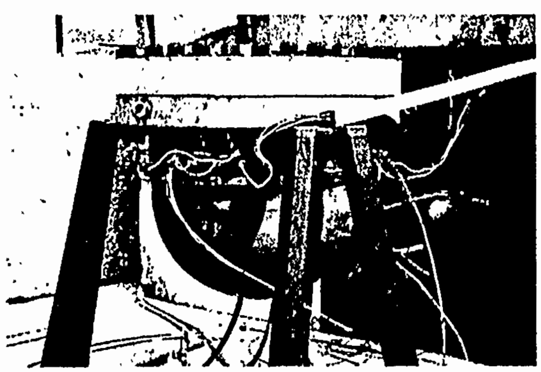
Explosive Firing Site

Severe Accident Phenomena/Analyses

Current Status of Severe Accident Test Facilities



Surtsey Test Facility

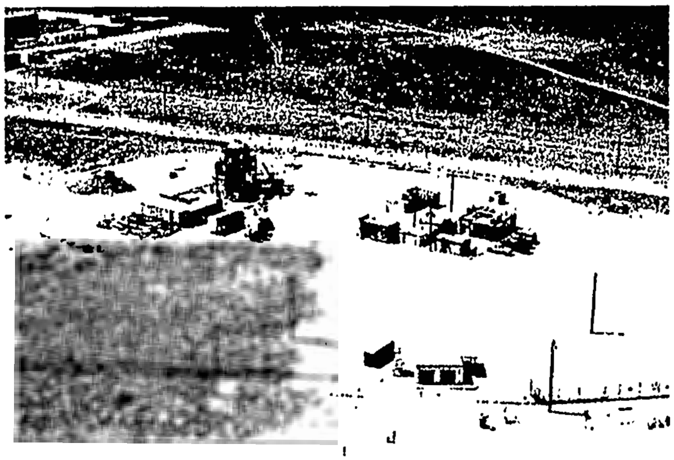


Lower Head Failure Test at Explosive Dynamics Laboratory

- Active Facilities Supporting LWR Research
  - Surtsey Facility
  - Explosive Dynamics Laboratory
- Active Facilities Supporting Other Activities
  - Annular Core Research Reactor (ACRR)
  - Hot Cell Facility (HCF)
  - Explosive Firing Site
- Facilities in Standby (Idle)
  - Cylindrical Boiling Facility (CYBL)
  - Containment Technology Test Facility (CTTF)
  - Large Melt Facility (LMF)

Severe Accident Phenomena/Analyses

Surtsey Facility is a Large Sealed Pressure Vessel for Studying Containment Atmosphere Processes

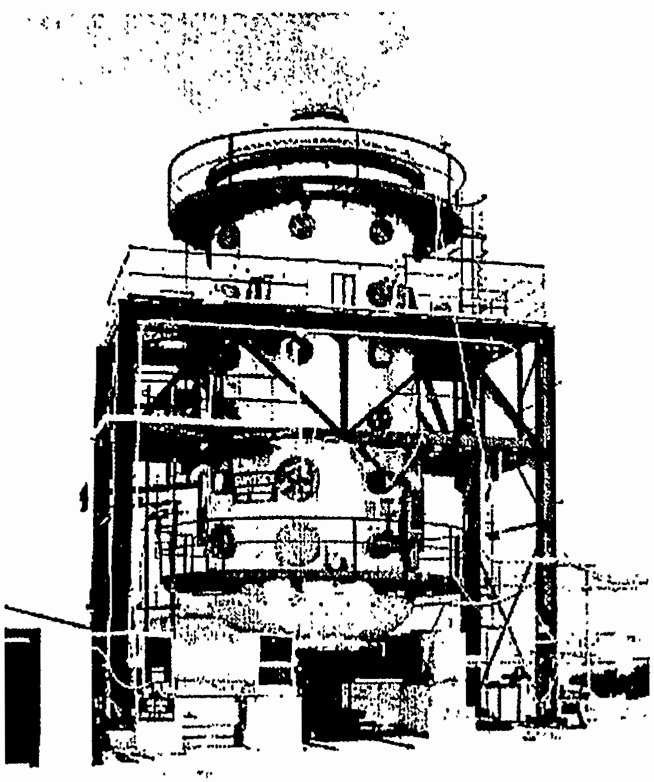


Surtsey Test Site

- 100 m^3 ASME Steel Pressure Vessel
- 1 MPa Working Pressure
- Insulated - Prototypic Steam/Air/H_2 Atmosphere
- Realistic Scaled Containment Structures (1/10th Scale)
- Removable Upper/Lower Heads
- Instrumentation Ports At Six Levels
- High Volume Gas and Steam Supply Systems
- Flexible Data Acquisition and Control

Severe Accident Phenomena/Analyses

Surtsey Facility



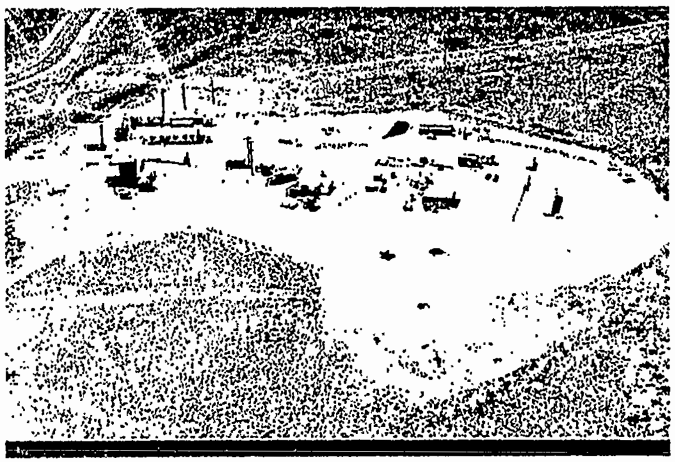
Surtsey Test Facility

- Studies of Containment Atmosphere Processes at Relatively Large Scale
- Direct Containment Heating Resulting from High Pressure Melt Ejection in Scaled NPP Geometries
- Steam Explosion Phenomena in Reactor Cavities
- Behavior of Hydrogen Ignitors in Condensing Steam Environments
- Performance Characteristics of Passive Autocatalytic Hydrogen Recombiners in Prototypic Hydrogen, Air, Steam Environments

Sandia National Laboratories

Severe Accident Phenomena/Analyses

The Explosive Dynamics Laboratory is a General Purpose Facility for Remote Testing of Systems Involving High Temperature, Reactive, or Energetic Materials with the Potential for Release of Significant Energy.

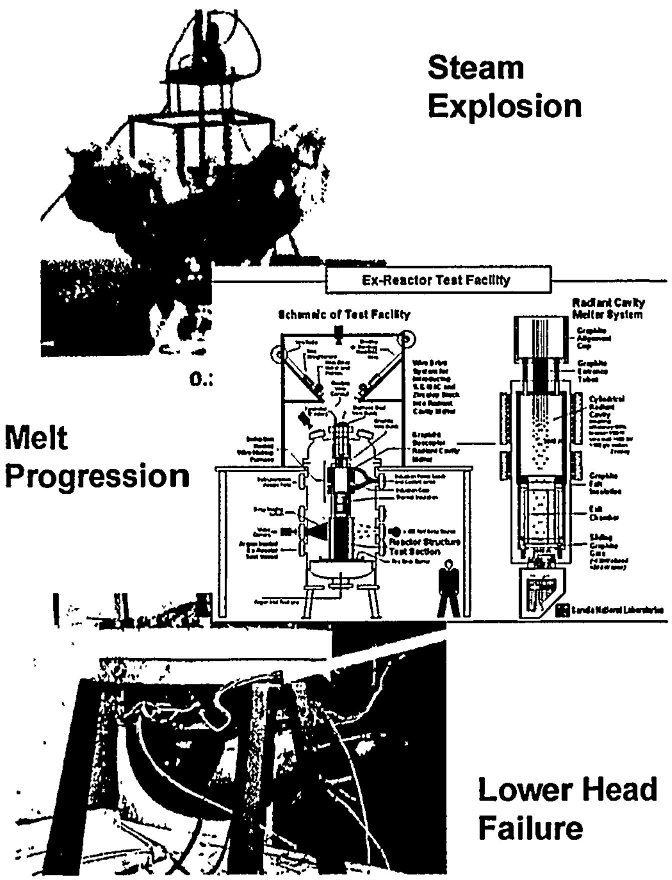


Explosive Dynamics Laboratory

- Remote Operations
- Capacity - 10 Pound TNT Equivalent
- Facilities
  - Open Test Pads
  - Closed Test Cell
  - FITS Vessel (5m^3 Volume - 2 MPa working pressure)
  - VAT Facility (Open Water Tank - 50,000 Gal)
  - Induction Power Supplies
  - High Pressure Gas Systems
  - Flexible Data Acquisition and Control

Explosive Dynamics Laboratory

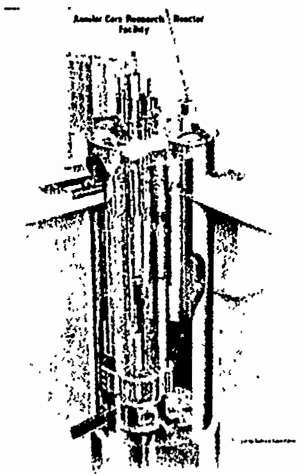
Facilities at the Explosive Dynamics Laboratories Have Been Used for A Wide Variety of Studies



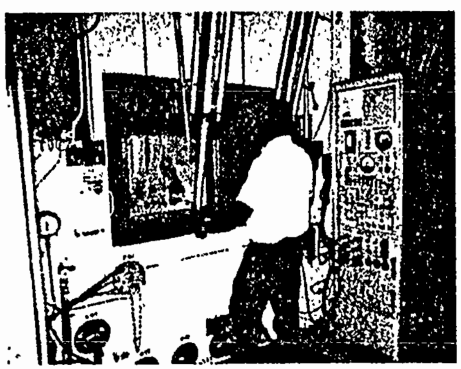
- Fuel - Coolant Interactions (FCI) or Steam Explosions
  - Thermite, UO_2, or Aluminum in Water
- Hydrogen Combustion
- BWR Melt Progression
  - Ex-Reactor (XR) Experiments
  - Relocation of Molten Core Materials
- Lower Head Failure
  - ~One-Fifth Scale, Reactor Vessel Lower Heads Tested to Failure Under Prototypic Heating and Pressure Conditions

Severe Accident Phenomena/Analyses

Annular Core Research Reactor (ACRR)
Hot Cell Facility (HCF)



Annular Core Research Reactor (ACRR)

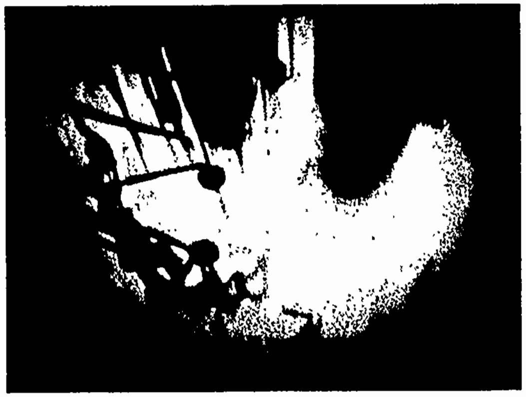


Hot Cell Facility

- ACRR
  - Pool Type Reactor with Dry Central Experiment Cavity (.23m Dia) and Dry External Cavities (up to .51m Dia)
  - Operates in Pulse, Steady State, and Programmed Transient Modes
- HCF
  - Heavily Shielded Canyon and Glove Boxes (up to 50,000 Ci FPs)
  - Fuel Preparation, Experiment Assembly, Post-Irradiation Exams
- Uses
  - LWR Melt Progression (DF, MP), Fission Product Release (ST), Debris Coolability (DCC), LMFBR & Space Reactor Fuel Behavior
  - Weapons Effect Simulation
  - Isotope Production

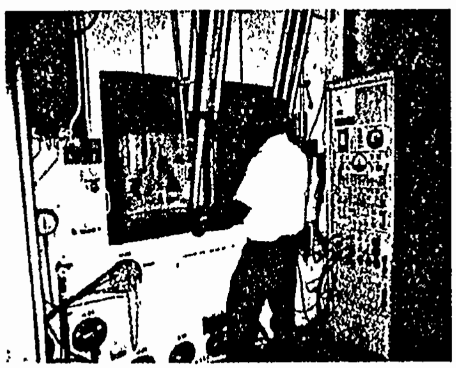
Severe Accident Phenomena/Analyses

In-pile Testing Experience



25

Annular Core Research Reactor (ACRR)



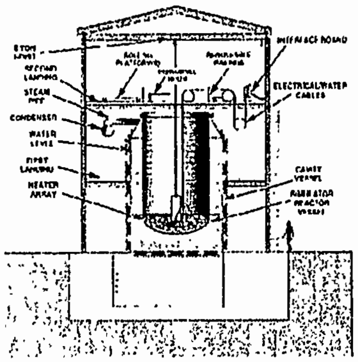
Hot Cell Facility

- Annular Core Research Reactor (ACRR) and Hot Cell Facility (HCF)
- Hundreds of Safety and Development Tests
- LMFBR, LWR, HWR, ACRR Fuel Development, Space Propulsion
- Studies in Many Areas
  - Fuel Behavior
  - Accident Energetics
  - Debris Coolability
  - Core Melt Progression
  - Fission Product Release
  - Performance Characteristics
- Facilities Currently Devoted to the Production of ^{99}Molybdenum

Severe Accident Phenomena/Analyses

CYBL Facility and Containment Technology Test Facility

CYBL



CYBL Facility

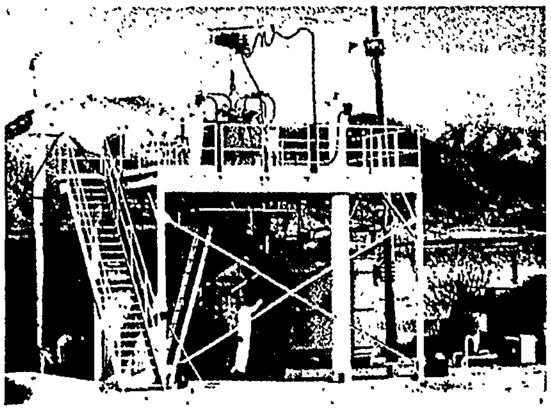
Containment Technology Test Facility (CTTF)

- CYBL Facility
  - Full Scale Representation of AP600 RPV in a Flooded Reactor Cavity ("Tank within Tank")
  - Internal Radiant Heating to Simulate Heat Transfer from Molten Pool
  - Characterize Downward Facing Boiling Heat Transfer from Vessel to Pool for Invessel Core Retention
- Containment Technology Test Facility
  - 250 m^3 Volume - 1/6th Scale - Surry NPP Reinforced Concrete Containment
  - 1 MPa Failure Pressure
  - DCH and Hydrogen Behavior Studies Similar to Surtsey; i.e. Prototypic Atmosphere and Structures

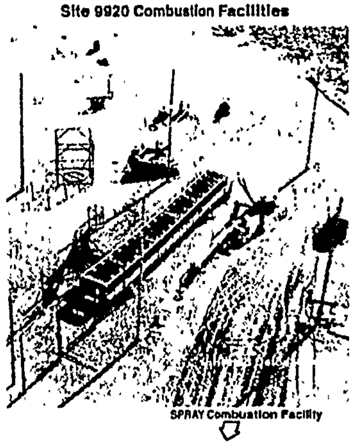
Sandia National Laboratories

Severe Accident Phenomena/Analyses

Large Melt Facility and Explosive Firing Site



Large Melt Facility (LMF)



Explosive Firing Site (9920)

- Large Melt Facility (LMF)
  - Inductively Melt and Sustain 200kg of Metallic or Prototypic UO_2 Core Debris (13m^3 Containment Chamber, 280kW 100Hz Inductive Power Supply)
  - Core/Concrete Interactions (Metallic and Oxidic Melts) w/ & w/o Water
- Explosive Firing Site (9920)
  - Remote Explosive Test Site
  - Open Test Pads, 5 m^3 Pressure Vessels, .5m Dia x 13 m Long Heated Detonation Tube, FLAME Facility (Full Scale Ice Condenser Basket Room)
  - Hydrogen Combustion, Detonation, and Transition to Detonation
  - General Explosive Testing (100lb equiv.)

VIEWGRAPH PRESENTATIONS

Welcome and Overview of SNL's Mission

Dan Hartley, VP

Laboratory Development Division

Sandia National Laboratories Overview

Presented to

The Committee to Evaluate Sandia's Risk Expertise

Dr. B. John Garrick, PLG Inc.

Prof. George Apostolakis, MIT

Dr. Frank Parker, Vanderbilt University

Dr. A. Alan Moghissi, *Technology*

Dr. John Ahearne, Sigma Xi Center

Dr. Rush Inlow, U. S. DOE Albuquerque Operations Office

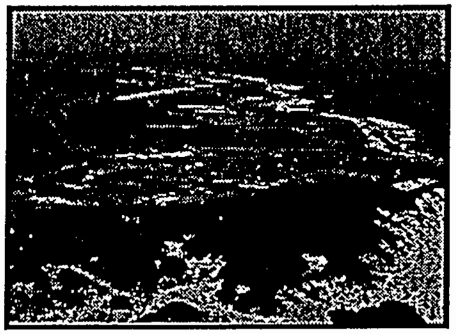
Dan Hartley, Vice President

July 1, 1997

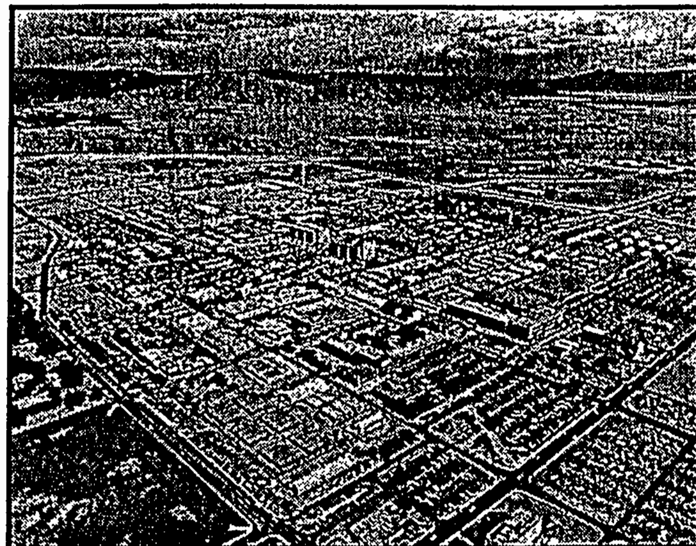
Sandia National Laboratories


Sandia
National
Laboratories
LOCKHEED MARTIN
Sandia is a Multiprogram Laboratory
Operated by Sandia Corporation,
a Lockheed Martin Company,
for the United States Department of Energy
Under Contract DE-AC04-94AL85000.
Eagle.FIC.OV(Rev) 1

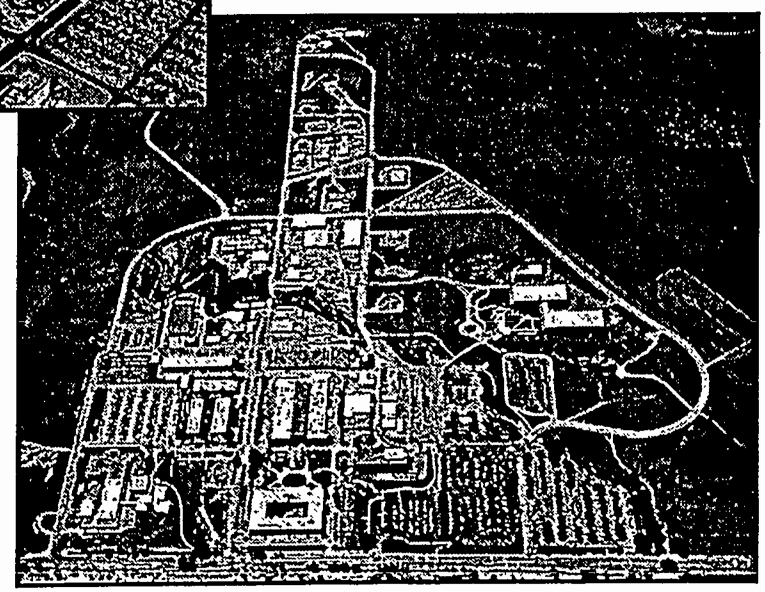
Sandia National Laboratories sites



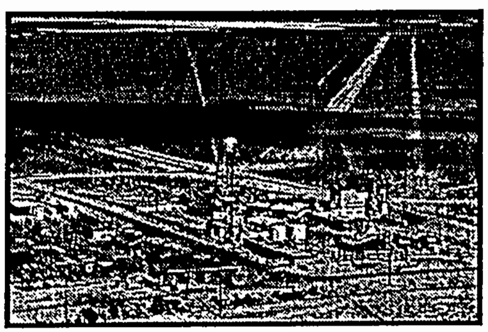
Kauai Test Facility, Hawaii



Albuquerque, New Mexico



Livermore, California

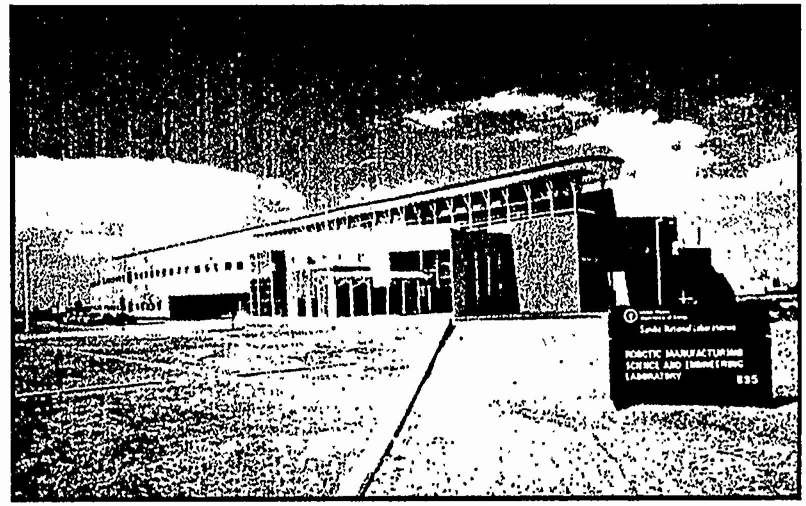


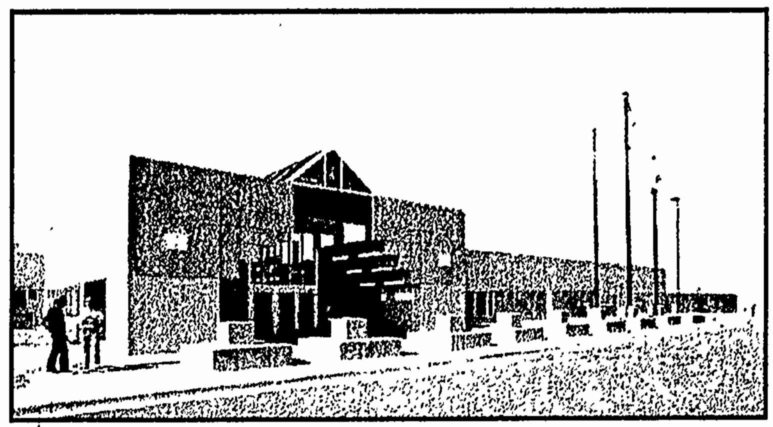
Tonopah Test Range, Nevada

Sandia National Laboratories

Sandia — in round numbers

- 8000 full-time employees
  - ~7,000 in New Mexico
  - ~1,000 in California
- 600 buildings, 5M square feet
- 1,400 Ph.D.s, 1,700 Masters
  - 55% engineering
  - 33% science and mathematics
  - 12% computing and other
- Annual budget $1,300M

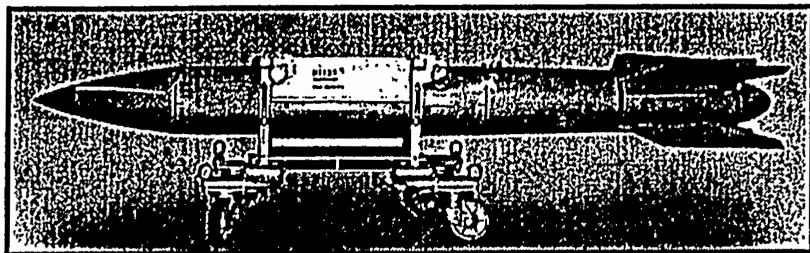




Sandia National Laboratories

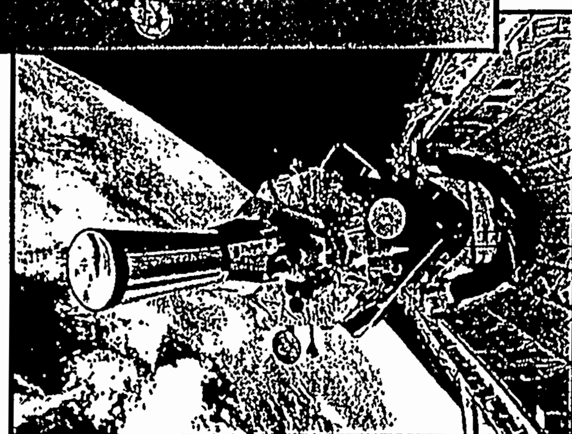
T370 CP8945.02

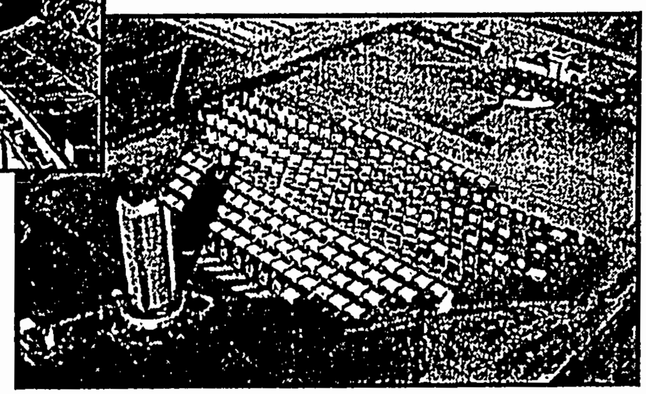
Sandia's missions support national security



Our primary mission is stewardship of our nation's nuclear weapons stockpile – from development to dismantlement

We also perform certain derived activities stemming from our nuclear weapons mission (arms control, clean-up, etc.)

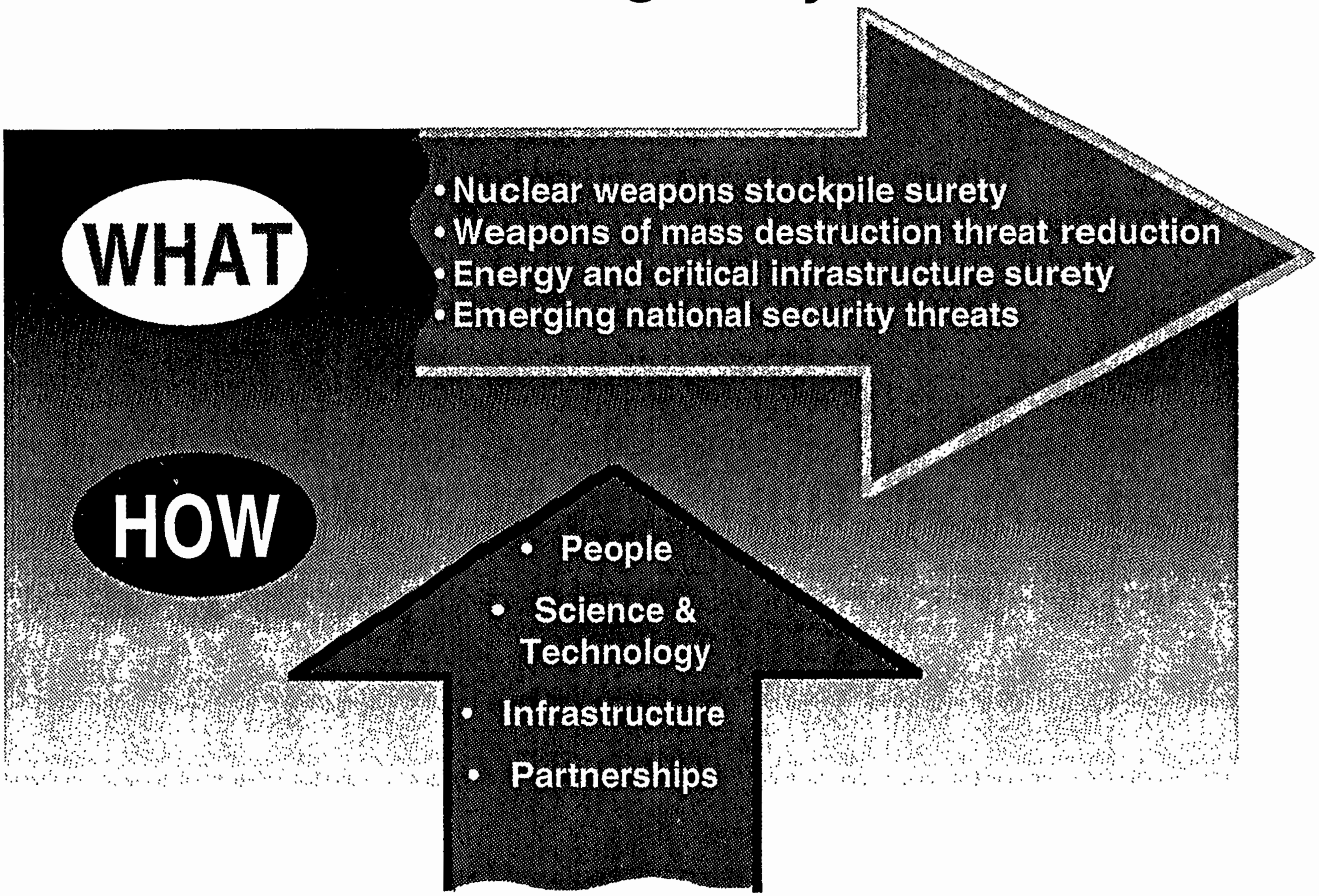




And we have a shared mission with other DOE laboratories in energy research and development

Sandia National Laboratories

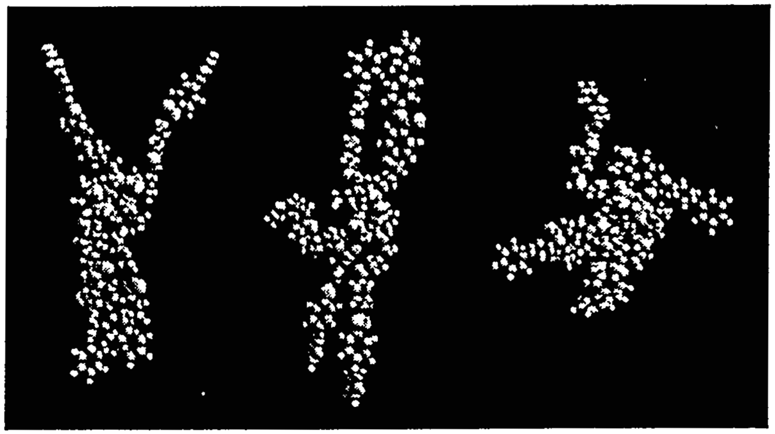
Sandia's Strategic Objectives



4200 Comm- JAZ2-97- PartDev prc1

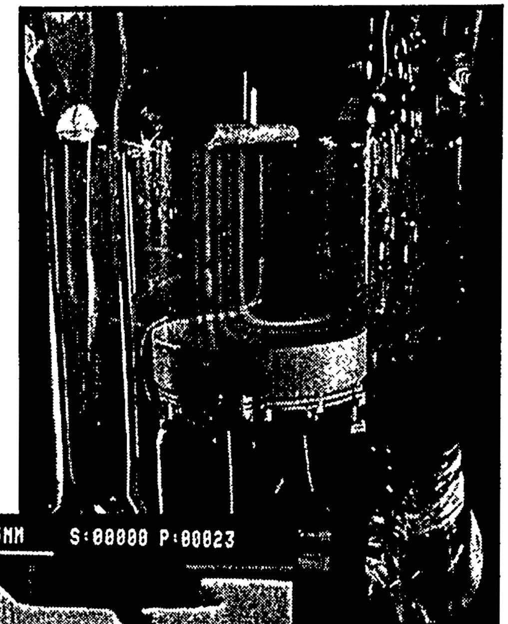
Sandia National Laboratories

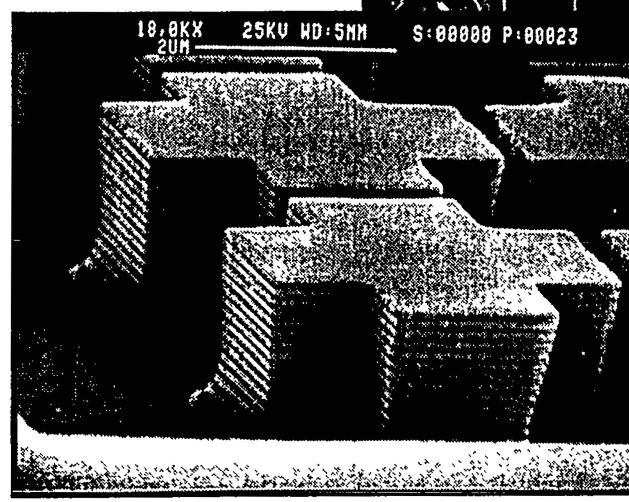
Sandia's research foundations are the fundamental basis of its core competencies



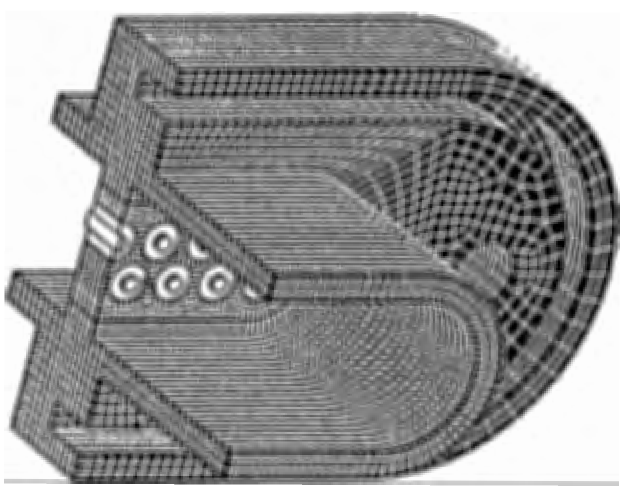
Computational and information sciences

Engineered processes and materials





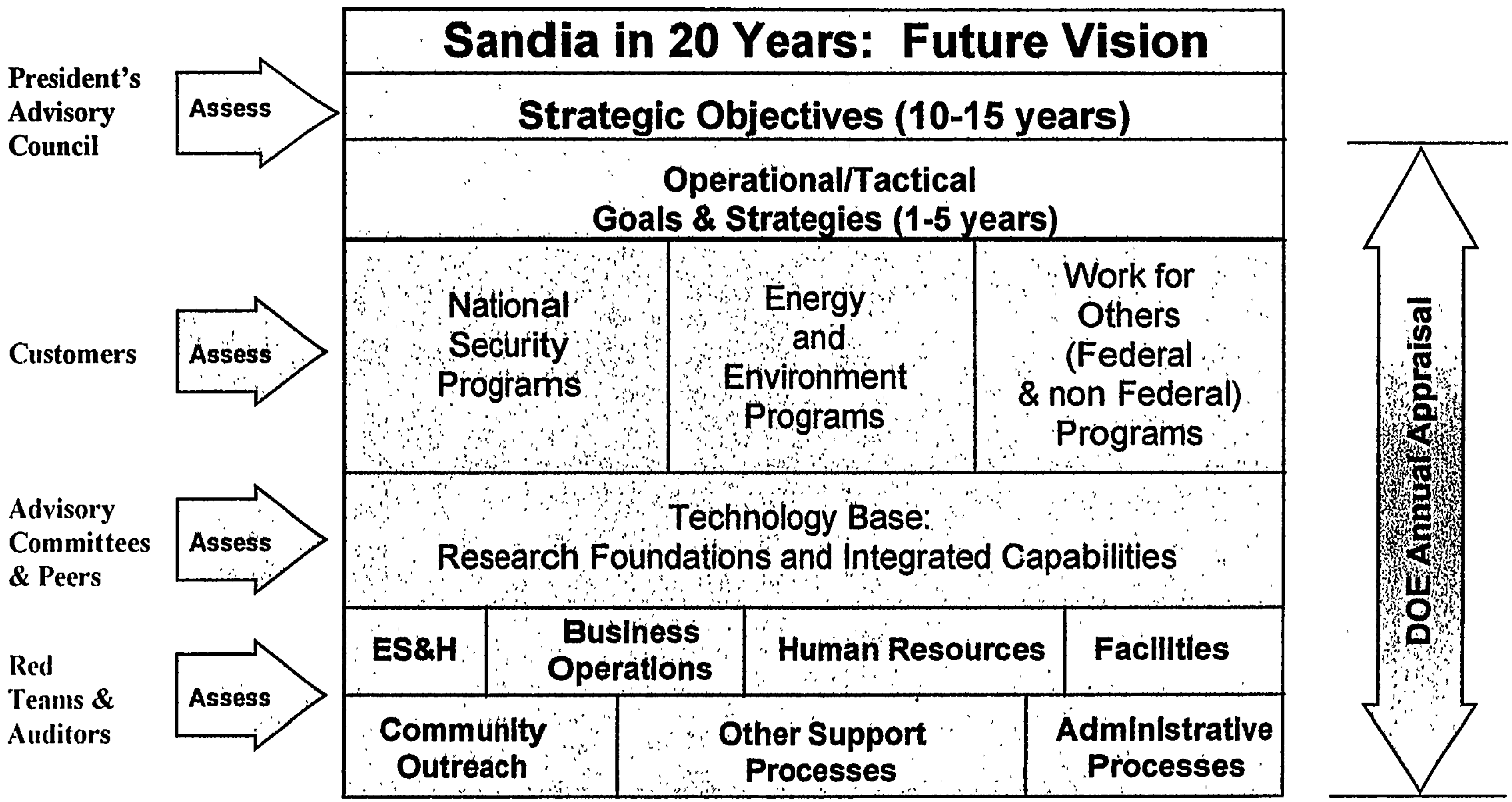
Engineering sciences



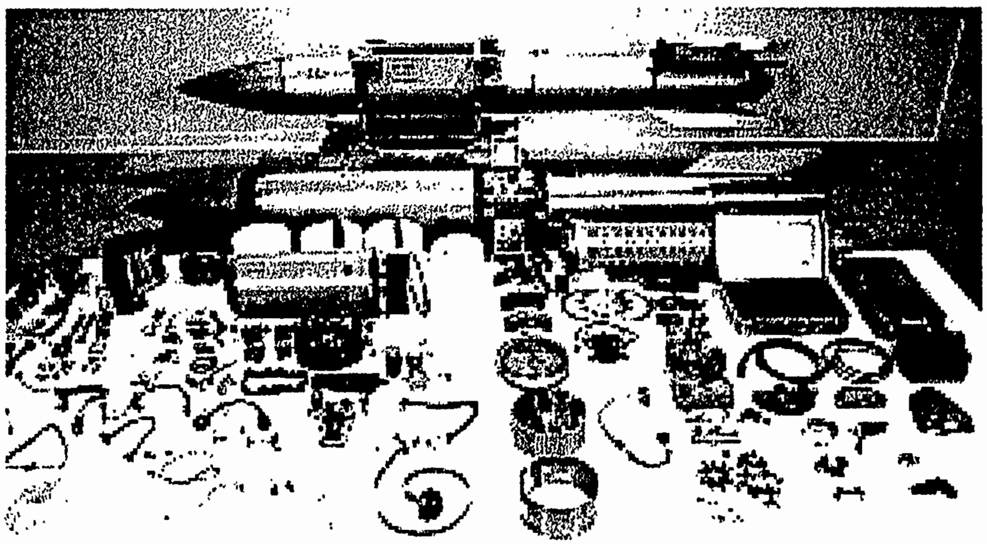
Microelectronics and photonics research

Sandia National Laboratories

Sandia's Corporate planning efforts involve a Plan / Do / Check cycle



Sandia Designs, Develops, and Qualifies a Wide Range of Products



Sandia has Responsibility for:

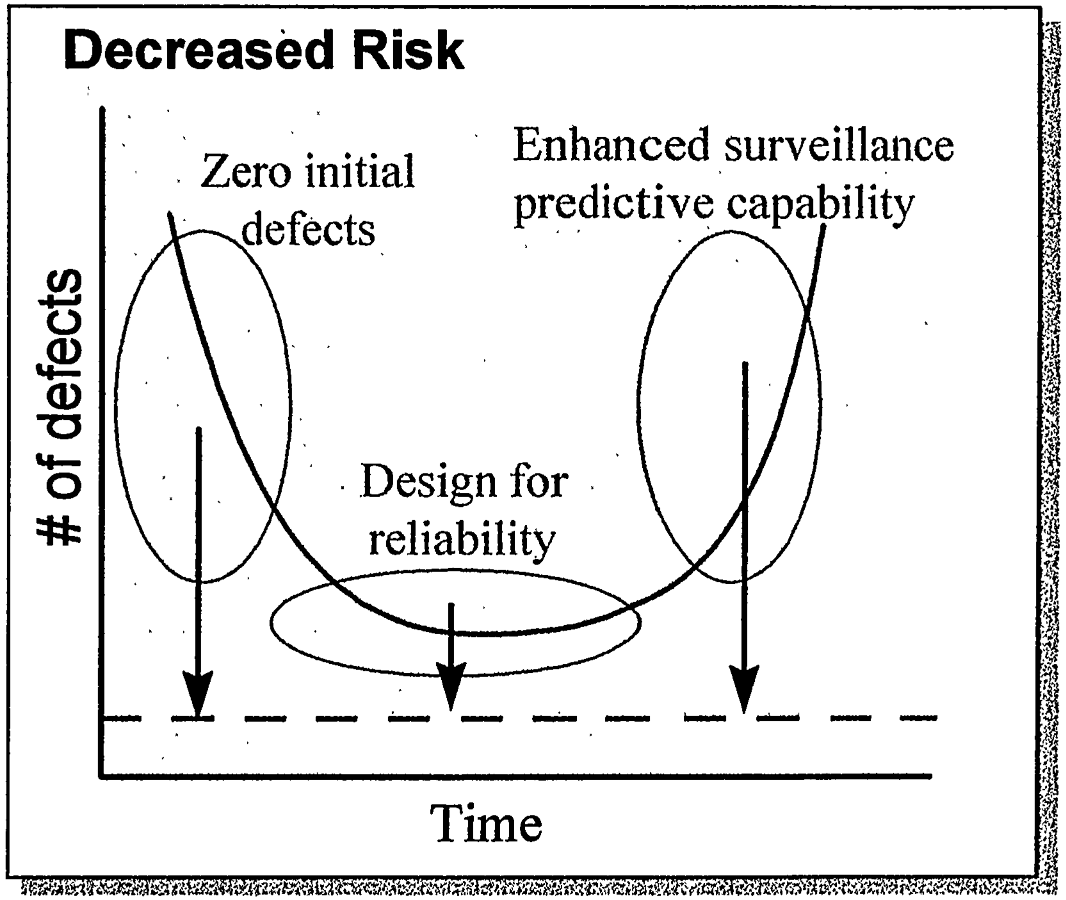
- Electronic components
- Use control components
- Energetic components
- Power storage
- Neutron generators
- Gas transfer systems
- Radars
- Firing sets
- Joint test assemblies
- Parachutes
- Cables & connectors
- Mechanical components
- Handling gear
- Test gear
- Software

Sandia National Laboratories

The Compelling Need
Our Nuclear Deterrent depends upon the stockpile which cannot be put at risk!

Increased Risk

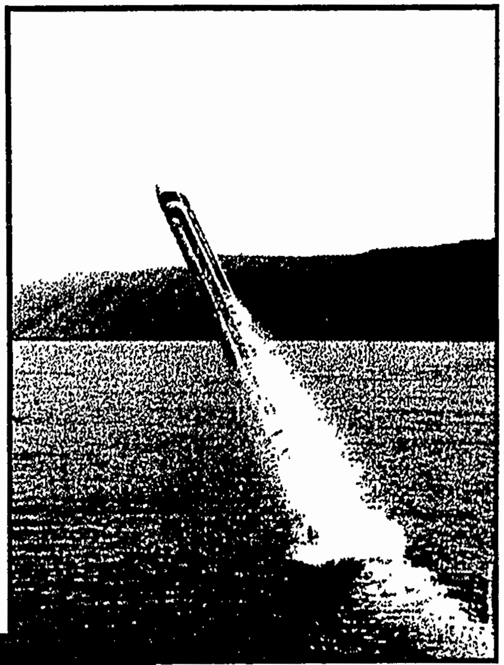
- No new systems
- Aging, smaller, less diverse stockpile
- Greatly reduced design and production capacity
- Reduced budget

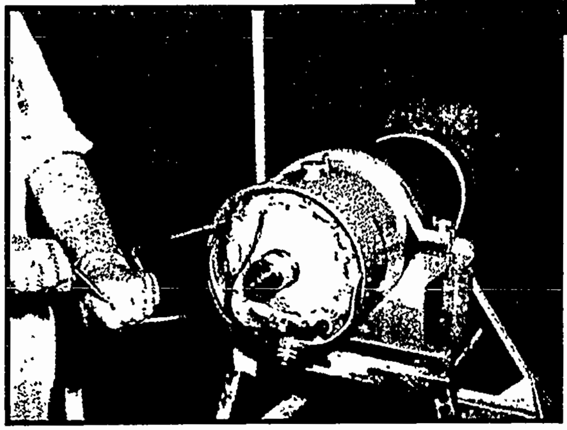


Sandia National Laboratories

Sandia's missions emphasize national security (broadly defined)

- *Primary mission:* design and development of nonnuclear portion of US nuclear weapons
- *Systems integrator:* safety, security, use control
- *Energy & environmental research:* utilization, alternate sources
- *Arms control:* verification, non-proliferation and counterproliferation
- *Nonnuclear defense technologies:* countering WMD
- *Foreign technology assessments*





Sandia National Laboratories

T370 CP8945.05

Announcements

NRC's International Risk Center at Sandia

High Consequence Engineering Conference Series

Overview of Risk Programs

Nestor Ortiz, Director
Nuclear Energy Technology Center and SIISRS

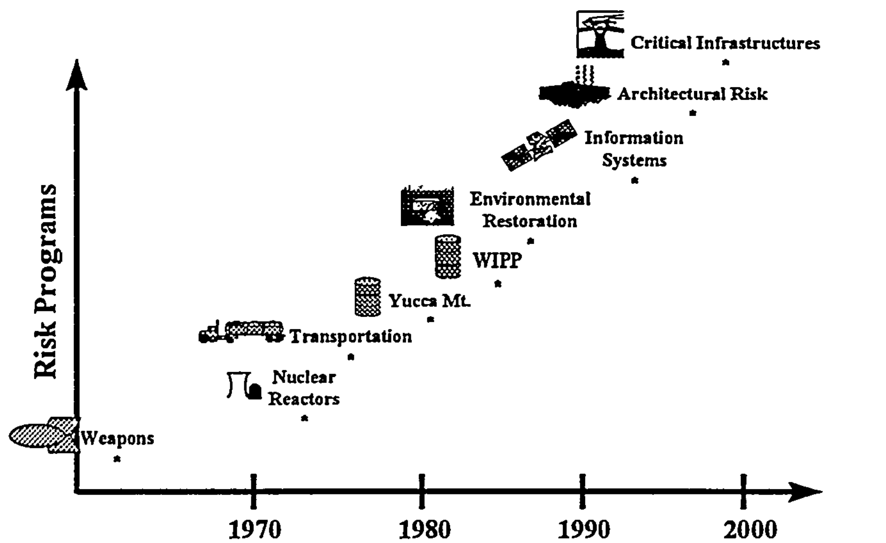
Nestor R. Ortiz, Director
Nuclear Energy Technology Center

Sandia's Risk Expertise Meeting
Albuquerque, New Mexico

July 1-2, 1997

Sandia National Laboratories

Chronology of Risk Programs



Sandia National Laboratories

6400-97D-121A.ppt

6/26/97

The phrase "Risk Assessment and Management" has a broad definition at SNL

It encompasses as many as five activities:

1. **Identification of the hazards.**

2. **Determination of the risks of those hazards.**

3. **Reduction of the risks to acceptable levels.**

4. **Thorough documentation of Activities 1 through 3.**

5. **Continuing reevaluation in order to improve the system or solution.**

Sandia National Laboratories

6400-97D-121B.ppt

6/26/97

Risk: The right tool for the right job

Selected Risk Tools *	Major Steps in Risk Assessment			
	Hazards Analysis	Scenario Development	Scenario Quantification	Analysis of Results
Human Factors	X			
Fault Tree				
Event Tree		X		
Data Evaluation			X	
Phenomenological Modeling			X	
Cost/Benefit				
Decision Support				
Regulatory/Certification Support				X

*Not a complete list.

Sandia National Laboratories

6400-97D-121C.ppt 6/26/97

Surety Definition

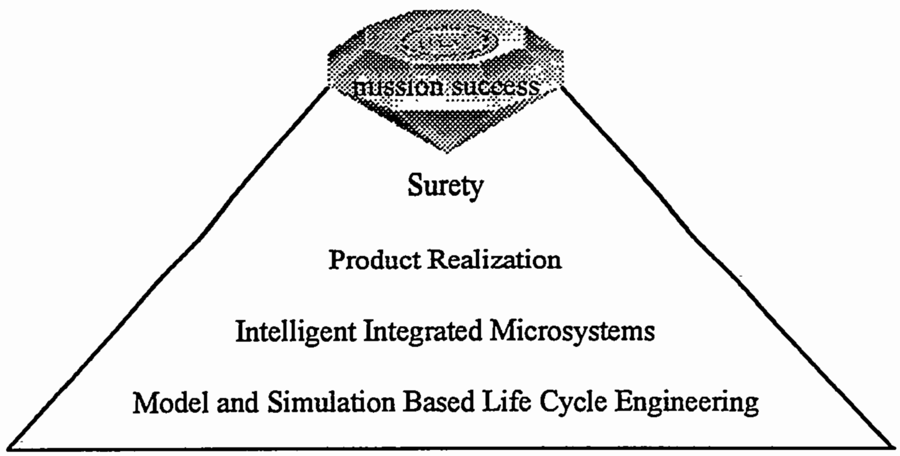
"Surety is confidence that a system will perform in acceptable ways under normal, abnormal, and malevolent environments."

To address system performance under the different environments, Sandia National Laboratories uses systems engineering and risk assessment and management capabilities.

Sandia National Laboratories

6400-97D-121D.ppt 6/26/97

Sandia's Key Science and Technology Areas



Sandia National Laboratories

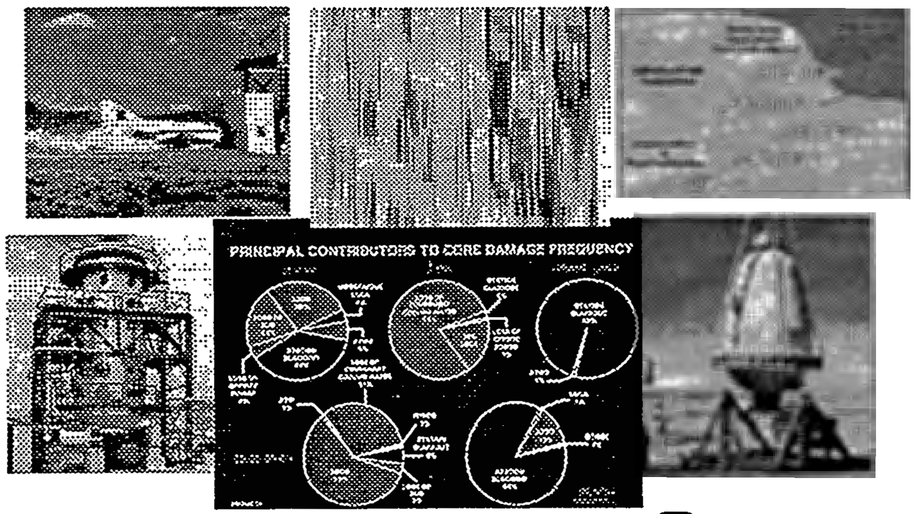
What information do we need from the panel?

The panel's impressions on

- **Scientific and Technical Soundness of the risk methodology and technology for each program area (e.g. Weapons, Nuclear Reactors, Transportation, Waste Management and Environment and Environmental Restoration).**
- **Recommendations of "risk technology advances" for the future. (Does the panel have different suggestions?)**
- **Relevance of the recommended "risk technology advances" to current and emerging national security issues. (Does the panel see major technology gaps?)**
- **Appropriateness of the risk work as it supports Sandia National Laboratories' Mission.**

Sandia National Laboratories

Risk Technology



Sandia National Laboratories

6400-97D-1210.ppt

6/26/97

Sandia has advanced the state of the art in risk analysis

- *Weapons:* We created an algorithm to search a parameter space to identify regions of vulnerability.
- *Nuclear Power Plant PRA:* Much of the current state of the art was developed at Sandia, e.g., large fault trees, integrated treatment of dependent failures and of external events, parametric source term models, and probabilistic phenomenological models.
- *Uncertainty of Consequence Analysis:* We have improved methods for inverse modeling and expert elicitation, and we separated stochastic uncertainty from state-of-knowledge uncertainty in an integrated uncertainty calculation.
- *Transportation:* RADTRAN was the first transportation risk-assessment code, in 1977, and it was the first risk-assessment code available on the Internet, in 1985.
- *Architectural Surety:* We are applying existing capabilities to provide a foundation for decisions about mission, environment, and public confidence for as-built infrastructure.
- *Environmental Programs:* Sandia has created and applied probabilistic risk assessment methods to waste management and extended these methods to environmental restoration, and we submitted the first application for certification of a nuclear waste repository.
- *Information Systems:* We are advancing the state of the art in modeling for surety analysis and for networks.

Sandia National Laboratories

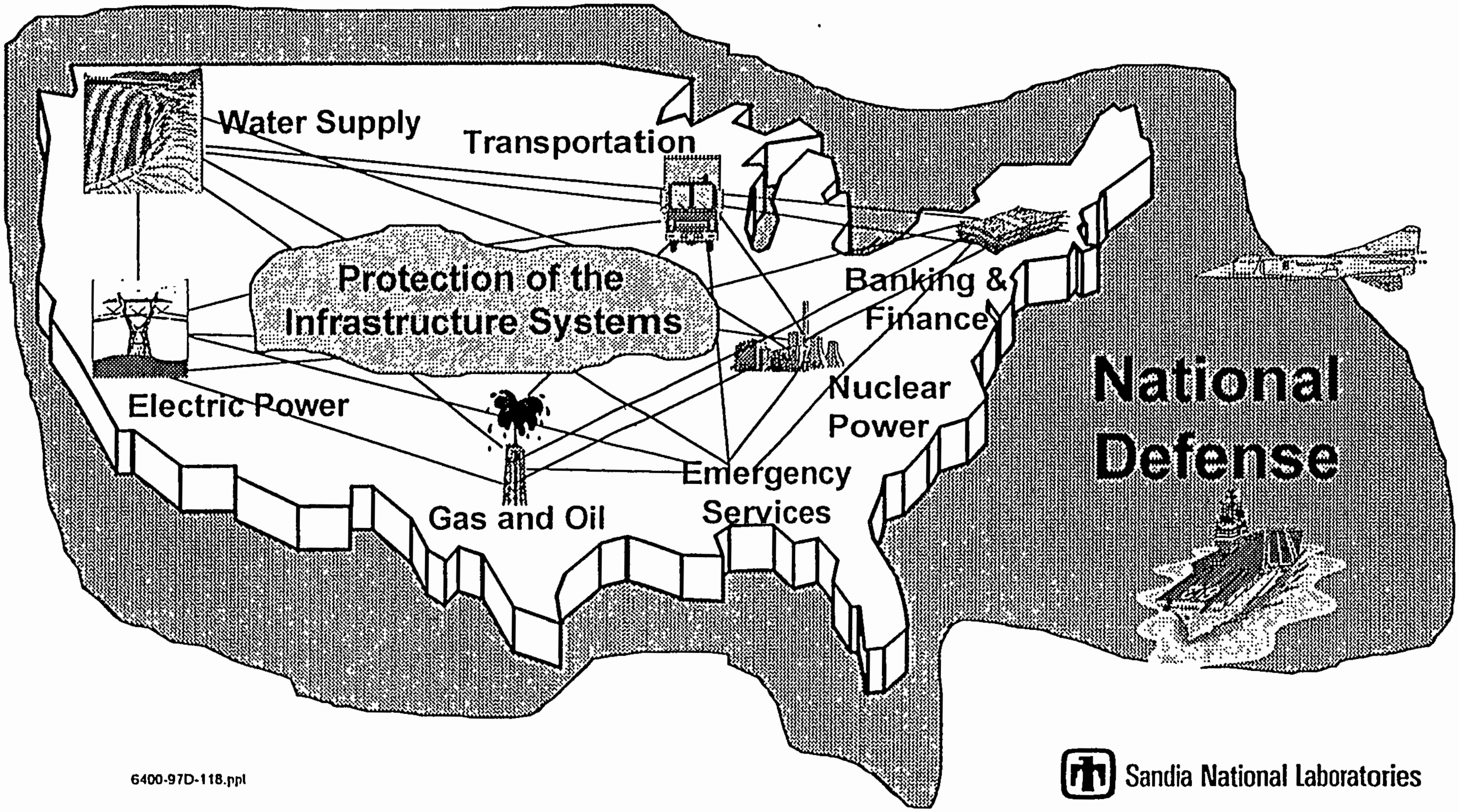
6400-97D-121H.ppt

We would like to further advance the state of the art

- *Weapons:* We would like to automate the vulnerability search algorithm and put it on an ASCI platform, and we would like to perform additional testing to gather data on components.
- *Nuclear Power Plant PRA:* Two key areas for improvement are time-dependent analysis and object-oriented PRA model development.
- *Uncertainty of Consequence Analysis:* We would like to work in the area of correlations, processing, and integrating information that we already have in a logical uncertainty study.
- *Transportation:* We would like to test to destruction for more packages to improve data bases, and we'd like to fully integrate RADTRAN into a GIS system.
- *Architectural Surety:* We'd like to do time and motion studies on the location of people and assets, and we'd like to expand our security to encompass surety and remodel the tools for ease of use by new users.
- *Environmental Programs:* We would like to extend risk management practices to environmental restoration, D&D, and other environmental problems to prioritize resource allocation.
- *Information Systems:* We'd like to do more pure research on modeling, and we'd like to improve best practices for applications of advanced software.

Sandia National Laboratories

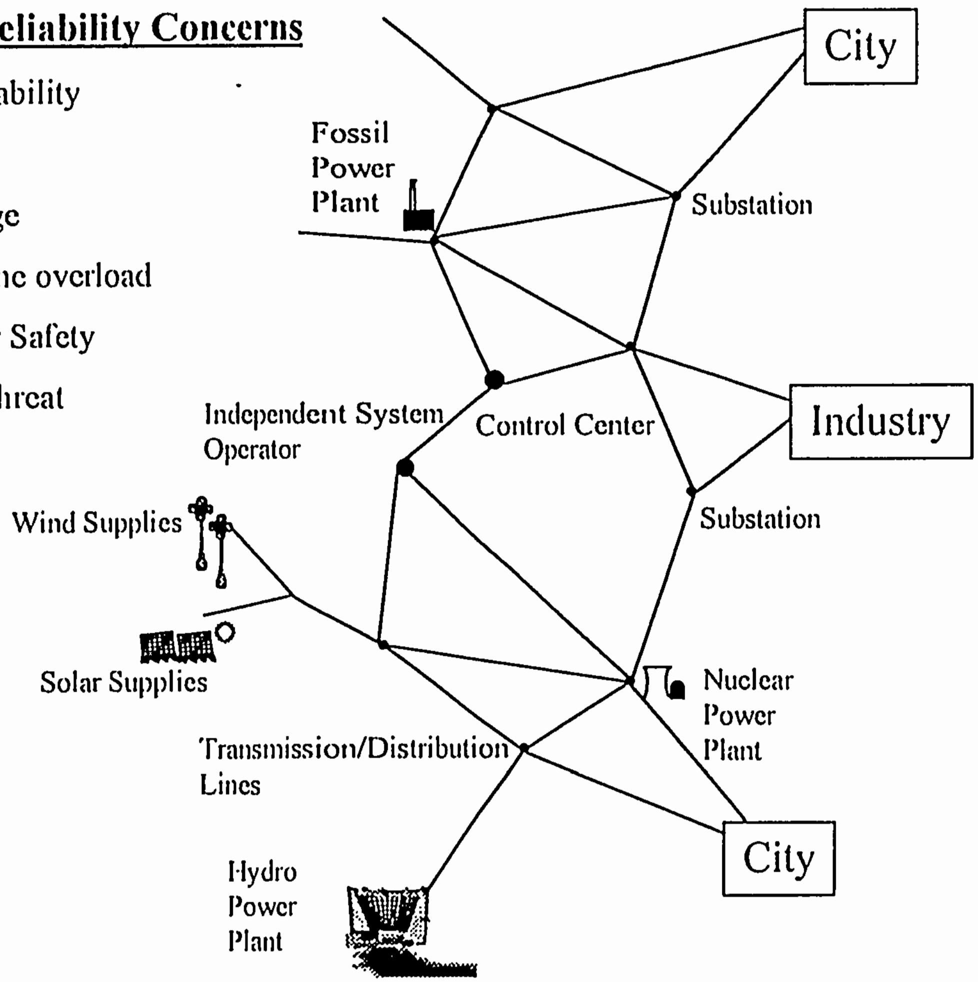
...to add more value in enabling the nation to protect its critical infrastructures



Risk and Reliability Implications of Electrical Deregulation

Risk/Reliability Concerns

- Grid Stability
- Nature
- Sabotage
- Long line overload
- Reactor Safety
- Cyber threat



Consequences

- Social/economic impact
- Health and safety impact
- Increased size and duration of outages

Current Technology Issues

- Existing reliability/flow models inadequately address:
  - —generation unit cycling
  - —load limits of lines
  - —dynamics of transmission changes
- New equipment will be needed to:
  - —Remotely switch power
  - —Accomodate distributed power sources

Weapons

Todd Jones
Assessment Technologies Department

Nuclear Weapons Assessments Utilizing Risk Assessment Tools

Todd R. Jones
Sandia National Laboratories
July 1997

Outline of Presentation

- Nuclear Weapon Design
- Weapon Safety Theme
- 1st Principle Assessments
- Model Based Safety Assessments *(PRA methods)*

Interest in PRA Applications to Nuclear Weapon Systems

- Drell (December 1990):

  "Continue safety studies and, in particular, . . . analyses which calculate overall risk and safety . . ."

- DOE Surety Plan (1991):

  "Provide comprehensive surety assessment of warheads supported by an appropriate accident database, adequate warhead response characterization, and a thorough risk/consequence assessment methodology."

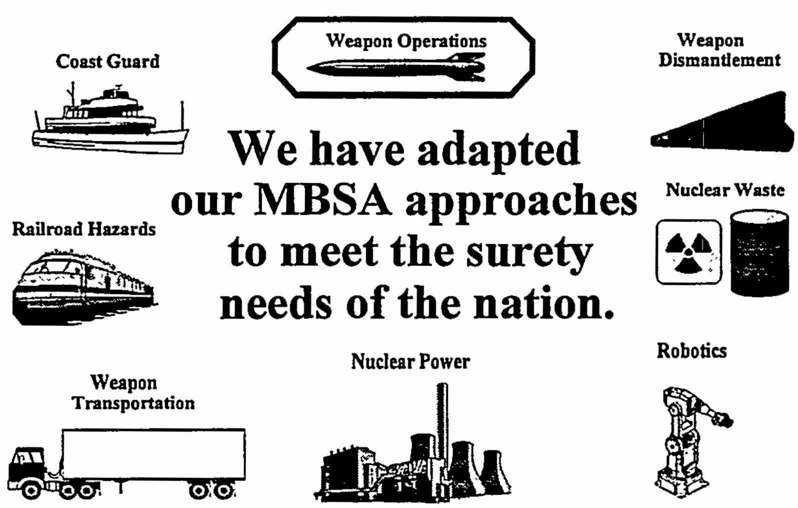
- DOE Orders:

  –DOE Order 452.1a Nuclear Explosive & Weapon Surety Program

  –DOE Order 452.2a Safety of Nuclear Explosive Operations

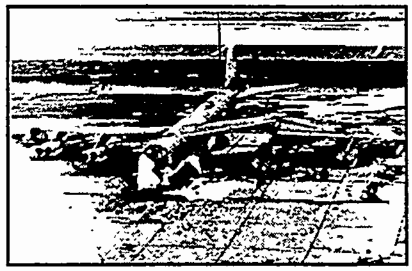
3

Meeting the Nation's Surety Needs using Model Based Safety Assessments



4

Nuclear Weapons Safety: One of Sandia's Most Important Missions



We must **assure** a safe weapon response
We must **certify** that safety standards are met

Assured Warhead Safety

A Corner Stone

Predictability and Analyzability

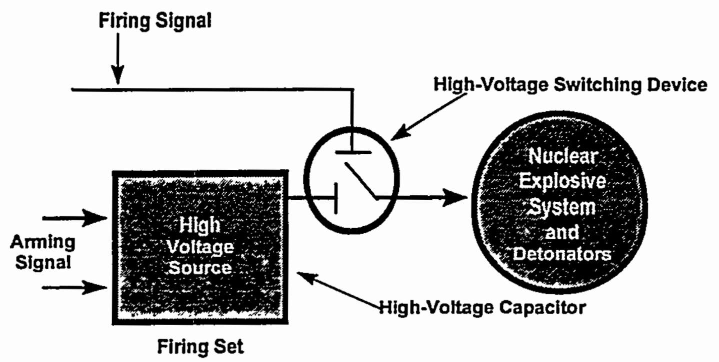
Nuclear Warheads
must
Respond in a Predictably Safe Manner

- Normal environments
  transportation, storage and operational use
- Abnormal environments -- accidents
  any credible combination of abnormal environments

Critical Elements

necessary for

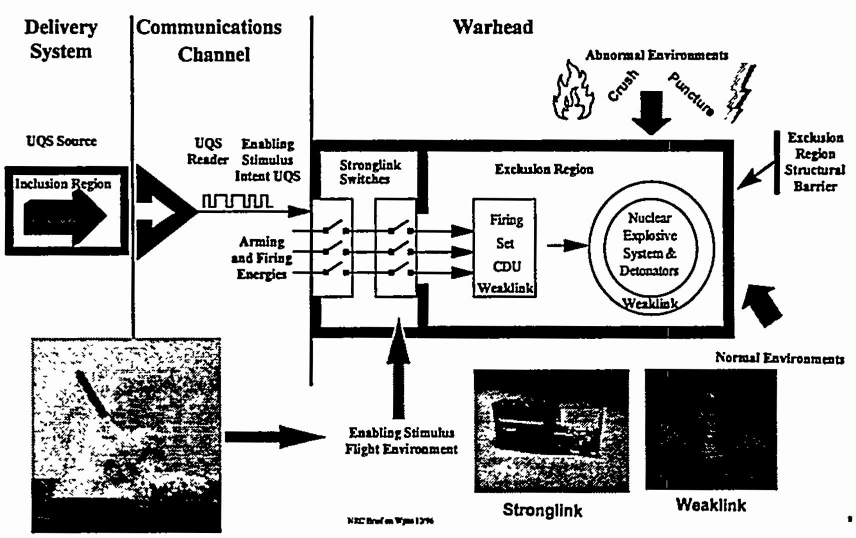
Intentional Nuclear Detonation



Safety Positive Design Measures should focus on protecting these critical elements.

This focus will:
Minimize the number of design features to be analyzed, and
Bound the range of abnormal environments that must be considered.

Nuclear Detonation Safety
US Generic System



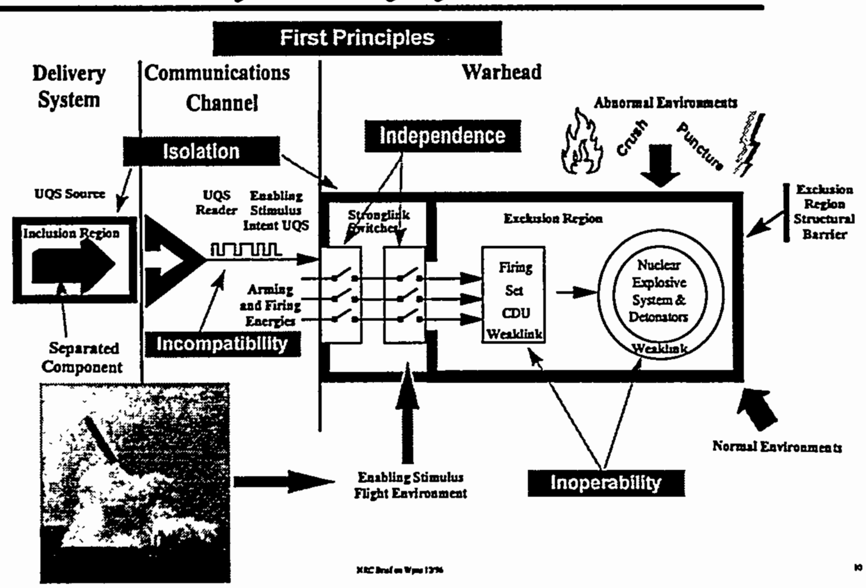
Nuclear Detonation Safety First Principles

- Isolation (Electrical)
  - Barriers
  - Stronglink switches
- Incompatibility
  - Intended enabling stimuli (e.g. unique signals)
  - Stronglink switches protect against unintended operate stimuli
- Inoperability
  - Weaklinks
  - Co-location
- Independence
  - Multiple independent safety subsystems

THEME -- Application of First Principles

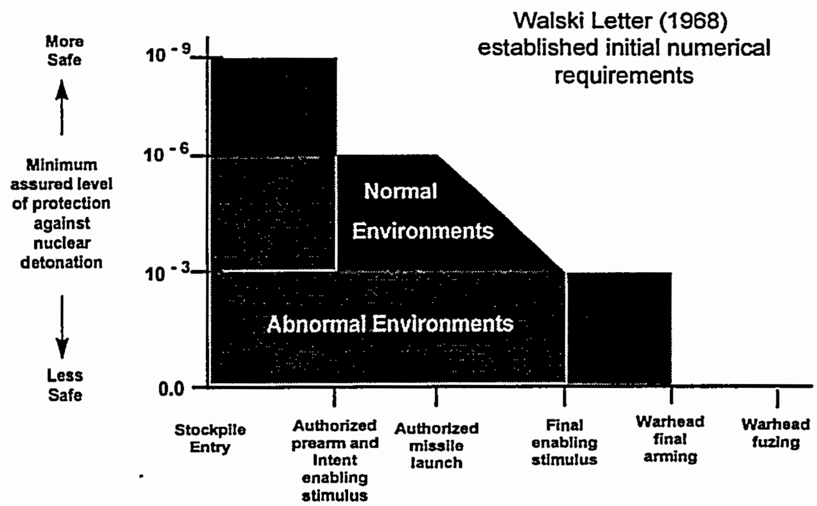
Limit safety design features to absolute minimum → **Bounds range of abnormal environments to be addressed** → **Limits analysis required for safety assessment**

Nuclear Detonation Safety US Generic System Safety Theme



10

Weapon System Safety Requirments

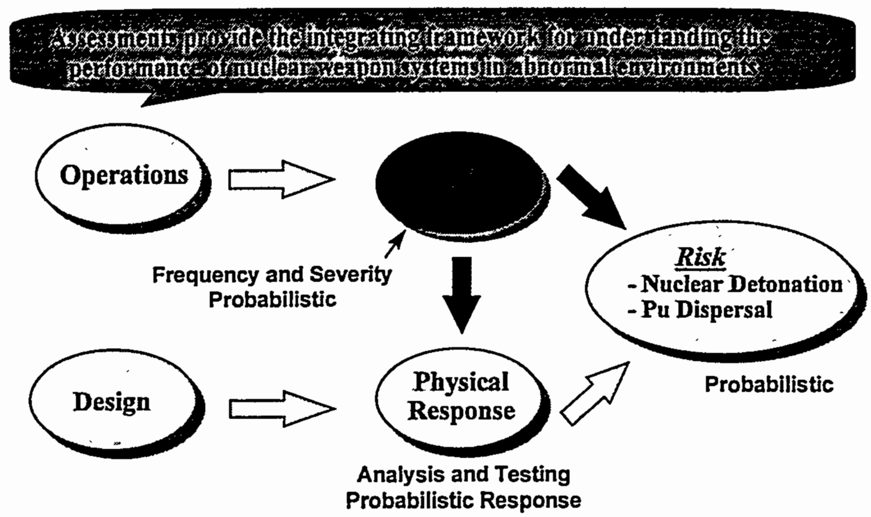


Nuclear Detonation Safety
First Principles Assessment

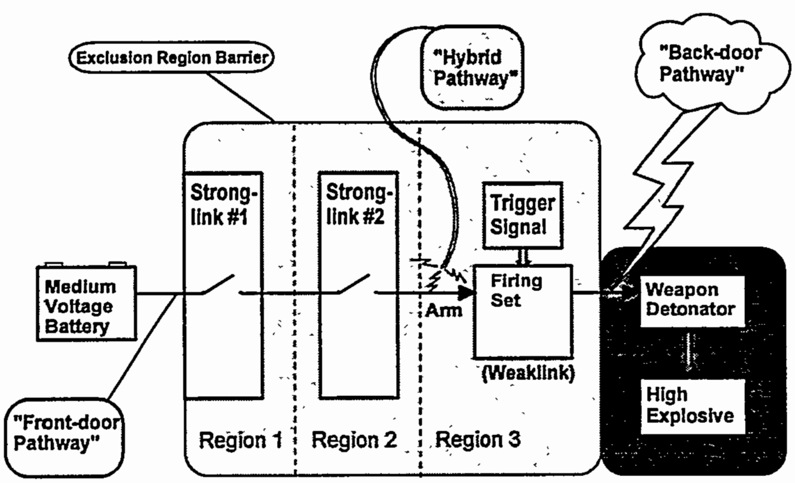
APPROACH
(Qualitative)

- Assume accident will occur
- Postulate representative range of possible accidents (abnormal environments)
- Identify potential failures -- system and component levels
  FIRST PRINCIPLE DESIGN FEATURES

Nuclear Detonation Safety Assessments
Integrated Frame Work
Probabilistic Risk Assessment -- QUANTITATIVE

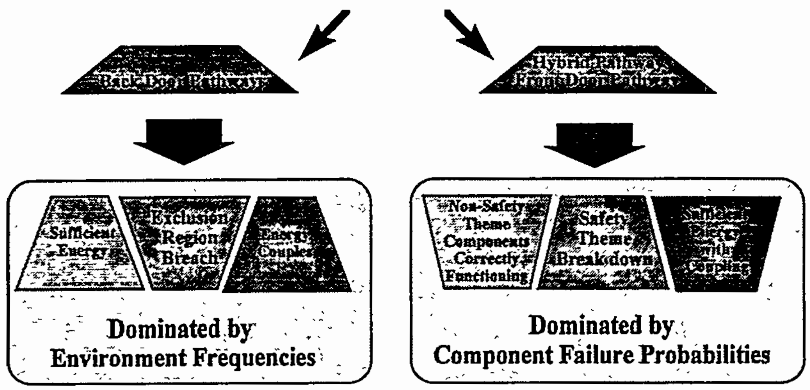


Weapon System Pathway Examples



Weapon System Pathway Requirements

INADVERTENT NUCLEAR DETONATION
(Nuclear Explosive Package Operable)



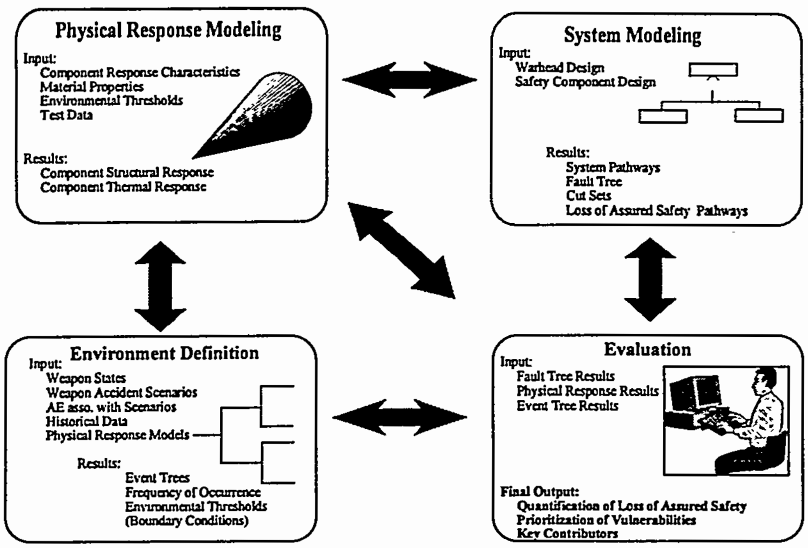
15

Inadvertant Nuclear Detonation & Loss of Assured Safety

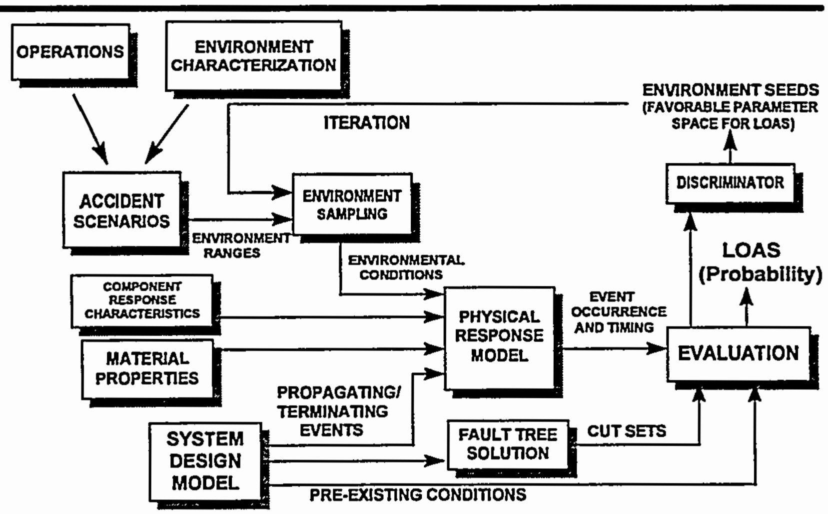
- **Inadvertant Nuclear Detonation**
  - When the Safety Theme of a weapon system is no longer assured to function as it was designed in normal and abnormal environments and sufficient energy is available and can couple to the system in a manner that will allow an unintended release of energy through a nuclear process.
- **Loss of Assured Safety**
  - When the Safety Theme of a weapon system is no longer assured to function as it was designed in normal and abnormal environments.
    - ➔Examples
      - Stronglinks lose their predictability before the weaklinks
      - Breach of exclusion region before weaklink fails

16

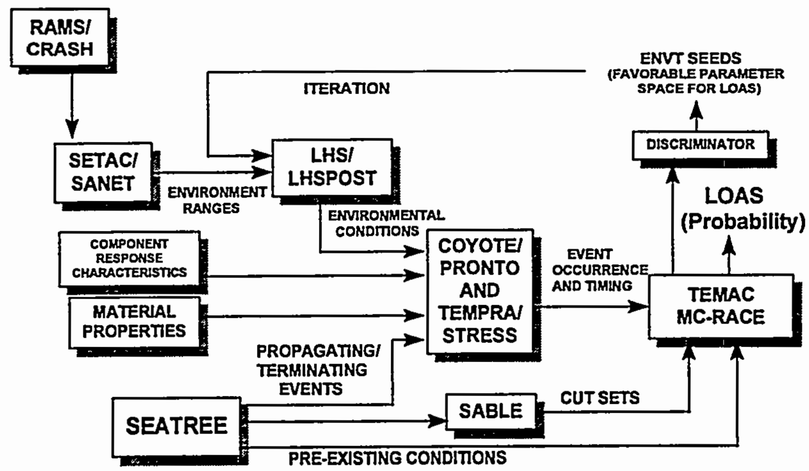
Model Based Safety Assessment Process Flow



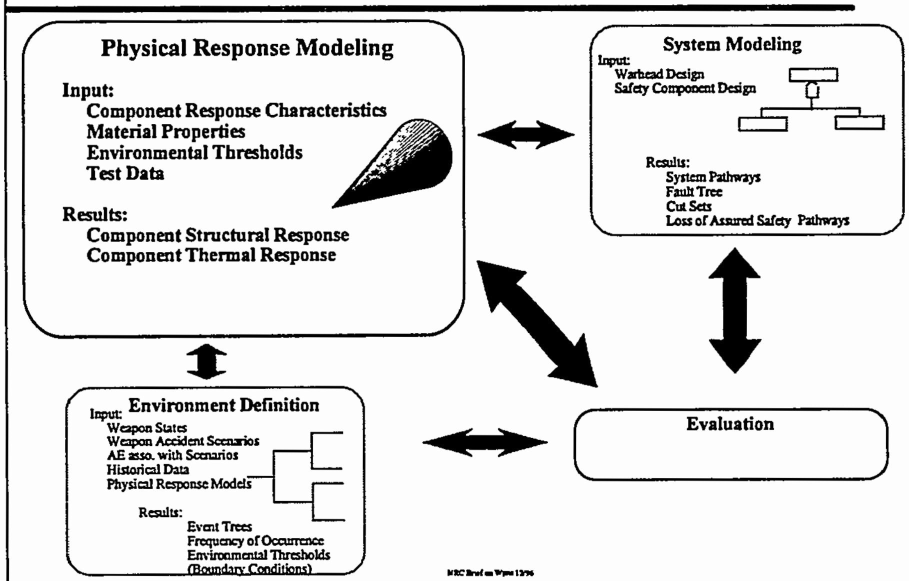
Model Based Safety Assessment Process

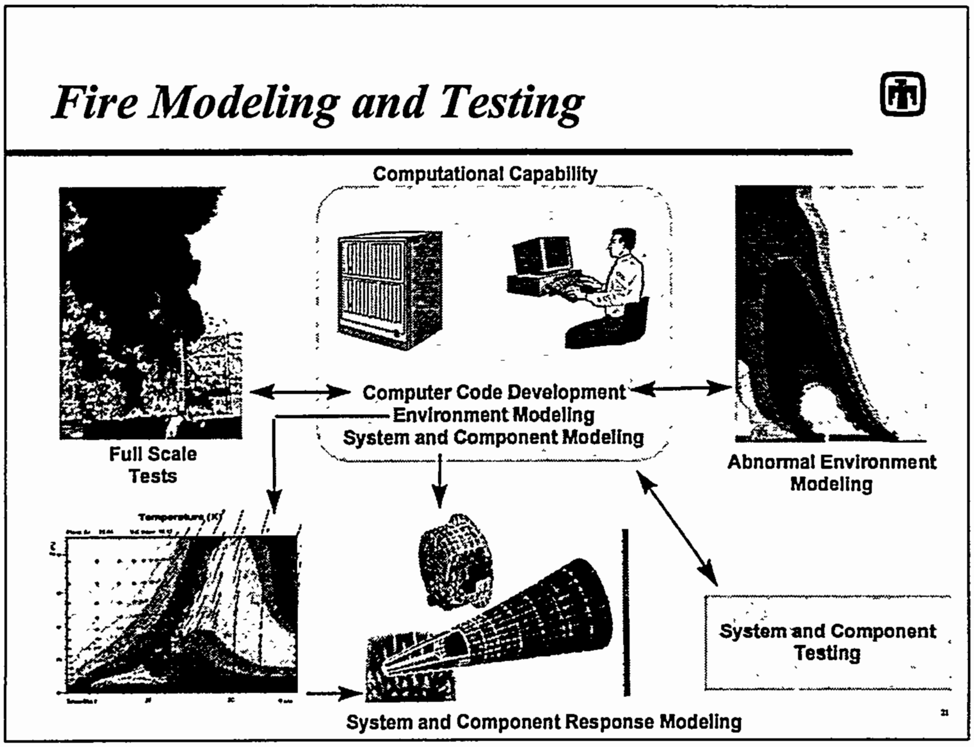


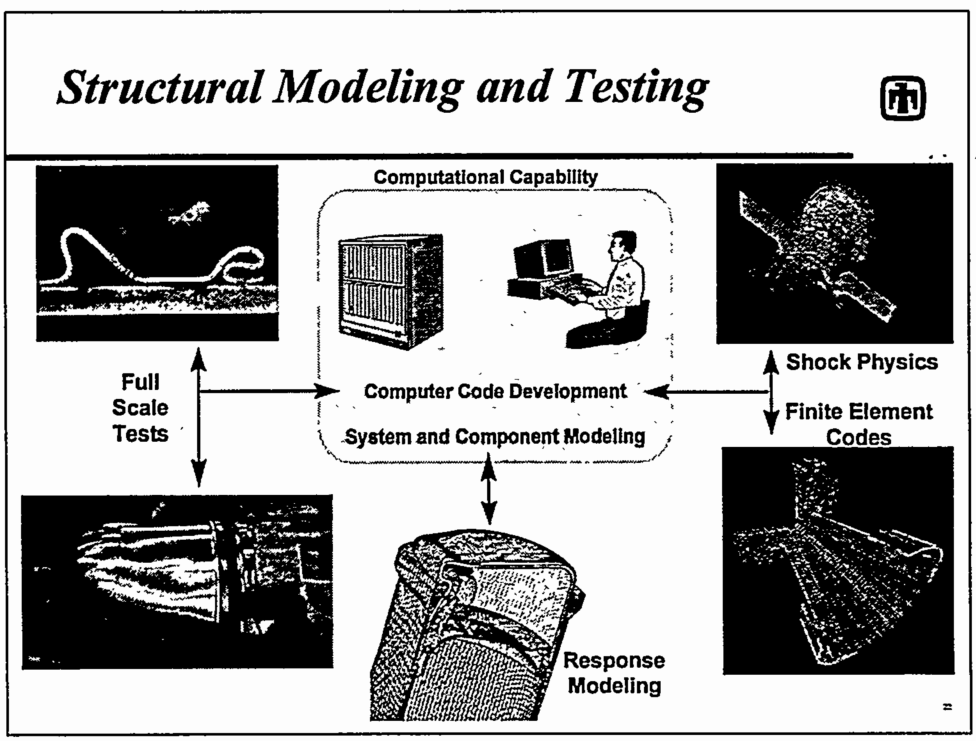
Analysis Codes Used in the MBSA Process



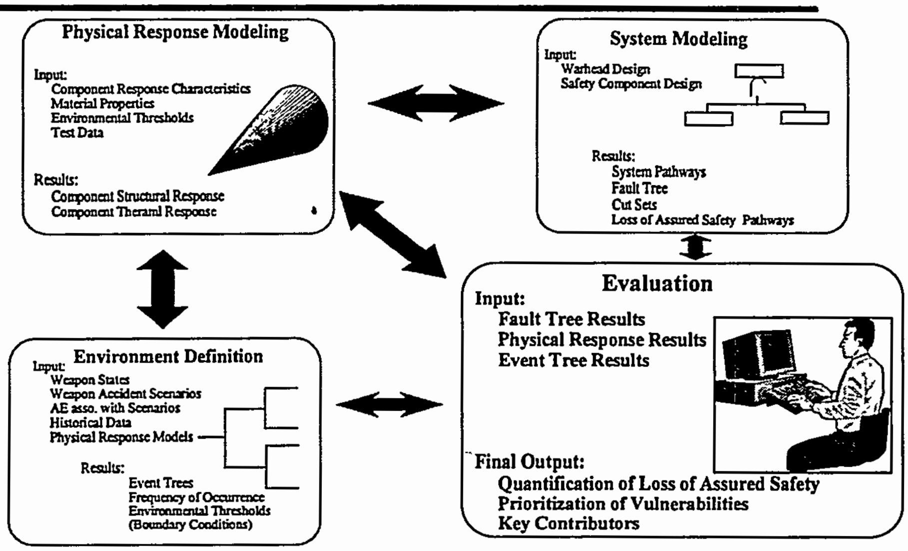
Model Based Safety Assessment Process Flow




Fire Modeling and Testing
Computational Capability
Computer Code Development
Environment Modeling
System and Component Modeling
Full Scale Tests
Abnormal Environment Modeling
Temperature (K)
System and Component Testing
System and Component Response Modeling

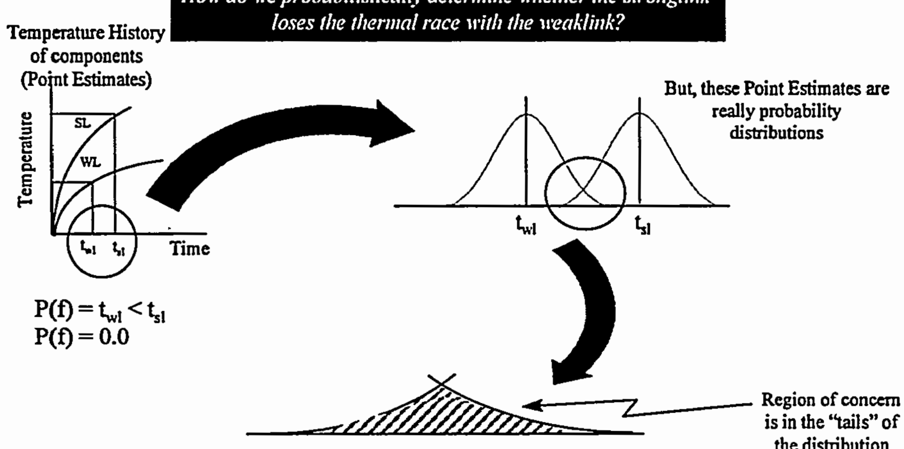

Structural Modeling and Testing
Computational Capability
Full Scale Tests
Computer Code Development
System and Component Modeling
Shock Physics
Finite Element Codes
Response Modeling

Model Based Safety Assessment Process Flow



Thermal Race Problem Weaklink – Stronglink

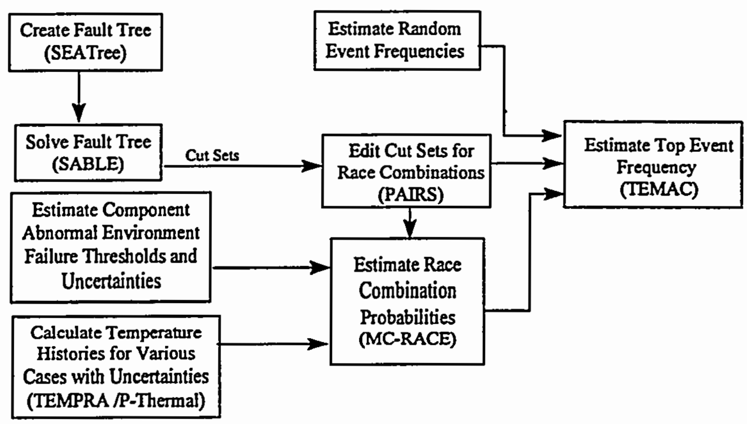
How do we probabilistically determine whether the stronglink loses the thermal race with the weaklink?



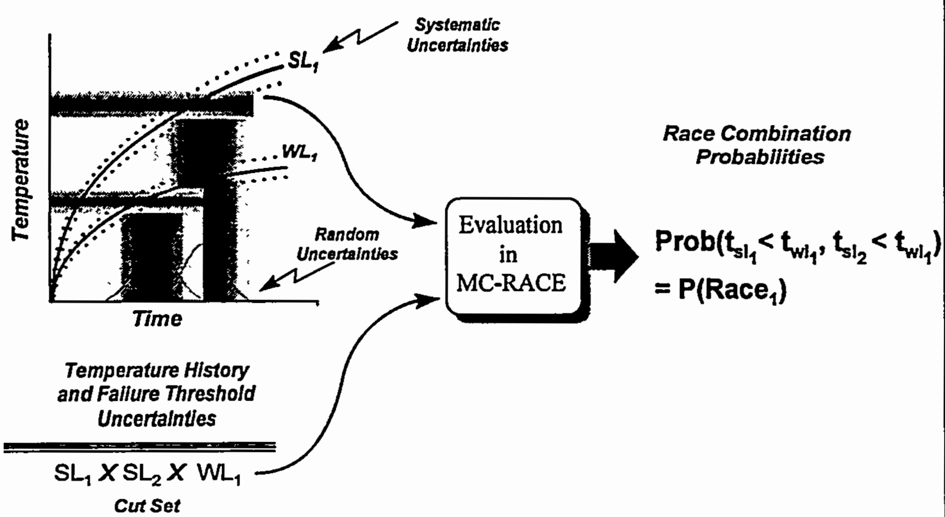
$P(f) = t_{wl} < t_{sl}$
$P(f) = 0.0$

$P(f) = P(t_{sl}) < P(t_{wl})$

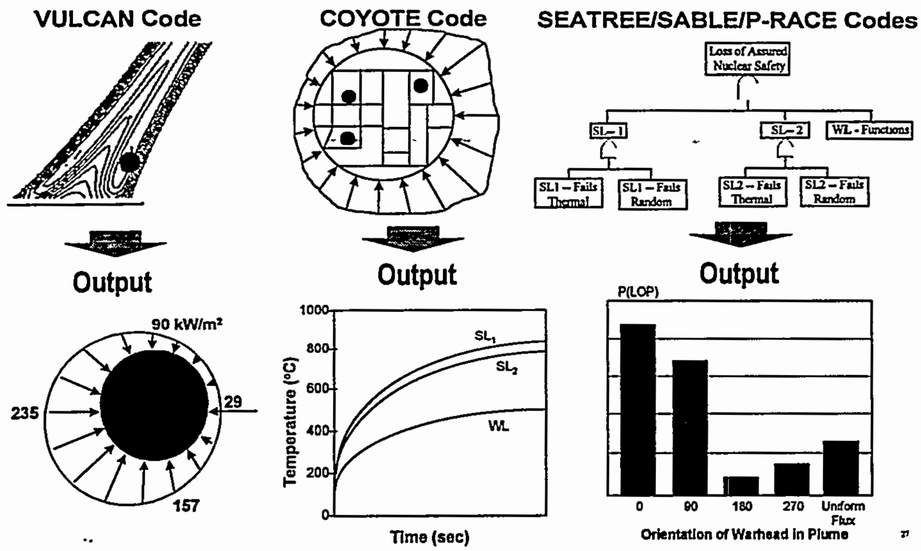
Evaluation Methodology (*Envisioned*)



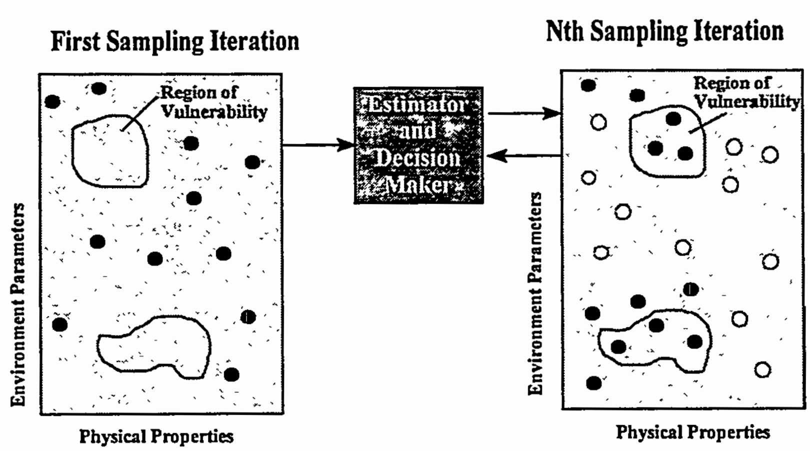
Estimating Multiple Race Combination Probabilities with Uncertainty and Random Event Probabilities *using MC-RACE*



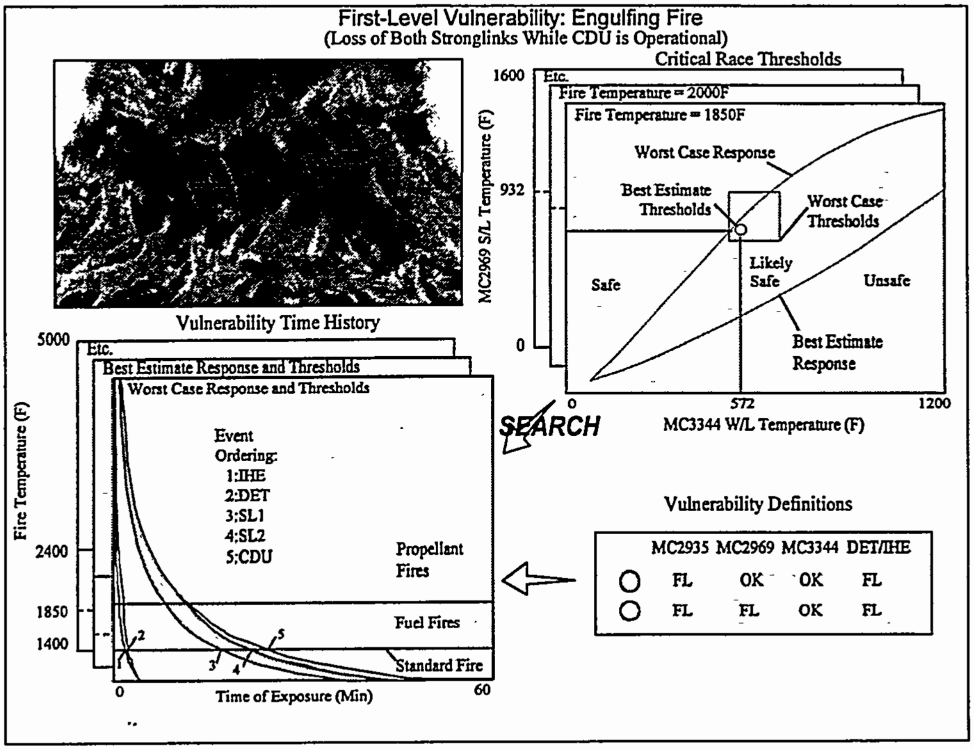
Initial Calculations Coupling Realistic Fire Conditions with High Fidelity Thermal Models



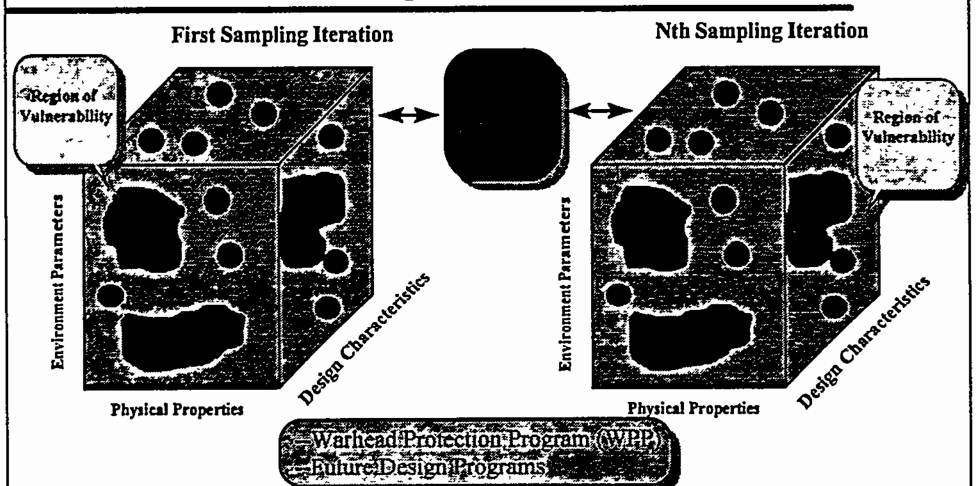
We Search the Space for Vulnerabilities



- *Optimization techniques, computational intelligence, & ASCI will improve efficiency of our search*

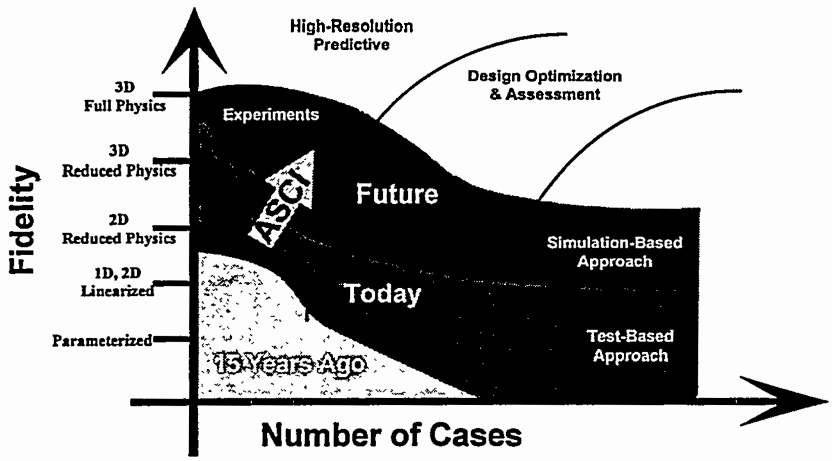


We are Exploring the Use of These Processes in Design



We wish to understand and eliminate vulnerabilities in the design process!

We will Exercise both the Capacity and Fidelity of High Performance Computing



31

MBSA Resources

- Application Funding
  - $1.5M
  - Assessed W78
    W80
    B61-7
    W76 in progress
- Application Organizations
  - 12333 -- Risk Analysis
  - 9113 -- Detailed Thermal Models
  - 6413 -- R-C Thermal & Structural Models
  - 9753 -- Electrical Analysis
- Development Funding
  - $2M
  - Code Development
  - SEARCH Algorithm
  - End to End Demo
  - ASCI integration
- Development Organizations
  - 12333 Risk Analysis
  - 6413 SEARCH development
  - 6412 ARRAMIS development
  - 9113 ASCI & End to End demo

32

Nuclear Power Plant PRA

Allen Camp, Manager
Risk Assessment & Systems Modeling
Department

Nuclear Reactor Risk Assessment

Presented to

Risk Evaluation Committee

Presented by

Allen Camp, Manager

Risk Assessment & Systems Modeling Department

July 1, 1997

First Major PRA Activities at Sandia

- Established risk assessment as major activity at Sandia
- Formed basis for many of the other PRA programs at Sandia
  - Staff
  - Methods
- Formerly produced most of the state-of-the-art PRA technology generated at Sandia

Sandia Has Led the Development of Reactor PRA

1975	1979	1981	1983	1987/1990	1990	1994
WASH-1400	RSSMAP	IREP	TAP A-45	NUREG-1150	RMIEP/PRUEP	LP&S
Reactor Safety Study	Methodology Application Program	Interim Reliability Evaluation Program	Decay Heat Removal Studies	Reactor Risk Study	Integrated LaSalle PRA	Low Power/ Shutdown for Grand Gulf
NRC	SNL	SNL	SNL	SNL	SNL	SNL
First Major PRA Study for Two Plants	Applied WASH-1400 Methods to More Plants	Improved Treatment of Operator Actions And More Detailed Logic Models	Added External Events Sabotage Cost/ Benefit Analysis	Added Detailed Containment Event Tree Integrated Analysis of Uncertainties Improved Consequence Analysis	More Detailed Logic Models Consistent Treatment of Consequence Uncertainties	Detailed Study of Low Power/ Shutdown Risk For a BWR6-Mk III

NRR-REC 3 July 1997

PRAs Performed Under the Technical Management of Sandia

Plant	Program	Type	Level
Sequoyah	RSSMAP	PWR W4IC	1
Calvert Cliffs	RSSMAP	PWR CE	1
Oconee	RSSMAP	PWR B&W	1
Grand Gulf	RSSMAP	BWR6 Mk III	1
Crystal River	IREP	PWR B&W	1
ANO-1	IREP	PWR B&W	1
Calvert Cliffs	IREP	PWR CE	1
Milestone-1	IREP	BWR3 Mk I	1
Browns Ferry	IREP	BWR4 Mk 1	1
Point Beach	TAP A-45	PWR W2	1 + EE
Turkey Point	TAP A-45	PWR W3	1 + EE
St. Lucie	TAP A-45	PWR CE	1 + EE
ANO-1	TAP A-45	PWR B&W	1 + EE
Quad Cities	TAP A-45	BWR3 Mk 1	1 + EE
Cooper	TAP A-45	BWR4 Mk 1	1 + EE
Trojan	TAP A-45	PWR W4	1 + EE
La Salle	RMIEP/PRUEP	BWR5 Mk II	3 + EE
Surry	NUREG-1150	PWR W3	3 + EE
Sequoyah	NUREG-1150	PWR W4IC	3
Peach Bottom	NUREG-1150	BWR4 Mk 1	3 + EE
Grand Gulf	NUREG-1150	BWR6 Mk III	3
N Reactor	——	Production Reactor	3 + EE
Grand Gulf	LP&S	BWR6 Mk III	3 + EE

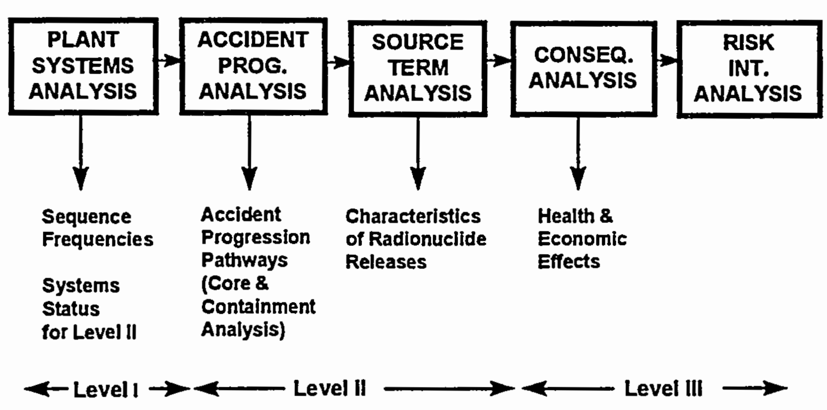
* EE - External Events

NRR-REC 4 July 1997

Other Applications and Extensions of Reactor PRA Methods

- Nuclear Rocket
- N Reactor
- Cassini
- Other Smaller Activities

Integrated PRA Analysis



PRA Must Be Based on Sound Science

- Models and Codes, e.g.,
  - MELCOR
  - CONTAIN
  - THERP
- Experiments and Data, e.g.,
  - Generic Data Bases
  - Hydrogen Combustion
  - Containment Strength
  - DCH
  - Cable Testing
  - Simulator Exercises

NRR-REC 7 July 1997

Examples of Important SNL PRA Activities

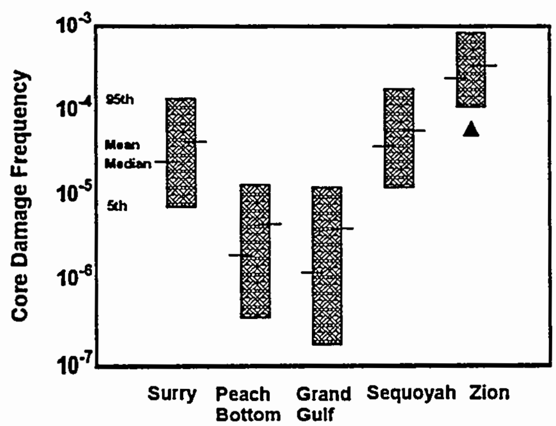
- Application-Based Methods Development
  - NUREG-1150 Methods
  - Dependent Failure Analysis
  - External Event Methods
  - Consequence Uncertainties
  - Software

NRR-REC 8 July 1997

Examples of Important SNL PRA Activities (cont.)

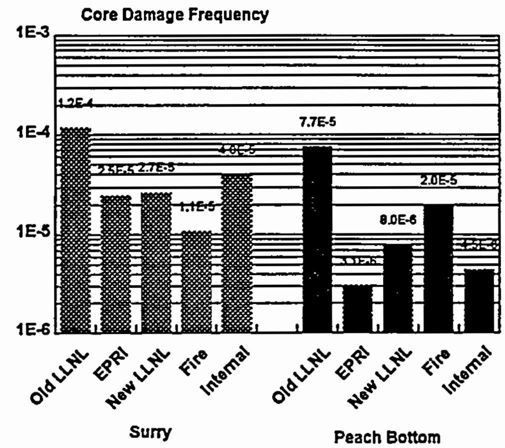
- **Major Studies**
  - NUREG-1150
  - Fire Risk Scoping Study
  - LaSalle
  - Low Power/Shutdown

NUREG-1150 CDFs

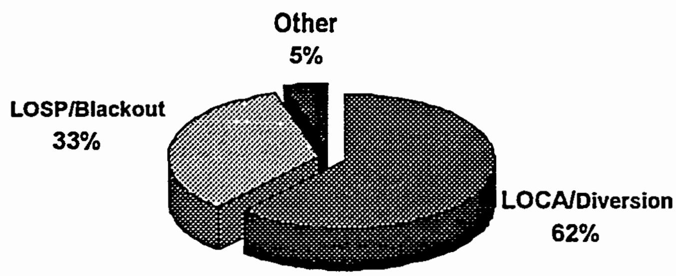


▲ indicates revised Zion CDF based on October 1990 plant modifications

Seismic and Fire are Significant Contributors to Overall Risk



BWR Low Power/Shutdown Study



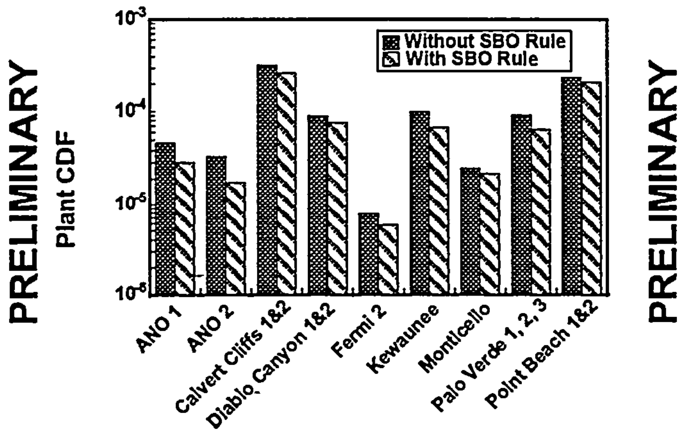
Examples of Important SNL PRA Activities

- Event Assessment
  - LER Reviews
  - ASP Rebaselining
  - Fire Events Database
- Issue Resolution
  - Decision Methods for Generic Issues
  - Prioritization Guidelines
  - Numerous Issues Including:
    - Decay Heat Removal
    - Fire Suppression
    - Service Water
    - Control Circuit Isolation
    - Shear Walls
    - Pressurized Thermal Shock

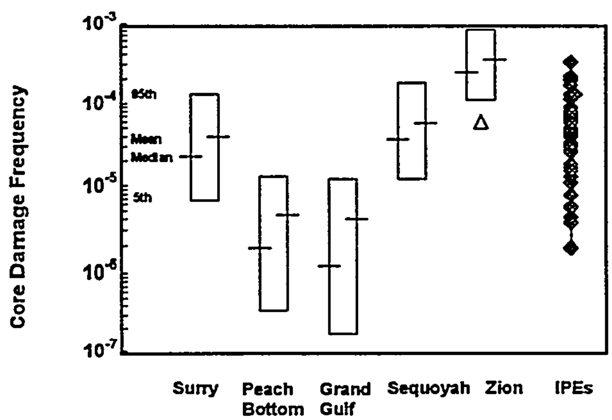
Examples of Important SNL PRA Activities (continued)

- Regulatory Effectiveness
  - Station Blackout
  - Appendix R Impact Evaluation
  - IPE Insights Program
- Other Regulatory Applications
  - IPEEE Requirements
  - PRA Working Group
  - PRA and Reactor Safety Training
  - Low Power/Shutdown
  - Low Power/Shutdown -- Tech Specs
  - 10 CFR 100 Modifications
  - Inspection Support

Before and After SBO Rule

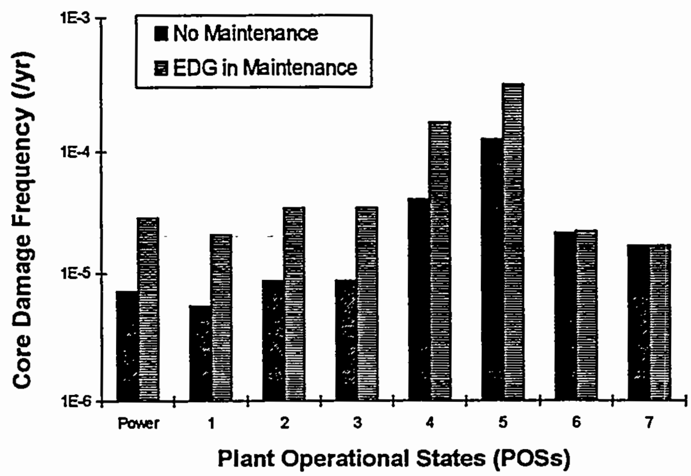


Comparison of NUREG-1150 to IPEs



△ Indicates revised Zion CDF based on October 1990 plant modifications

Change in CDF Due to EDG Maintenance



Current Methods Development Activities

- Human Errors of Commission
- Digital Control Circuits
- Consequence Uncertainties
- Fire PRA Methods
- Software Development

ATHEANA: A Technique for Human Error Analysis

- Represents human performance found in real nuclear power plant events
- Operator 'actions' based logically on their understanding of the conditions in the plant
- The operators can be misled resulting in inappropriate actions, including actions to termiante operating equipment
- ATHEANA can identify event sequences involving inappropriate actions
- ATHEANA can identify and quantify the most important combinations of plant conditions and weaknesses in the human-machine interface or gaps in job aids
- ATHEANA can quantify the human errors and incorporate the effects of these errors into the PRA logic models and quantification process.

Integrity of Digital/Software-Based Safety Systems

- Utilities are switching from analog to digital control systems
- Methods for evaluating digital systems are limited
  - Common cause failures
  - Software reliability
- SNL is developing a framework for guiding the design and review of digital systems
  - Completeness
  - Adequacy

Improvements: Fire Risk Assessment Program

- Objectives:
  - Assess current fire risk assessment methods and tools
  - Identify areas where significant improvements are needed and can be made in the near term
  - Implement the needed improvements
- Need areas have been identified and prioritized
- Preliminary implementation program plan developed
  - Improved data
  - Initiating event identification
  - Model validation
  - Other long-term activities

NRR-REC 21 July 1997

Risk-Informed Regulation Involves Three Potential Areas of Application

- Justification for new regulations or plant retrofits
- Elimination of regulations marginal to safety
- Use of risk to focus NRC licensing and inspection activities

NRR-REC 22 July 1997

Key Elements of RIR Implementation

- Clearly identified decision criteria
- Standards for PRA and staff training
- Adequate data bases
- SRP for reviewing/auditing industry submittals
- Control of overall risk level
- Evaluation of regulatory effectiveness

Summary and Conclusions

- Comprehensive integrated capabilities have been developed at SNL.
- The methods have been applied on numerous programs, including the resolution of key issues.
- Substantial work remains to be done if risk-informed regulation is to achieve its full potential for cost-effective regulation.

Uncertainty of Consequence Analysis

Fred Harper
High Consequence Assessment and
Technology Department

Summary of CEC/USNRC Consequence Uncertainty Program

Presented to
Risk Evaluation Committee

Fred T. Harper
Sandia National Laboratories
July 1, 1997

Sandia National Laboratories

USNRC/CEC Consequence Uncertainty Program

Biggest Contribution:

Library of uncertainty distributions for use in both consequence uncertainty studies and assessments in related fields (dispersion, health effects, etc.)

Pushed the State of the Art in:

Processing elicited information

Expert elicitation

Other:

Correlations

Performance Based Weighting

Sandia National Laboratories

The USNRC and the CEC decided to collaborate on this project

1) To share project costs

2) To gain access to a greater pool of experts

3) To combine the knowledge and experience of the CEC and US in the areas of uncertainty analysis, expert elicitation, and consequence analysis

4) To capture the potentially greater technical and political acceptability of a joint project

5) The Commissions decided to jointly proceed with an initial feasibility study. Atmospheric dispersion and deposition parameters were chosen to be the initial focus.

Phenomenological Areas that Comprise a Consequence Calculation Under Consideration for Joint Study

Phenomenological Area
Atmospheric dispersion
Wet and dry deposition
Behavior of deposited material and calculation of related doses
Plume rise
Internal dosimetry
Early health effects
Late health effects
Food chain

Selected formal elicitation methods to compile encyclopedia of consequence uncertainty distributions

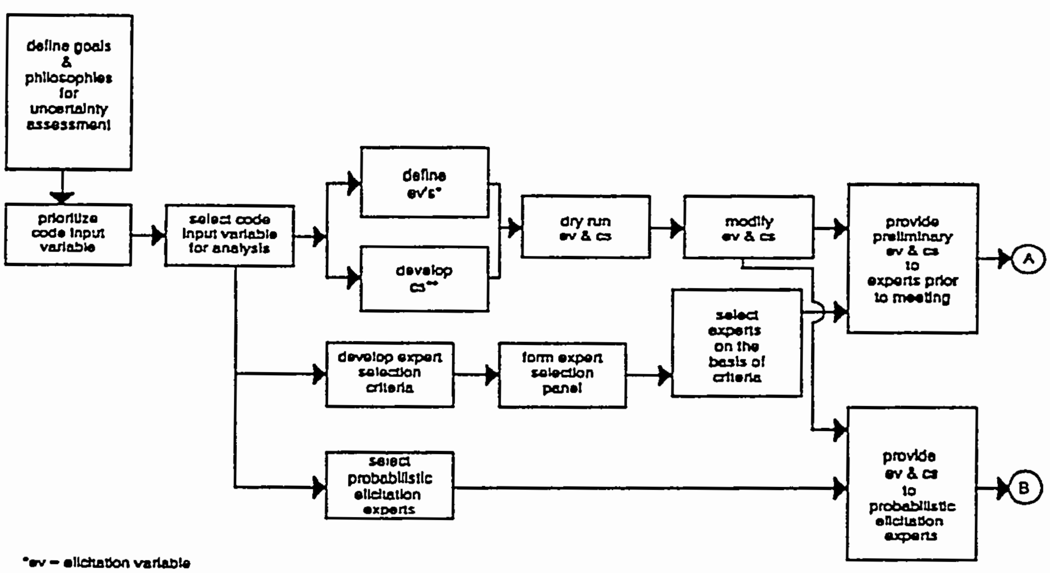
1) For multiple uncertainty studies and many other uses

2) Expert elicitation procedures allow the development of distributions on parameters which cannot be developed from experimental data or analytical models

3) The existing experimental database cannot provide necessary information (resource level required to obtain the data experimentally is unreasonable)

4) Information obtained from analytical models is not indisputably correct -- physics of the phenomenon not sufficiently defined by analytical models to allow a full uncertainty analysis

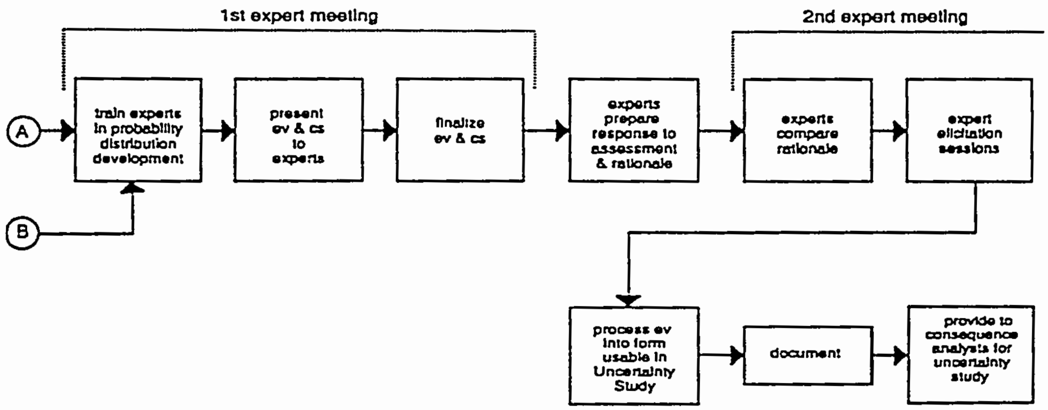
5) Formal expert elicitation process provides a well documented and easily trackable methodology conducive to review and defense



*ev – elicitation variable

**cs – case structure

Sequence of Methods Used for the Development of the Uncertainty Distributions



Sequence of Methods Used for the Development of the Uncertainty Distributions (Continued)

Objectives of study required uncertainty analysis using fixed codes

1) Fixed code requires distribution on input parameters
2) Philosophy of project -- do not prescribe model
3) Only elicit on potentially measurable parameters
4) Address important code input parameters
5) Project was led to explore inverse modeling to capture more than parameter uncertainty

Some modeling uncertainty is represented within distributions

1) Experts synthesize the available knowledge of a phenomenon from experimental, analytical, and theoretical sources

2) Uncertainty distributions, to some extent, are model independent

3) Aggregation of distributions incorporates different modeling philosophies into distributions (using equal weighted aggregation)

Elicitation variables chosen for the dispersion case structures:

1) The normalized concentration measured at a collector located at the centerline (χ_c/Q)

2) The concentration relative to the centerline concentration at a specified crosswind location y (χ_y/χ_c)

3) The concentration relative to the centerline concentration at a vertical distance, z and at the centerline, y=0 (χ_z/χ_c)

4) The standard deviation associated with the cross wind concentration (s_y) as would be measured by a line of collectors at specified distance from the source

5) The total area [km^2] covered by 90% of the time integrated concentration in that ring shaped distance region between r_1 and r_2 (r_1 and r_2 are in the far field)

Case structure for dry deposition questions

1) Four surface types: (1) urban, (2) meadow, (3) forest, and (4) human skin

2) Forms: aerosol, elemental iodine, and methyl iodide (iodine assumed not to deposit on aerosols)

3) Aerosol sizes: 0.1 μ, 0.3 μ, 1.0 μ, 3.0 μ and 10.0 μ (particle sizes are associated to spherical particles of unit density (1 gram/cm³))

4) Only initial condition specified was the average wind speed

Examples of External Dosimetry Elicitation Questions

1. Effective dose-rate and Effective Dose to an adult outdoors in "typical" urban and rural (open field) environments, following initial deposition of 1 Bq/m^2 of Zr-95/Nb-95, Ru-106/Rh-106, I-131 and Cs-137/Ba-137m to the lawned areas of the ground.

2. Ratio of time integrated air concentration indoors to that outdoors, given an outdoor value of 1 Bq m^{-3} for Pu-240.

3. Fraction of an average population in expert's own country that would be classed as (i) agricultural and other outdoor workers, (ii) indoor workers, (iii) non-active adult population and (iv) schoolchildren.

PSAM/FTH

Examples of Ingestion Pathway Elicitation Questions

1. Following a single deposit, what are the concentrations (Bq kg^{-1}) at maturity of Sr and Cs in grain, green vegetables, pasture grass, root crops and potatoes which are grown on soil that contains 1 Bq kg^{-1} of Sr and Cs?

2. Consider an animal that is continuously fed Sr or Cs at a constant daily rate under field conditions. What is the observed equilibrium transfer of activity, to the meat of the animal for each element?

PSA/96/l-T11

Examples of Internal Dosimetry Elicitation Questions

1. Initial deposition in the extrathoracic (ET) region, % of total deposition in the respiratory tract?

2. Retention of Pu on endosteal bone surfaces (considering a 10 µm depth of bone mineral) as a percentage of total skeletal retention, as a function of time after entry into blood?

PSA/96/l-T11

Example of Late (Stochastic) Health Effects Elicitation Questions

1. The number of radiation induced cancer deaths up to 20 years following exposure in a population of a hundred million persons (5×10^7 male, 5×10^7 female) each receiving a whole body dose of 1 Gy low LET (= gamma) radiation at a uniform rate over 1 minute.

PSA/96/FTH

Example of Joint Dosimetry/Late Questions:

1. The number of radiation-induced cancer deaths up to 40 years following exposure in a population of a hundred million persons (5×10^7 male, 5×10^7 female) each of whom inhales 10 K Bq of the radionuclides specified (Pu-239 and Sr-90 were specified) .

PSA/96/FTH

Examples of Early (Deterministic) Health Effects Elicitation Questions

1. For inhalation of aerosols that contain transuranic radionuclides provide:

2. The threshold lung dose rate below which no deterministic fatalities are observed within three years.

3. The lung dose rate that will result in deterministic dose in 10% of exposed individuals within three years. (There are additional questions for 50 and 90% of exposed individuals).

PSA/96/F11

Code input parameters are not always physically measurable parameters

1) Important dispersion code input parameters are mathematical constructs that define the spread of the plume in the Gaussian model: the horizontal spread (σ_y) and vertical spread (σ_z) parameters modeled using the power law:

$$\sigma_y = a_y x^{b_y} \; ; \; \sigma_z = a_z x^{b_z}$$

2) a_y, b_y, a_z, b_z assigned values in MACCS and COSYMA depending on the atmospheric stability class, but are not physically measurable parameters

3) Necessary to elicit distributions on physically measurable parameters which can lead to distributions on a_y, b_y, a_z, b_z

Gaussian Plume Equation

$$\frac{\chi}{Q}(x,y,z)=\frac{1}{2\pi\, u\, \sigma_y\, \sigma_z}\, e^{-\frac{1}{2}\left(\frac{y}{\sigma_y}\right)^2}\, e^{-\frac{1}{2}\left(\frac{z-h}{\sigma_z}\right)^2}$$

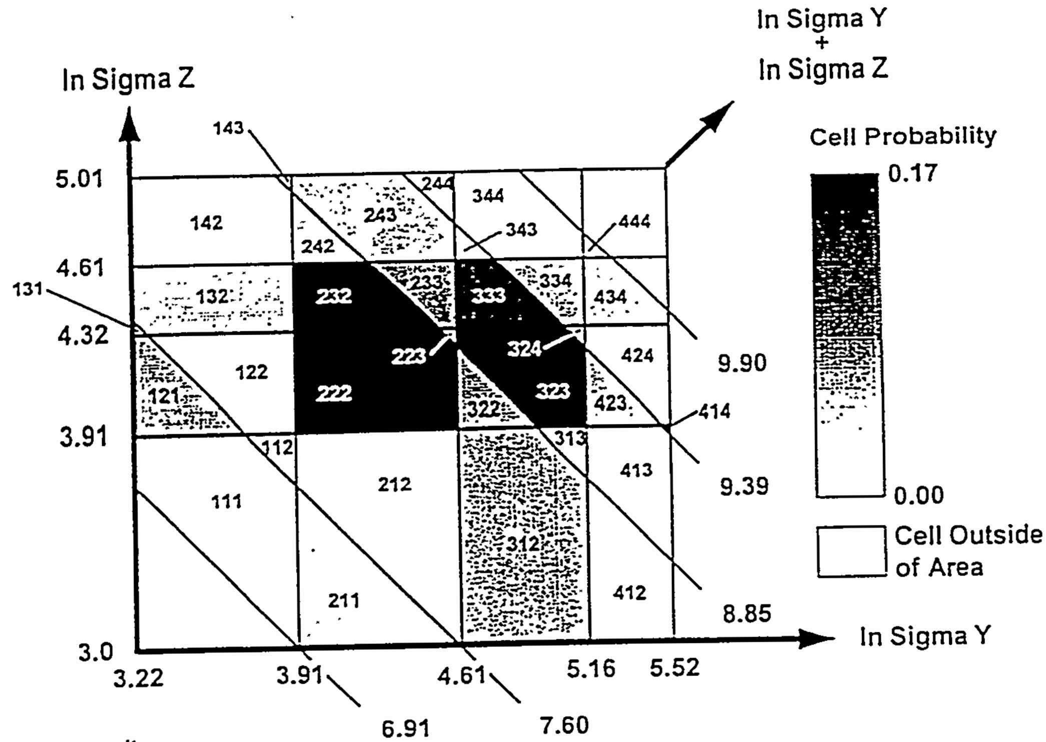
y = horizontal crosswind coordinate
z = vertical crosswind coordinate
σ_y = standard deviation to y direction
σ_z = standard deviation to z direction
u = mean wind speed
h = release height

Sandia National Laboratories

To Use Information in MACCS and COSYMA Uncertainty Studies

Elicit Distributions For		Process		Distributions in Code Input Parameters Used In Uncertainty Study
χ/Q, σ_y	→	Sigma Method	→	a_y b_y a_z b_z
$\frac{\chi_y}{\chi_c}$, $\frac{\chi_z}{\chi_c}$	→	Chi Method, Gausian Constraint	→	a_y b_y a_z b_z
V_d	→		→	V_d
1 - f	→	Sigma Method	→	a , b

Cell Labeling Mechanism



Elicited quantity (QC_{grain}[TEC) dependent on many parameters, even in a simple foliar absorption model

1. Time of deposition
2. Kp (percolation rate constant)
3. Kr (resuspension rate constant)
4. Kw (weathering rate constant)
5. Krs (Rainsplash Rate Constant)
6. BMAX (maximum edible crop biomass)
7. FV (interception factor)
8. FD (ratio of dry to wet weight)

PSA/96/FTII

A two step process was developed to obtain distributions for Kab

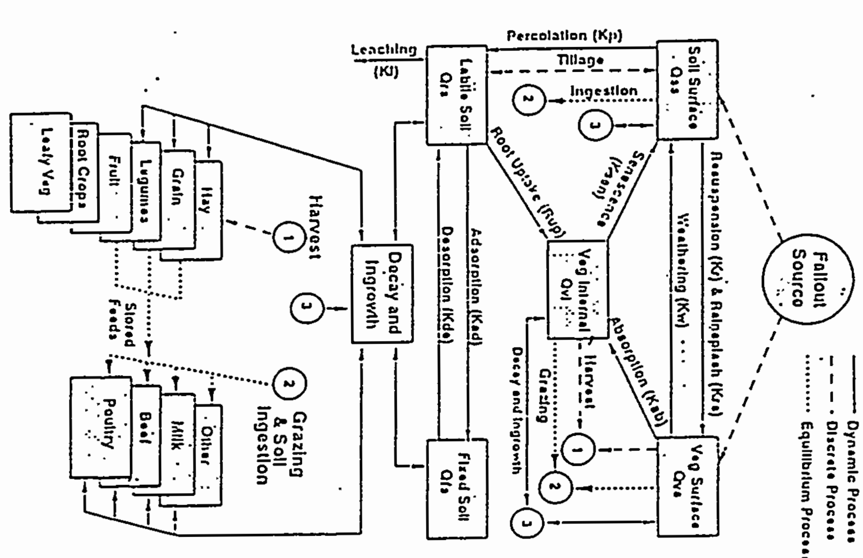
1. Obtain median

2. Obtain distributions

PSA/96/FTH

Khlopin Radium Institute Consequence Assessment Workshop

Transfer Processes



October 16, 1995

To obtain the median for Kab

1. *Kp, Kw, and Kr* are set at their median values as determined from the processing of other soil and plant questions from this program

2. *Krs*, *BMAX*, and *FV* are held at their point estimate values from COMIDA experience

3. Set $QC_{grain}[TEC]$ equal to the elicited median and then solve for *Kab*

PSA/96/FTII

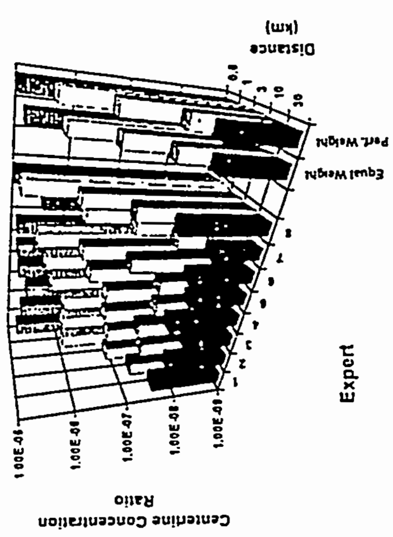
Example Range Factors from Ingestion Pathway Assessments

Elicitation Variable	Uncertainty Range	Comment
Soil Migration	<100 (Cs) <1000 (Sr)	Range factors order of magnitude higher for Sr compared to Cs
Soil Fixation	2 - 50	No significant difference between Cs and Sr
Root Uptake Concentration Factors	20 - 5000	Range factors for Sr smaller than those for Cs. Ranges for organic soil larger.
Interception Factors	10 - 20	
Resuspension Factors	10,000	Large ranges with 50th percentiles close to the 5th

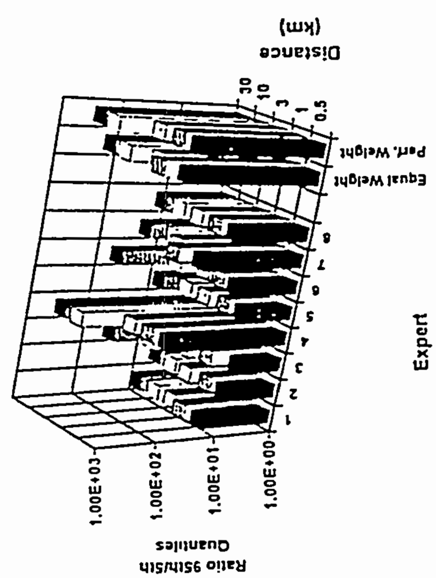
(cont.)

Retention Times	20	
Concentration in · Grain at Harvest	70 - 600	
Concentration in Root Crops at Harvest	1000	Cs ranges larter than Sr ranges
Availability of Radionuclides in Ingested Feed for Transfer Across Gut	2 - 3 (I) 2 - 4000 (Sr and Cs)	
Transfer to Meat, Milk and Eggs	10 - 80 (Cs) 600 - 1400 (I to eggs and sheep milk)	Higher ranges for transfer to lamb, eggs, pork and chicken
Biological Half Lives	10 - 30 (Cs) 200 - 500 (I) 500 - 1300 (Sr)	

PSA/96/F11



Elicited values for 50th quantile centerline concentration ratio. Stability class A.



Ratio of 95th/5th quantile elicited centerline concentration ratios. Stability class A.

Transportation

Sieglinde Neuhauser
Transportation Systems Analysis
Department

Presentation for External Committee to Evaluate Sandia's Risk Expertise

TRANSPORTATION RISK ASSESSMENT

Sieglinde Neuhauser, PhD
Transportation Systems Analysis
Department 6641

July 1, 1997

Statement of Purpose:

To Develop and Maintain Risk-Assessment Tools, Data, and Expertise to Continue to Confirm the Safety of Radioactive Materials Transportation by the DOE and others.

RISK ACTIVITIES AT SANDIA

•Sandia National Laboratories is a **world leader** in risk-assessment research and transportation technology for radioactive materials.

•Transportation Risk Assessment [Org. 6641] is **part of the extensive risk infrastructure at SNL.**

ACTIVITY AREAS IN E&E SECTOR

- RADTRAN Computer Code for Transportation Risk
- Data Processing Tools for Risk Analysis
- Applications (including Work for Others)
- Information Systems:
  - TRANSNET
  - RMIR (Radioactive Materials Incident Reports)
  - RADTRAN Website: **http://ttd.sandia.gov/Radtran/radtran.html**

TRANSPORTATION SCOPE:

- All commercial modes: truck, rail, maritime (barge & ship), air (passenger & cargo air, incl. helicopter)
- Intermediate stops (e.g, truck fuel stops, rail classification yards, ports of call, airports)
- Carriage of all types of weapons and non-weapons materials (LLW, VHLW, TRU waste, SNF, fresh fuel, Pu, radiopharmaceuticals)
- All types of RAM packagings from cardboard boxes to spent fuel casks.

HISTORY OF RADTRAN CODE

- RADTRAN I, 1977 - for NUREG-0170, "Final Environmental Statement on Transportation of Radioactive Material by Air and Other Modes."
- RADTRAN II, 1982
- RADTRAN III, 1986
- RADTRAN 4, 1989
- RADTRAN 5, beta release, 1997

RADTRAN HIGHLIGHTS

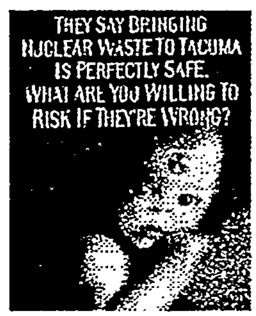
- RADTRAN Code
  - National and International Standard; source code for IAEA's INTERTRAN code
  - Approx. 150 users (e.g., LANL, Bettis Labs, UNLV)
  - RADTRAN 5 released this spring
- Input-File-Generator software (downloadable from RADTRAN website)
- Uncertainty and Sensitivity analyses
- Probabilistic Analysis with Latin Hypercube Sampling (LHS) "Shell" Code developed at SNL

RADTRAN QA PLAN - Verification

- Programmer's Log
  - Changes Sheets
  - Differences found
  - Test file comparisons
  - Other Information
    plots, hand calculations, notes
- askSam - data base program

RISK ASSESSMENT IS A RAPIDLY DEVELOPING FIELD

- Maintaining non-obsolescence requires frequent updates
- Risk "perception" often can be responded to quantitatively
- More access to high-resolution data than ever before (e.g., GIS systems)
  - population distributions >>>environmental justice
  - accident data >>> emergency response
- Latin Hypercube Sampling (LHS) is now the method of choice for probabilistic risk analysis
- Required to determine compliance with new risk-based regulations



Example of effective, though inaccurate, "risk communication" by intervenors.
This is the atmosphere DOE encounters during NEPA process.

Response must include the solid, accurate information that SNL provides in risk analyses.

RISK APPLICATIONS AT SANDIA

- Litigation Support (DOE/General Counsel)
- Provide National Transportation Program, other federal agencies, and the public with quality-assured Risk Analysis tools to support EAs, EISs and other risk analyses
- Participate in IAEA Coordinated Research Programmes, etc.
- Rapid response via DOE Congressional Liaison to lawmakers' queries

EXAMPLES OF APPLICATIONS & REQUESTS IN PAST DECADE

- Taiwan Spent Fuel Movement EAs & litigation (DOE/EM)
- Foreign Research Reactor Urgent Relief EA & litigation (DOE/EM)
- Address intervenor & stakeholder concerns
- Y-12 EA & Public Information Meetings (DOE/DP)
- Project Sapphire (now declassified)
- NRC - NUREG-0170 re-analysis
- Canadian request for Assistance (Ontario Hydro)

TRANSPORTATION RISK GROUPS NETWORK WITH OTHERS AT SNL

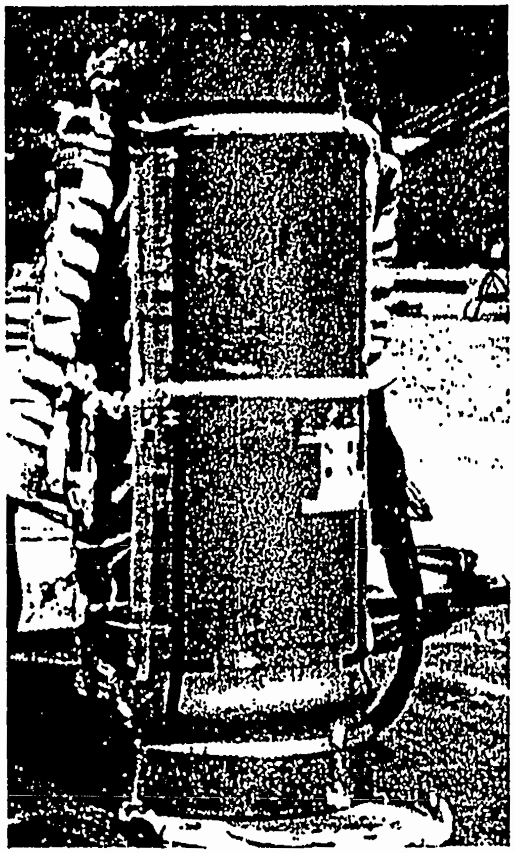
- Testing, Instrumentation - accident consequence data
- Package Design - various RADTRAN input values
- Statistical Methods - LHS Shell for RADTRAN
- Reactor Safety MACCS Code - models parallel
- GIS - route-specific analysis
- Weapons Transportation - ADROIT Code (Safe-Secure Transports); DOD and DOE are primary customers

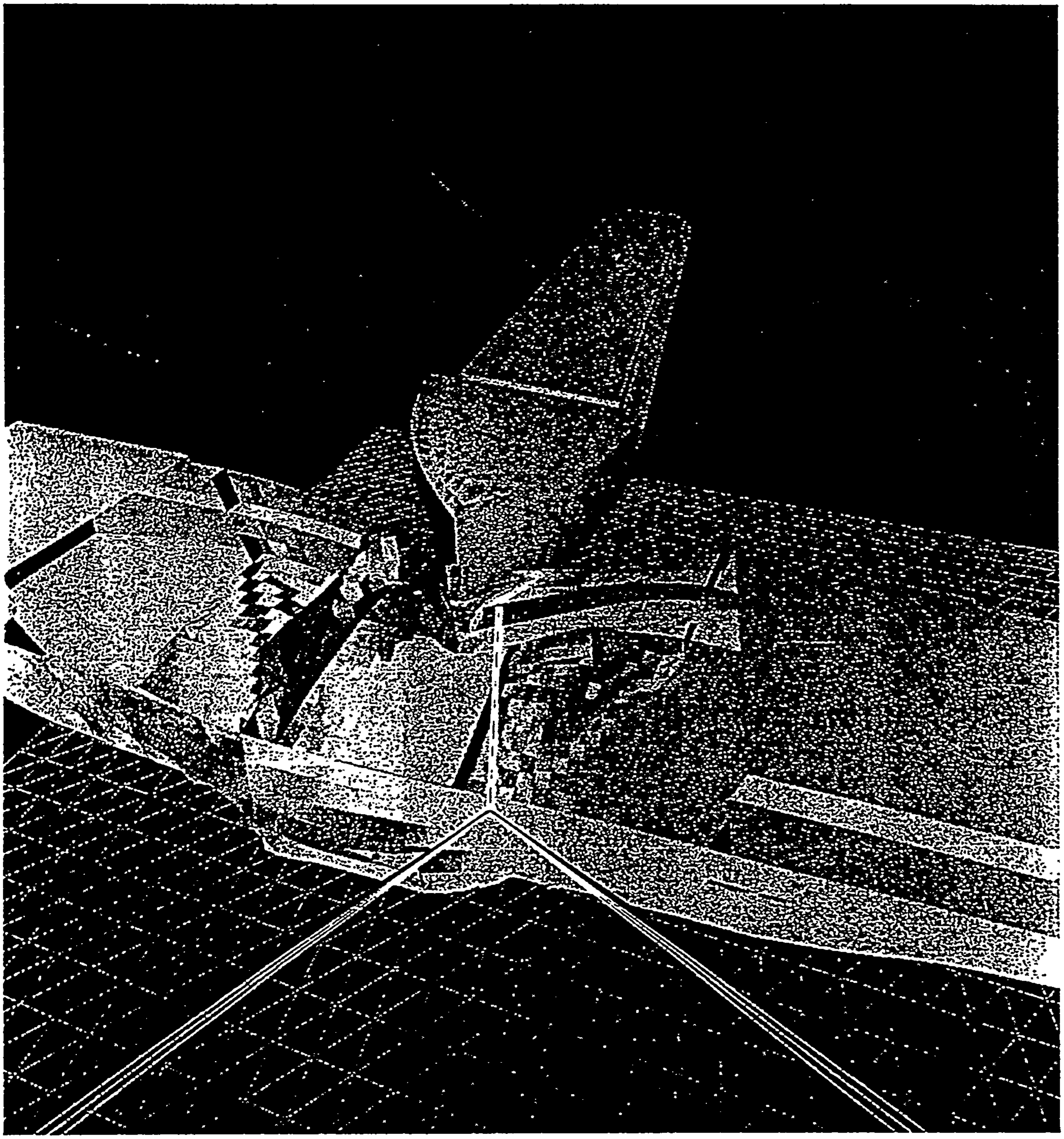
Transportation Systems Analysis Team

- Fran Kanipe- RADTRAN Development; Webmaster
- Sieglinde Neuhauser, Ph.D.- RADTRAN/Risk Analysis
- Jim McClure, Ph.D.- Information Systems (RMIR)
- Scott Mills, Ph.D.- Latin Hypercube Sampling (LHS), Sensitivity, & Uncertainty Analysis
- Rick Orzel - Information Systems; TRANSNET System Manager
- J.D.Smith-ORIGEN & Routing Calculations
- Jeremy Sprung, Ph.D. - MACCS/Risk Analysis
- Ruth Weiner, Ph.D. - Atmospheric Dispersion; Hazmat

Structural Evaluation Test Unit

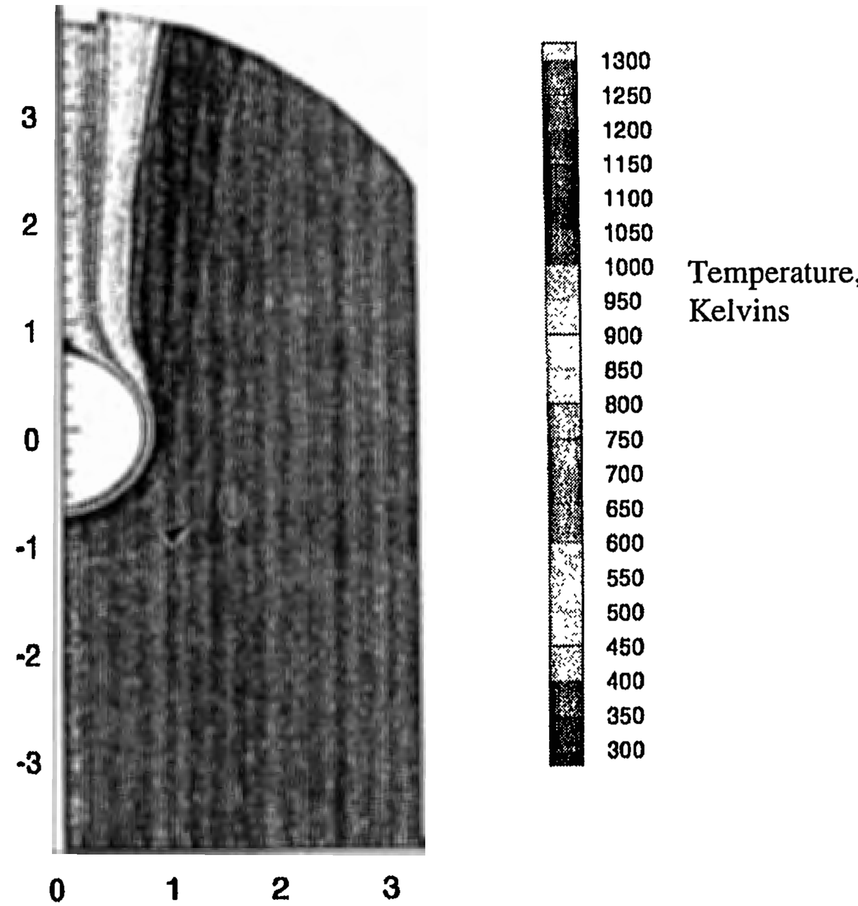
Impact tests at velocities up to 60 MPH did not fail the container.





Container Analysis Fire Environment Model

Cylindrical object engulfed in fire shows temperature distribution around object. Heat transfer to object also calculated.

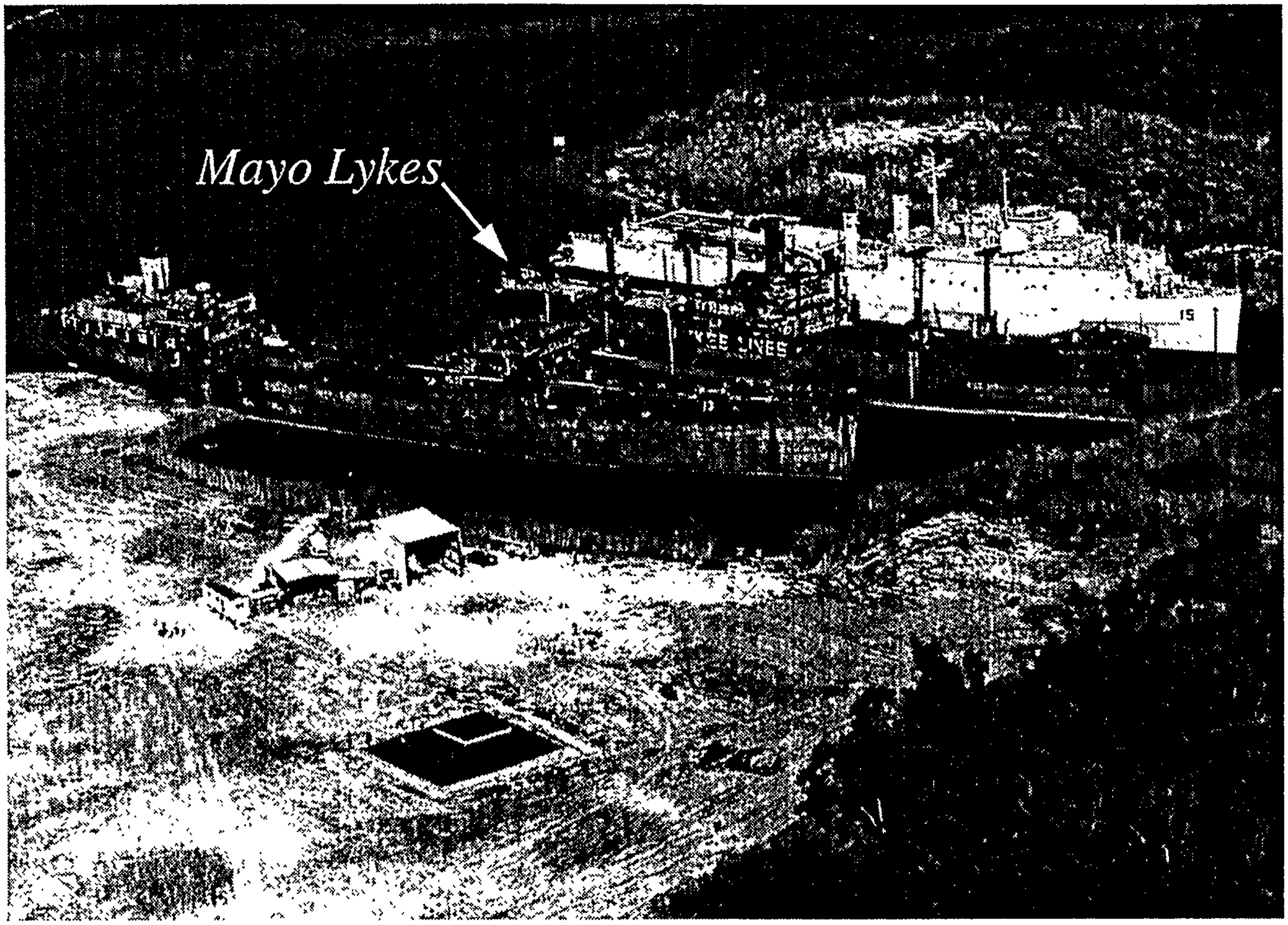


Sandia National Laboratories

ttd transportation technology development program

U.S. Department of Energy National Transportation Program

Shipboard Fire Testing

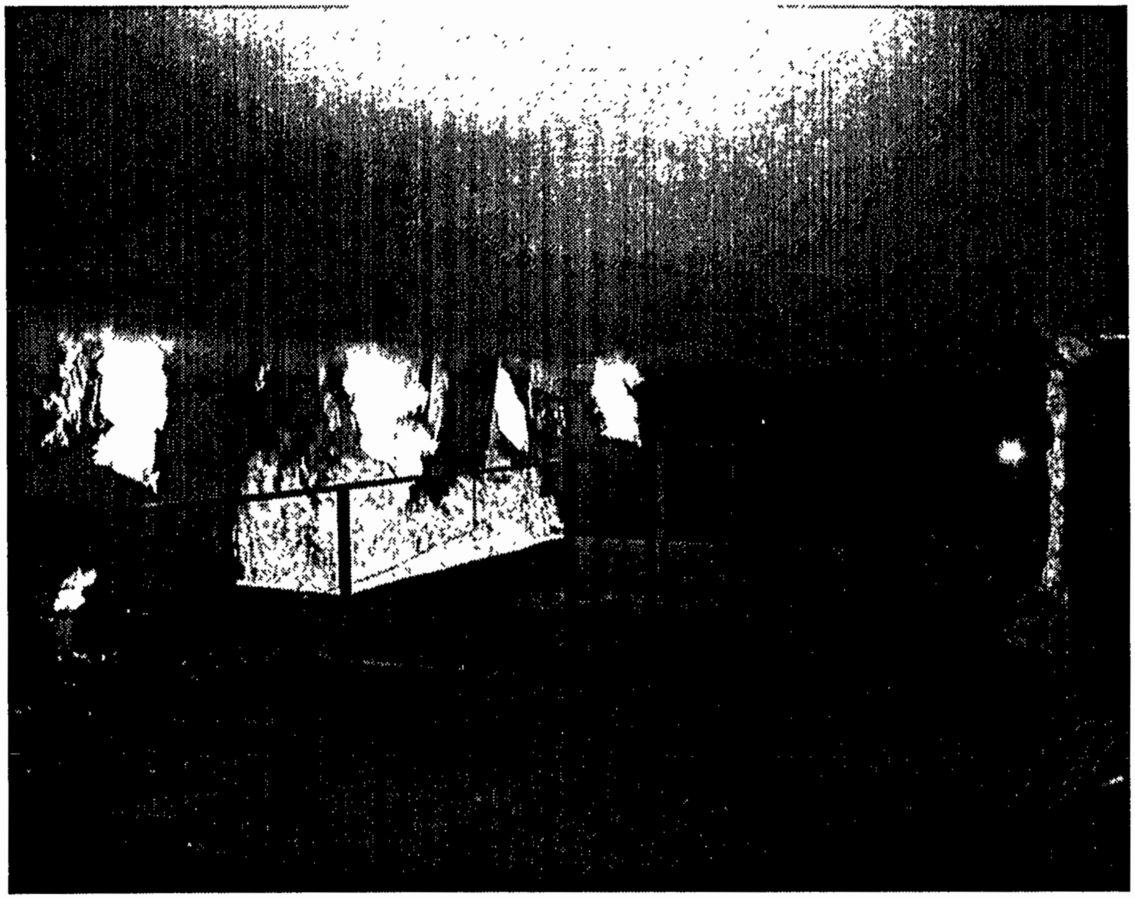


Sandia National Laboratories

ttd transportation technology development program

U.S. Department of Energy
National Transportation Program

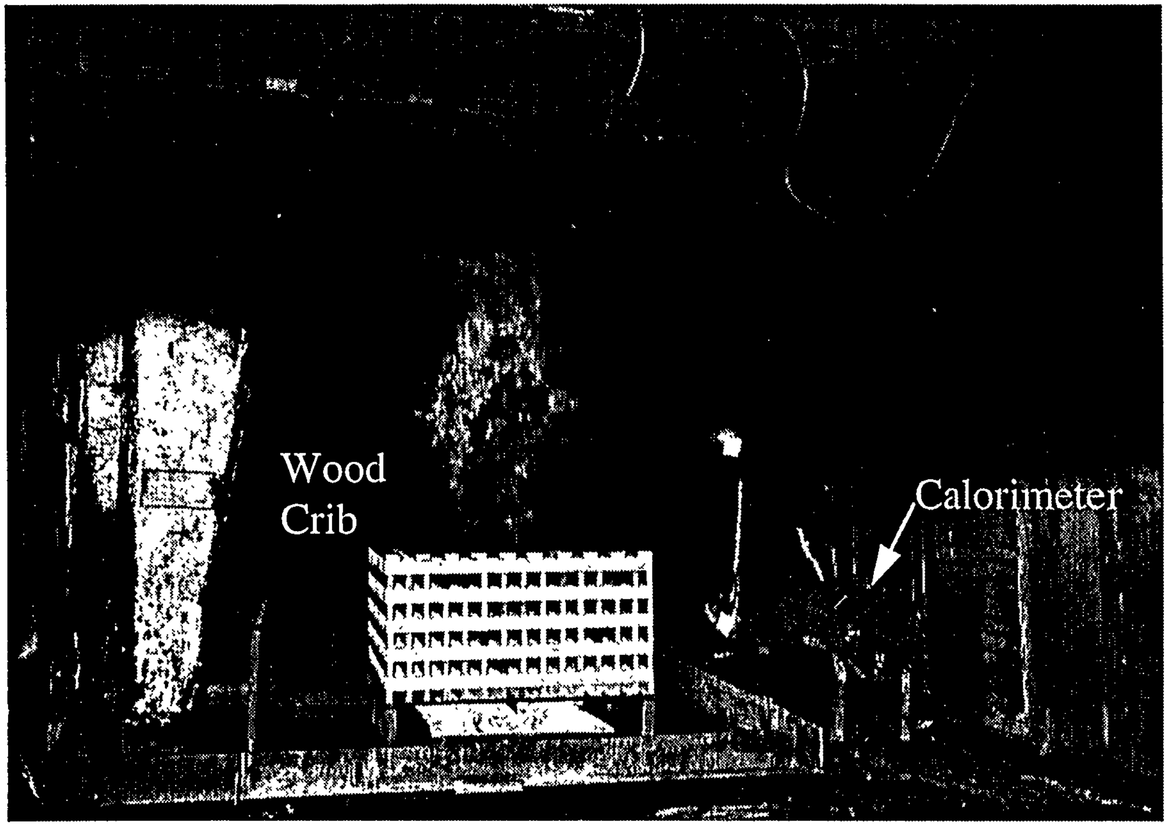
Heptane Spray Fire in Ship Hold



This 4-burner heptane spray fire on the *Mayo Lykes* used additional diesel fuel to create smoky conditions in hold

Example: Thermal Analysis

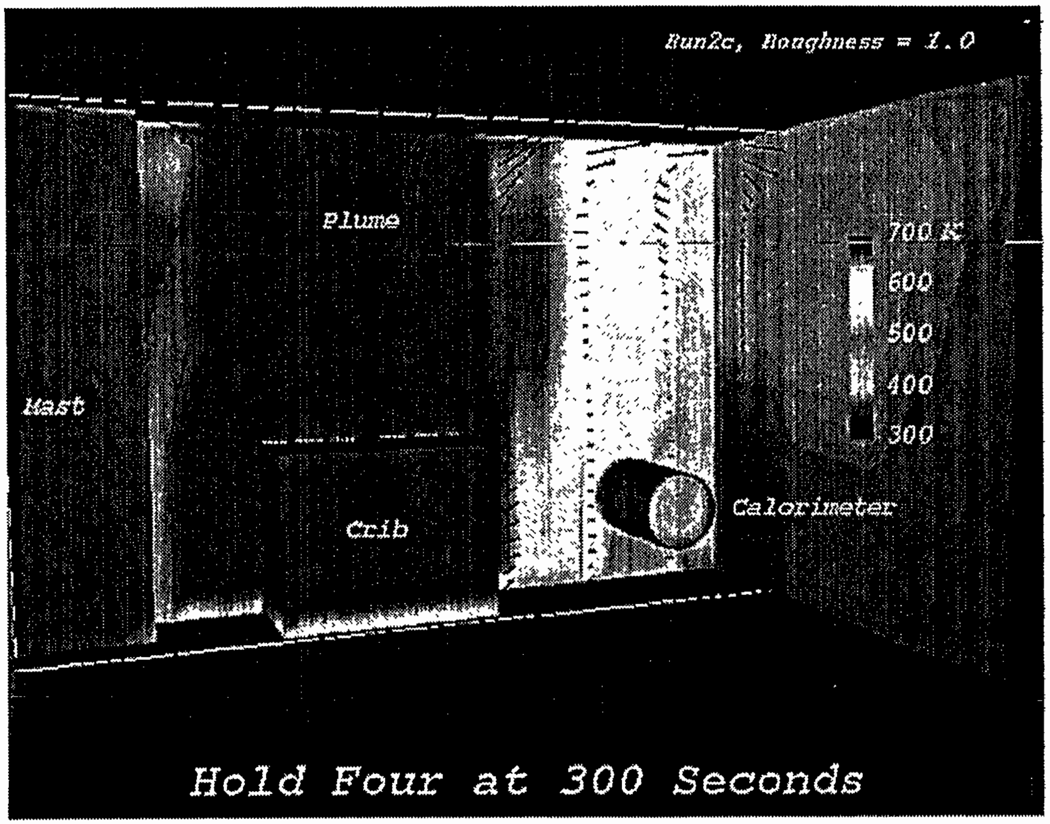
Ship Hold Fire Experiment



Experimental arrangement in Hold 4 of *Mayo Lykes* at Mobile, Alabama

Example: Thermal Analysis

Ship Hold Fire Calculations

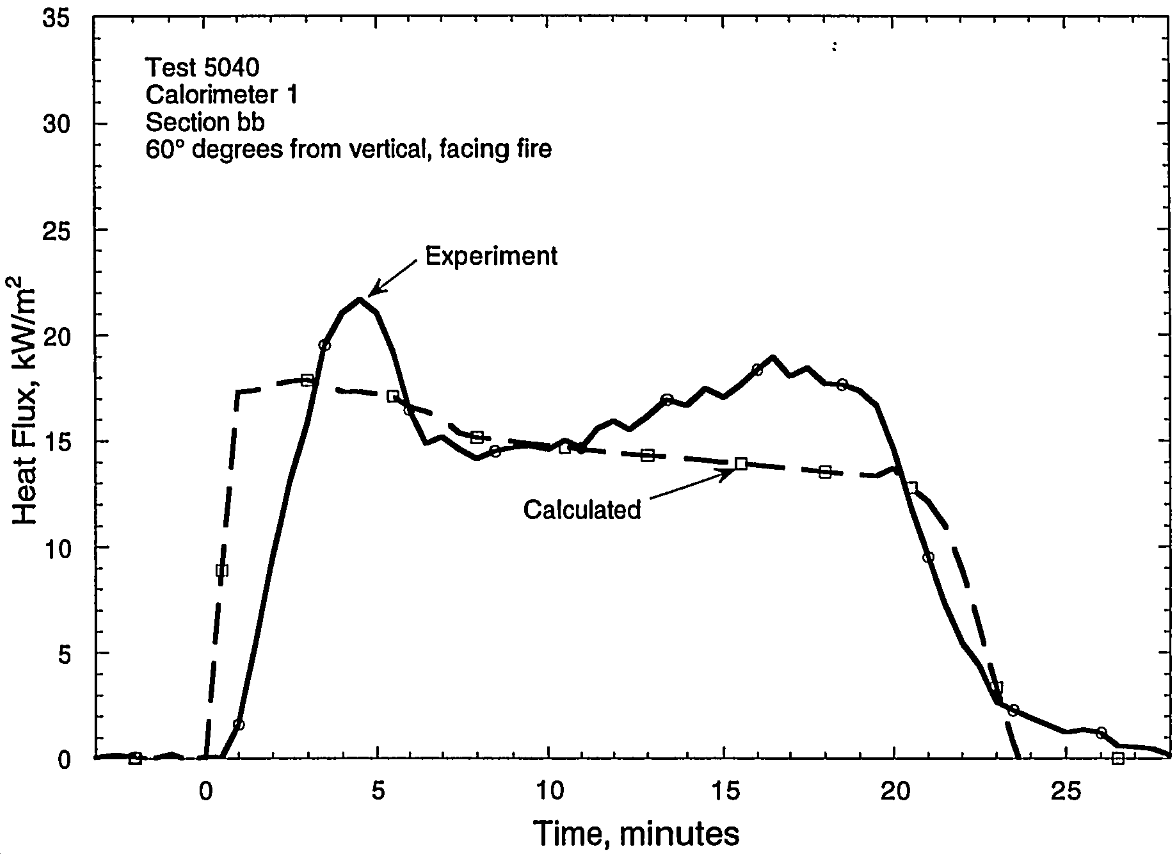


We can now successfully predict the shipboard fire environment with the use of computational fluid dynamics and other codes

Note color bar indicating local temperatures

Example: Thermal Analysis

Calculation vs. Experiment



Calculated heat transfer to simulated package closely matches experimental values. Calculations also confirm that thermal radiation is main heat transfer mechanism.

Sandia National Laboratories

ttd transportation technology development program

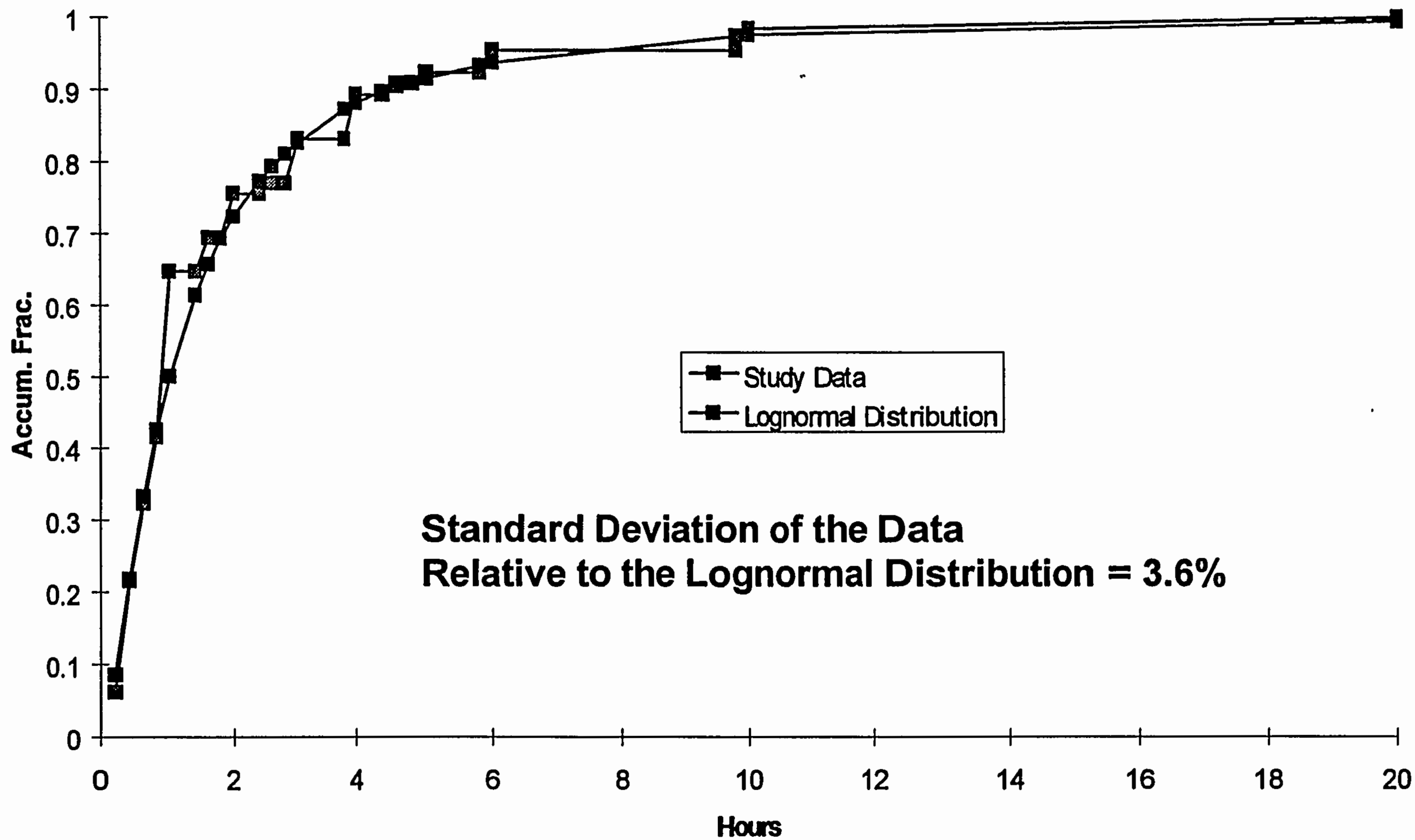
U.S. Department of Energy National Transportation Program

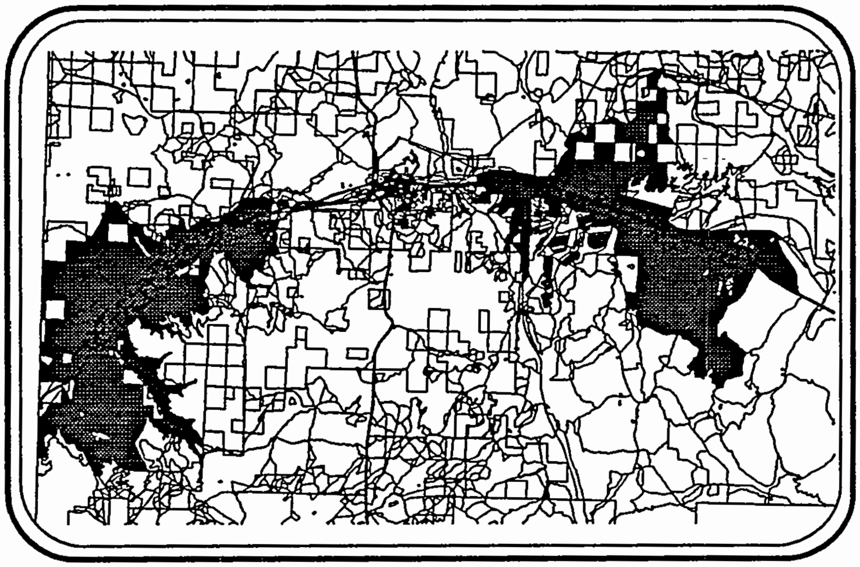
Container Analysis Fire Environment Model

- Models fire environment including local variations
- Integrated into standard heat transfer analysis code (MSC/Thermal)
- Runs in reasonable time on a standard computer work station
- Available to package designers and analysts

Goal: Give designers the confidence that their package will pass on the first try.

Figure I - Cumulative Histogram of Evacuation Times and Lognormal Distribution

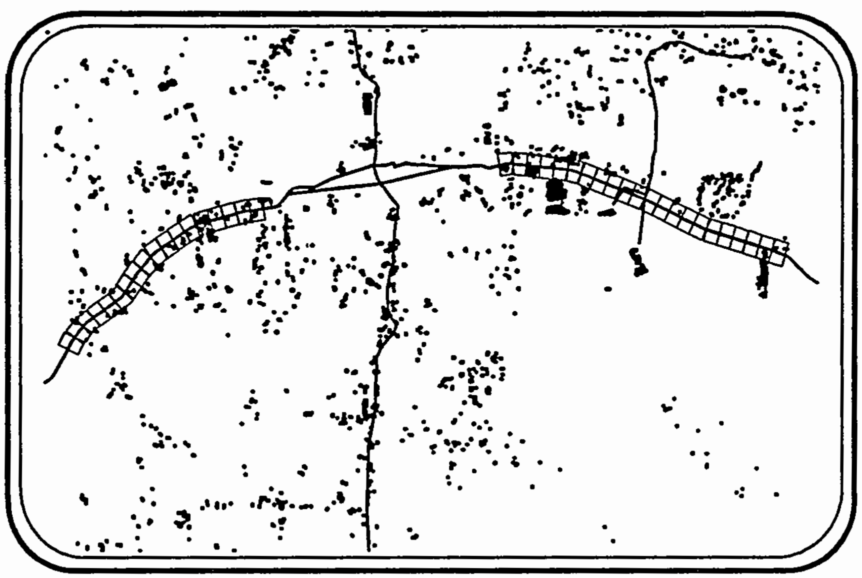




Sandia National Laboratories

ttd transportation technology development program

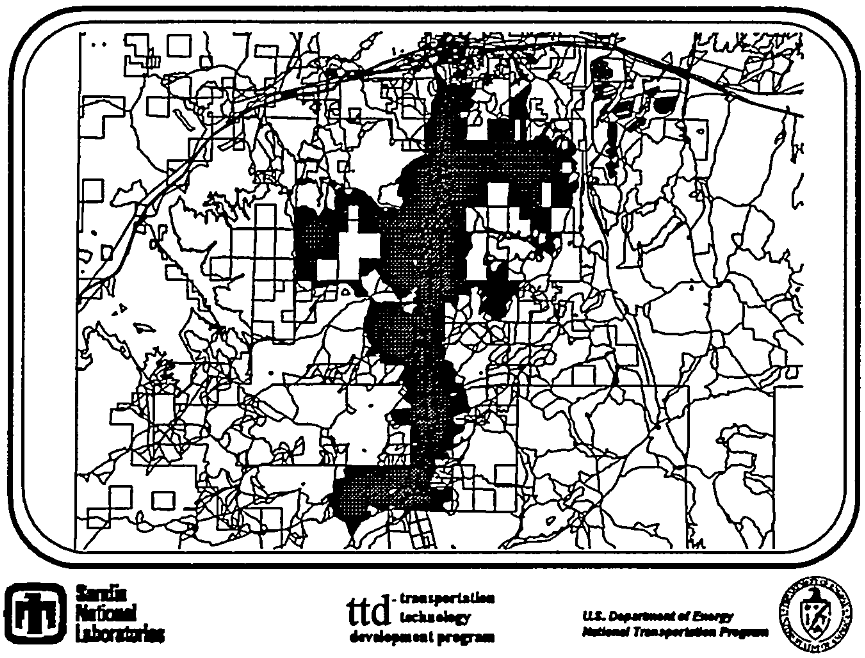
U.S. Department of Energy National Transportation Program

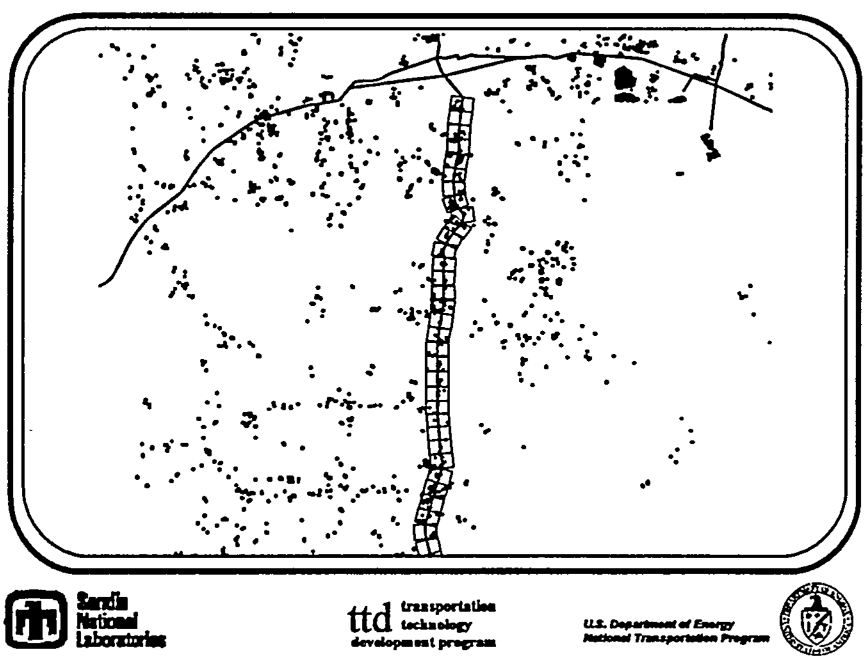


Sandia National Laboratories

ttd transportation technology development program

U.S. Department of Energy National Transportation Program


Sandia National Laboratories
ttd transportation technology development program
U.S. Department of Energy National Transportation Program


Sandia National Laboratories
ttd transportation technology development program
U.S. Department of Energy National Transportation Program

Architectural Surety

Dennis Miyoshi, Director
Security Systems and Technology

Architectural Surety Methodology

Using the Risk Equation for the Surety of Buildings and Structures

Presented to the Risk Panel

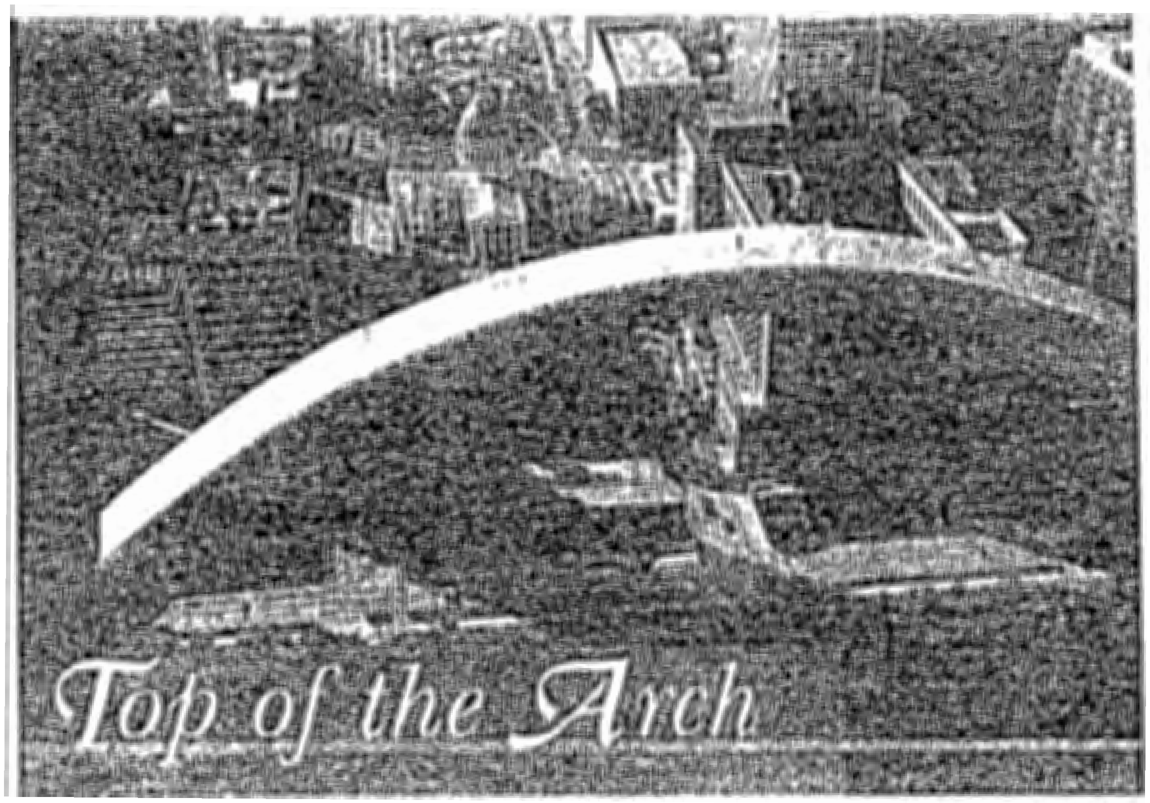
July 1, 1997

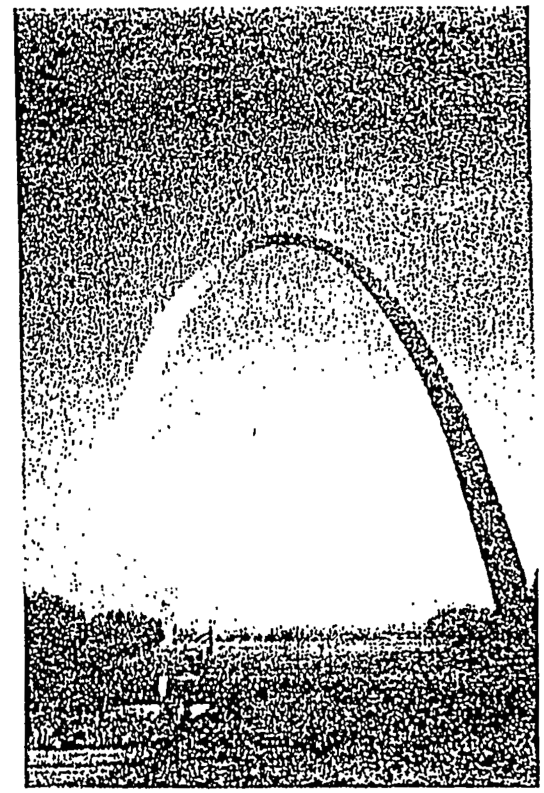
Sandia Proprietary Information

Architectural Surety....

- **What is it?**
- **What is it good for?**
- **How do we measure it?**
- **How do we know how good it is?**

Sandia Proprietary Information


Top of the Arch



Define surety....

- *Surety* is confidence that a system will perform in *acceptable* ways in both *expected* and *unexpected* circumstances

- *Surety* describes an elevated state of *safety* and *security*, a state which is *under control* and very *reliable*

Define Architectural Surety....

- *Architectural surety* is a *risk management* approach to providing confidence that buildings and infrastructures will perform in acceptable ways in *normal*, *abnormal*, and *malevolent* environments

Using Architectural Surety will....

- enhance reliability, safety, and security under normal, abnormal, and malevolent environments
  - » resistance to aging and weathering
  - » protection against natural disasters and fire
  - » protection against crime and terrorism

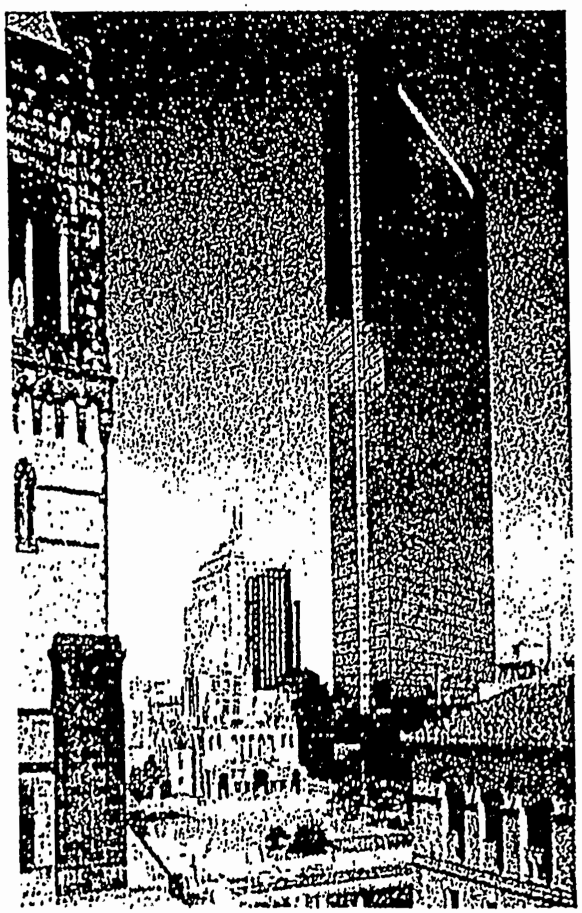
Our approach....

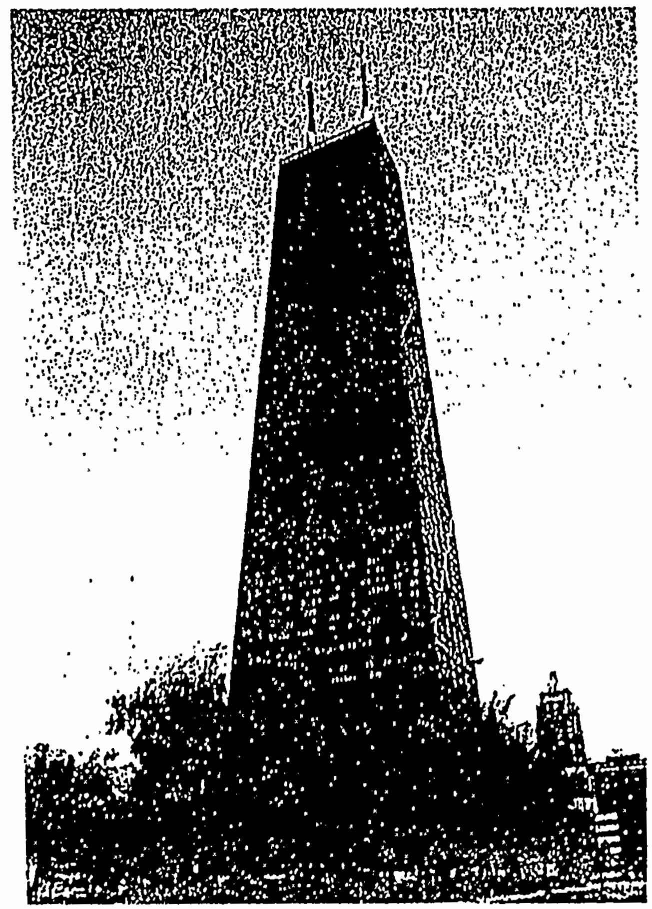
- develop a consequence-based methodology that utilizes the risk equation to rigorously determine how resources should be allocated to cost-effectively improve surety.
- we call this methodology: Engineered Surety Using the Risk Equation (EnSURE)

Sandia Proprietary Information

Architectural Surety

Hancock Buildings (Boston and Chicago)



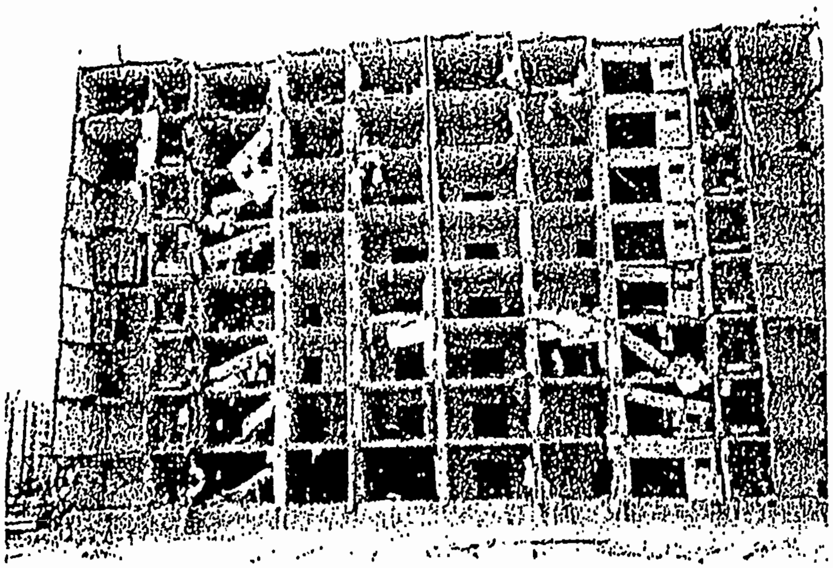


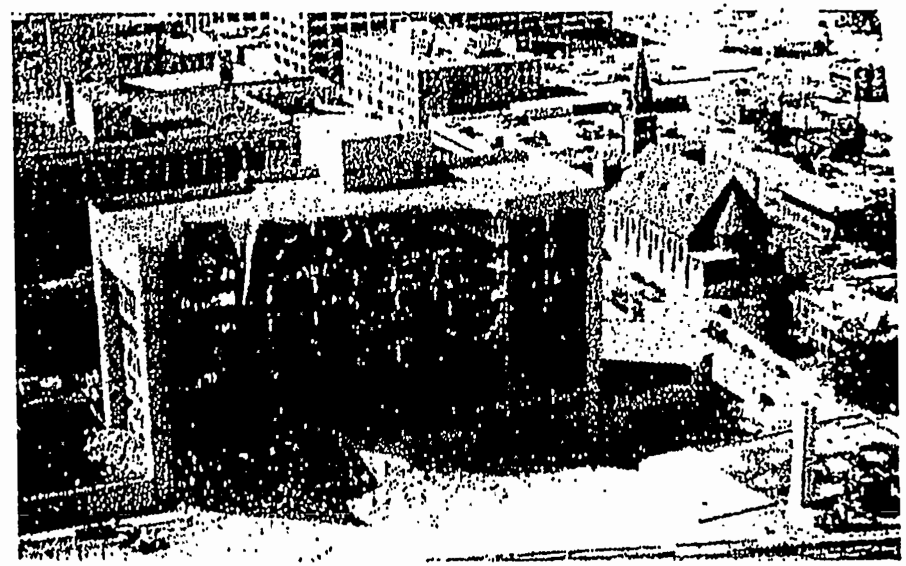
RVM, 5822 6/16/97 Arch_Photos.ppt 2

Sandia National Laboratories

Architectural Surety

Khobar Towers and Murrah Building





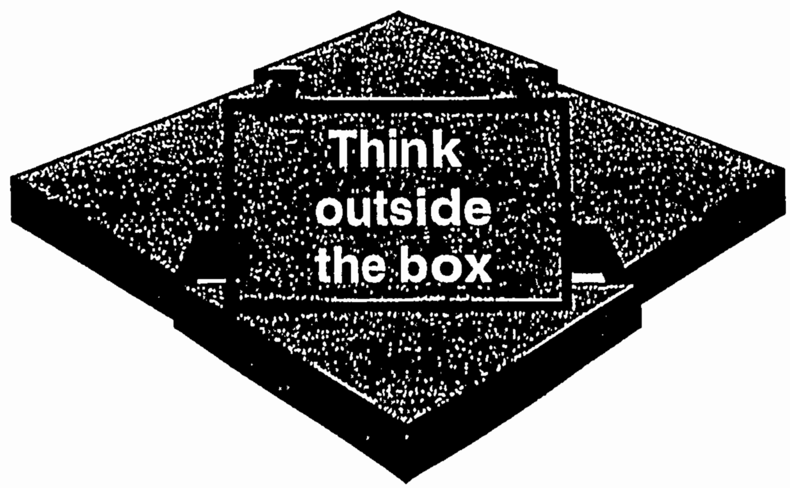
RVM, 7822 6/16/97 Arch_Photos.ppt 11

Sandia National Laboratories

Architectural Surety

Passion

Intuition



Creativity

Innovation

Sandia National Laboratories

Education

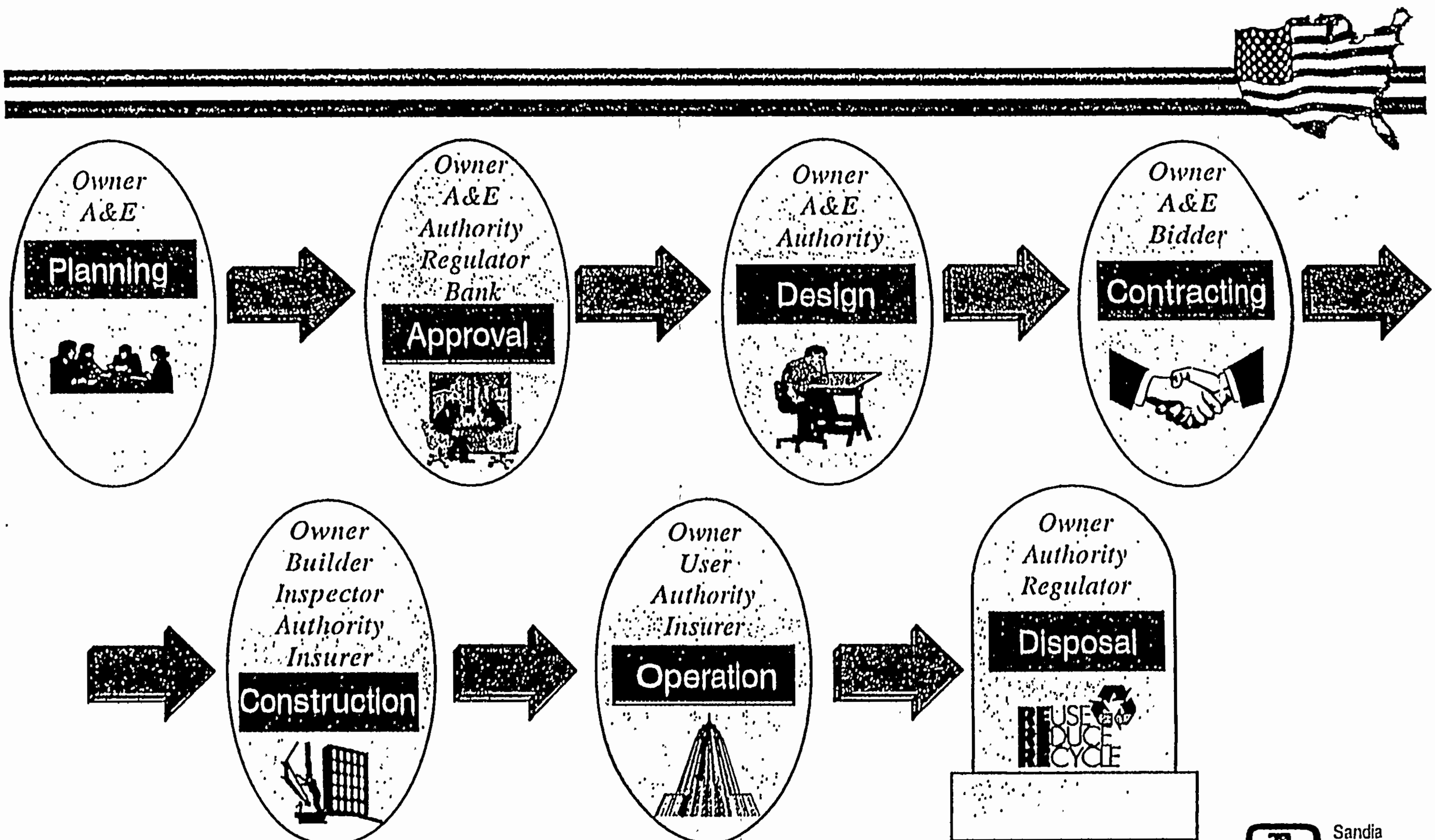
Graduate Level Course
Civil Engineering Department, University of New Mexico

Infrastructure Surety Curriculum, Jan - May 1997

- Threat Assessment
- Security
- Safety
- Reliability Analyses
- Risk Management
- Computational Modeling and Simulation
- Project Development and Life-Cycle Engineering
- Performance Codes and Standards
- Ethics and Legal Issues
- Failure Analysis and Case Histories

Sandia
National
Laboratories

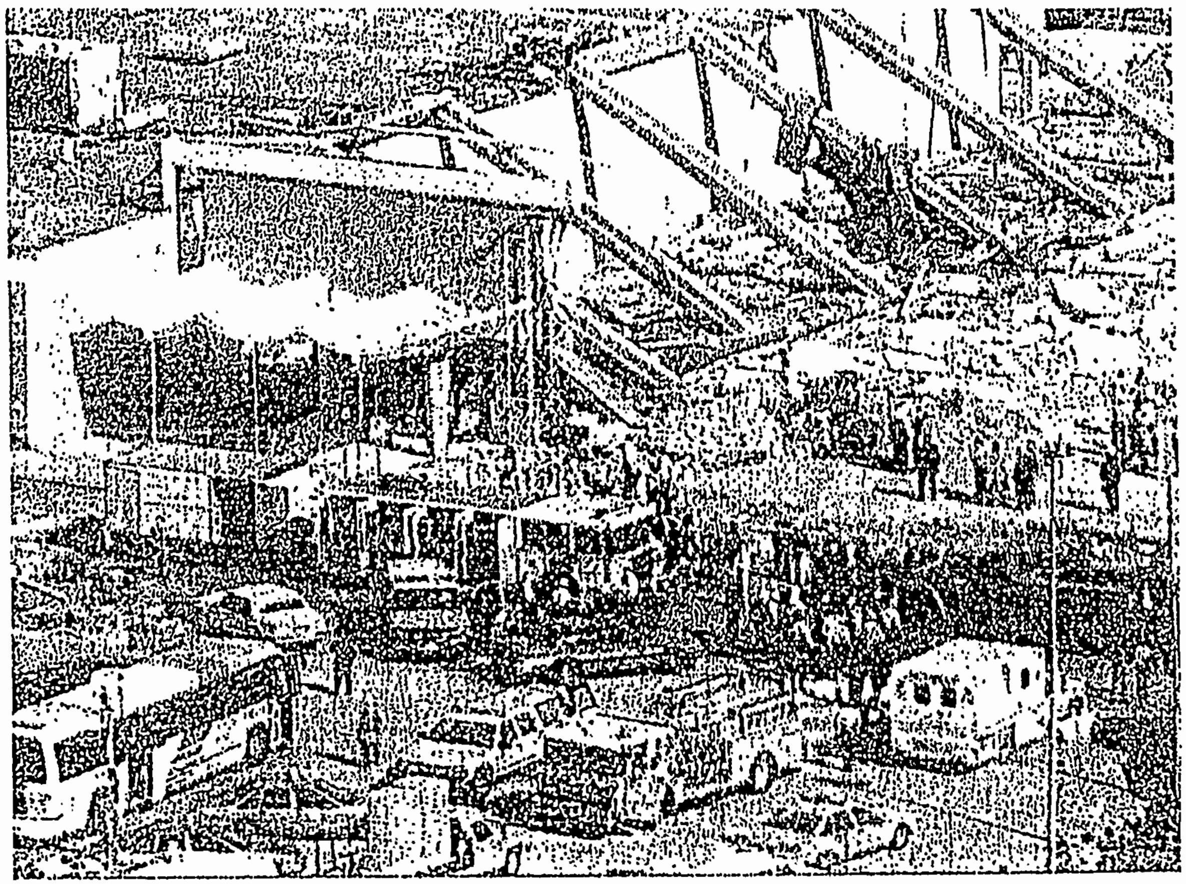
Life-Cycle Sustainable Development



Sandia National Laboratories

Architectural Surety

Houston Mall, 1997

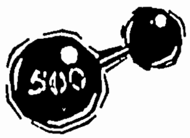


RVM. 5822 6/16/97 Arch Photos.ppt 9

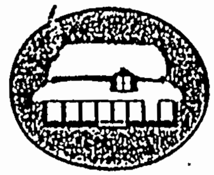
© Sandia National Laboratories

Sandia National Laboratories

Design Loads for Buildings and Infrastructures



Dead Loads



Snow Loads

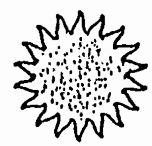
Soil and Hydrostatic Pressure

Flood Loads

Live Loads

Dynamic Loads

Wind Loads



Thermal Loads

Rain Loads

Settlement Loads

Earthquake Loads

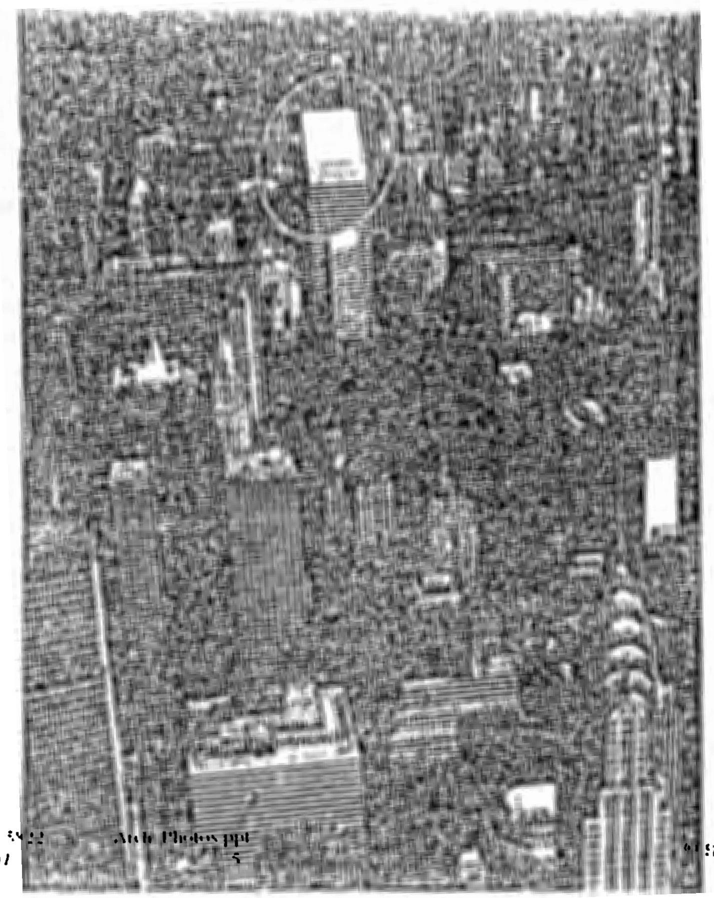
Ice Loads

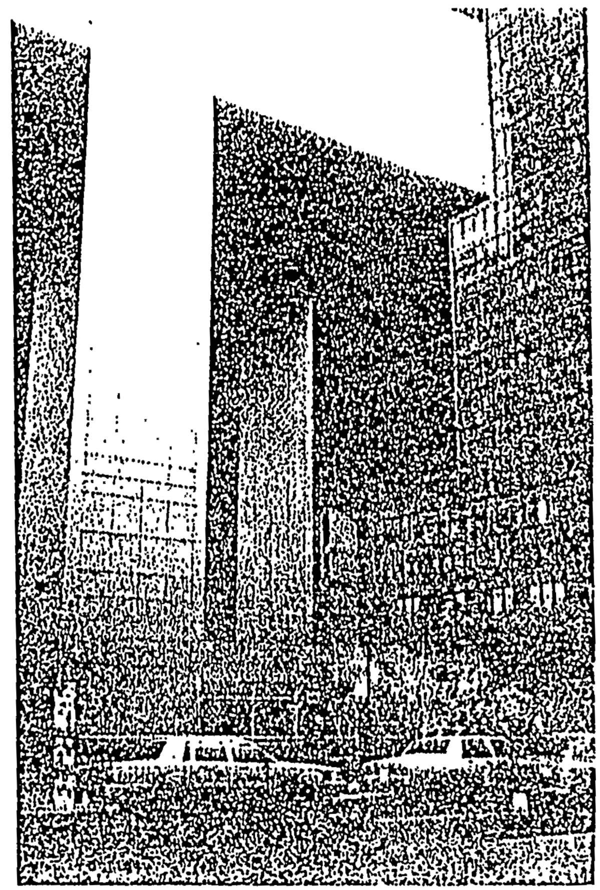
Blast Loads

Sandia National Laboratories

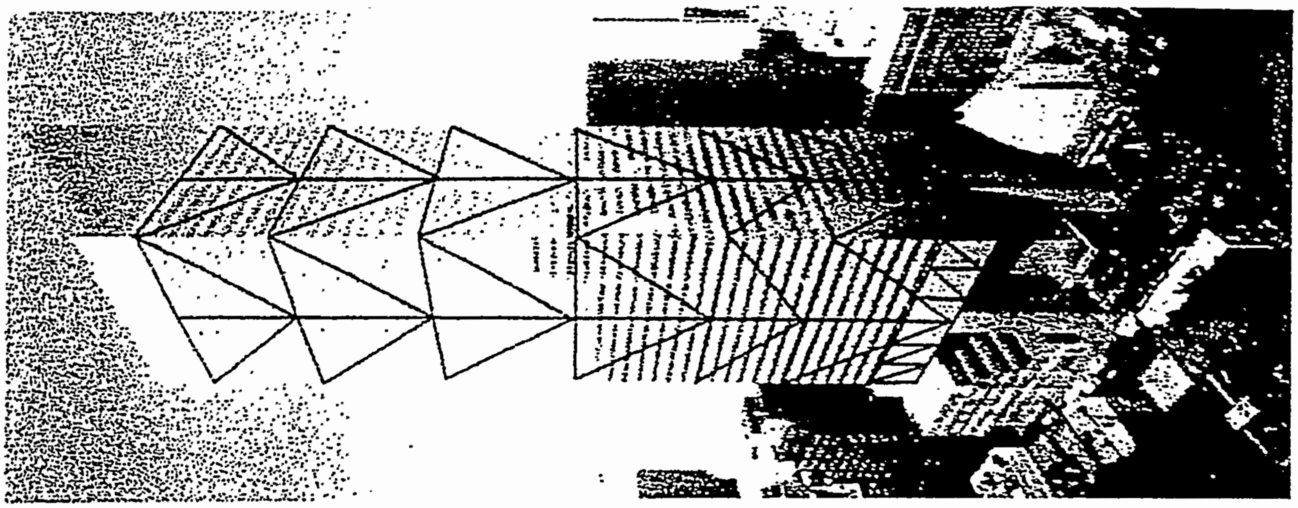
Architectural Surety

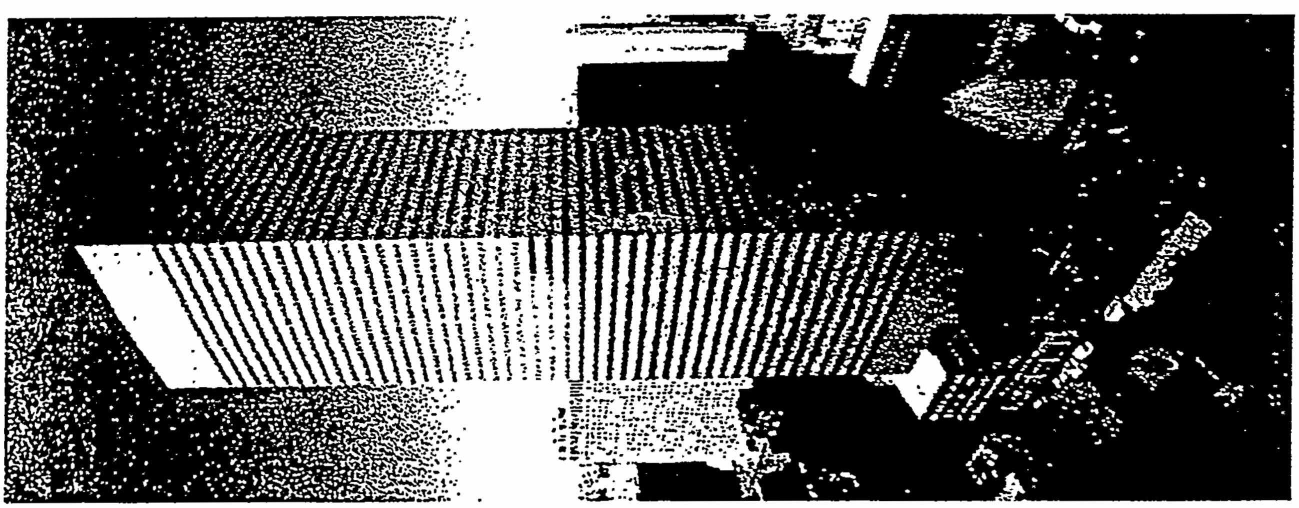
Citicorp Building, NYC





Sandia National Laboratories





The EnSURE methodology consists of....

- establish consequences
- define the threat spectrum
- formulate the risk equation
- characterize the facility
- identify the targets
- evaluate the protection effectiveness
- develop improvement options
- perform benefit/cost analysis

The methodology can be qualitative or quantitative....

- The qualitative approach uses expert judgement wherever possible
  - » can be done quickly at low cost
- The quantitative approach uses models, logic trees, and criteria to establish priorities
  - » rigorous, with good documentation

The process begins with a consequence analysis....

- identify the critical issues
  - » mission, people, assets, environment, confidence
- determine what is valued by the stakeholders
- determine the interrelationships
- determine the priorities

Sandia Proprietary Information

The Vital Issues Process provides these features....

- brings together a panel of stakeholders
- identifies the portfolio of consequences to be avoided
- identifies, defines and weights the evaluation criteria
- ranks the portfolio according to the criteria

Sandia Proprietary Information

Define the threat spectrum....

- establish the attributes
  - » aging, wind, earthquake, flood, fire, adversaries
- define the threat scenarios
- use experts to select threats to be considered, *or*
- use threat methodology to prioritize, driven by the consequence analysis

Establish the risk equation....

- Risk = L * (1-P(E)) * C
  - » L = likelihood of occurrence
  - » P(E) = system effectiveness in prevention
  - » C = consequence
  - » for the malevolent threat, L and P(E) may be dependent variables
- use risk matrix (C vs. L) to prioritize, *or*

- use risk model

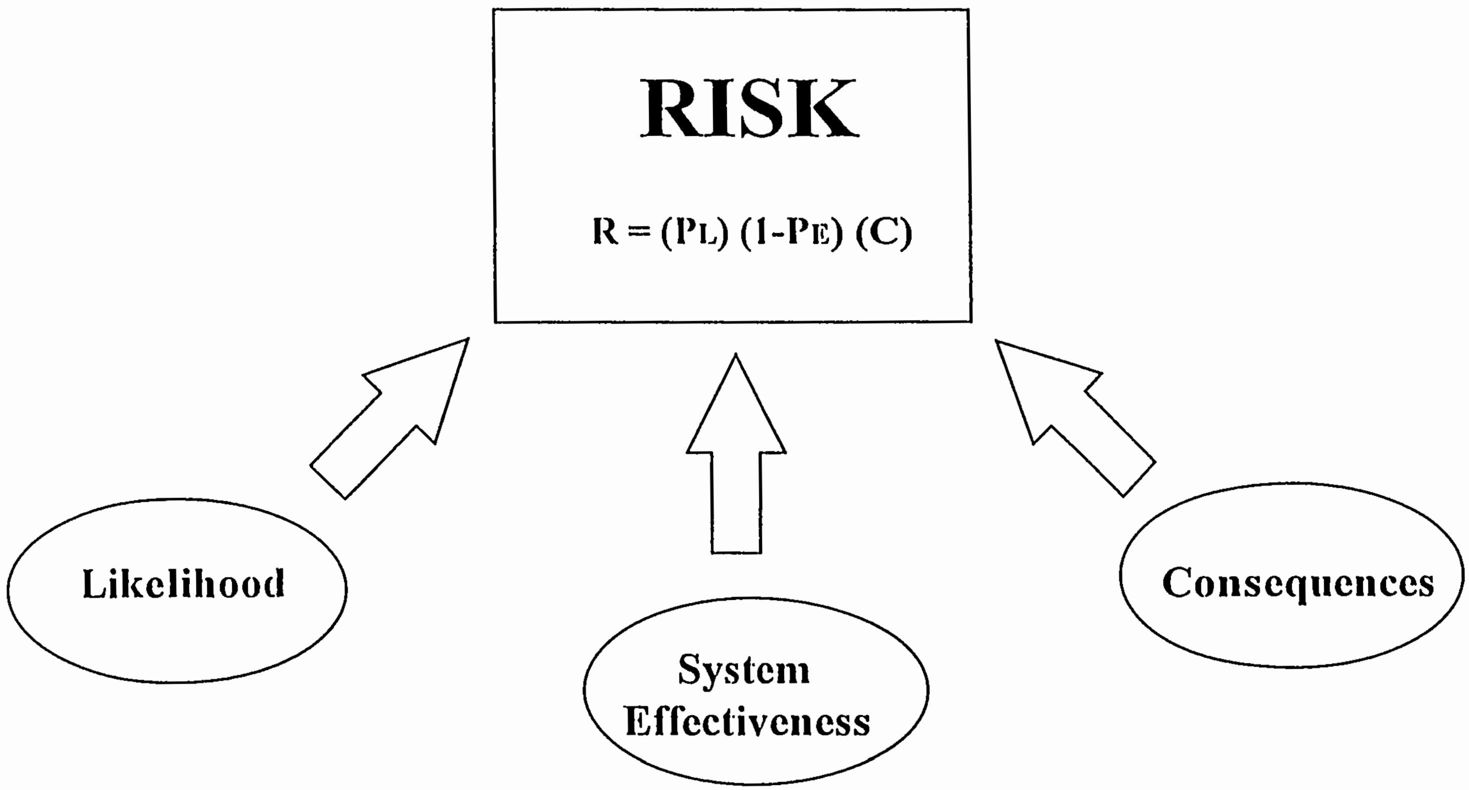
Prevention begins with facility characterization....

- consider mission, people, assets, environment, and confidence
- may need to include time and motion studies as variables change
- can be done with experts, *or*
- can develop a facility model based upon event trees leading to undesired outcomes

Continue with target identification....

- use the outputs from the risk equation and the facility characterization to identify the targets
- can be done with experts, *or*
- can develop a target model using inputs from the risk model and facility model

Engineered Surety Using Risk Equation (EnSURE)



Sandia Proprietary Information

Risk Analysis
(Albuquerque Pump Station - 2)

- Determine level of consequence
- Estimate probability of occurrence
- Fill in matrix for infrastructure

High Cons	Chem/Bio (Terrorist)		
Med Cons	Sabotage (Insider)	Sabotage (Upset Citizen)	
Low Cons			Graffiti (Kids)
	Low Prob	Med Prob	High Prob

Perform the system effectiveness evaluation

- identify the protection elements
- evaluate the effectiveness of the system
- use expert judgement, *or*
- select from a suite of evaluation tools
  - » structural analysis, single point failure analysis, blast effects, security analysis

Sandia Proprietary Information

Develop a suite of improvement options....

- structural improvements
- technologies
- reallocation of resources/assets/missions
- policy/procedures/training
- emergency preparedness

Sandia Proprietary Information

Develop
system design options....

- hardware emphasis
- policy/procedure emphasis
- mixed or balanced
- determine the risk for the baseline
- determine the risks for the upgrades

Sandia Proprietary Information

Do the benefit/cost analysis....

- establish the benefits (reduction in risk) for each option
- establish the cost (including operations and maintenance) for each option
- use expert judgement to evaluate, *or*
- use the Cost/Performance Analysis tool

Sandia Proprietary Information

Make the decision....

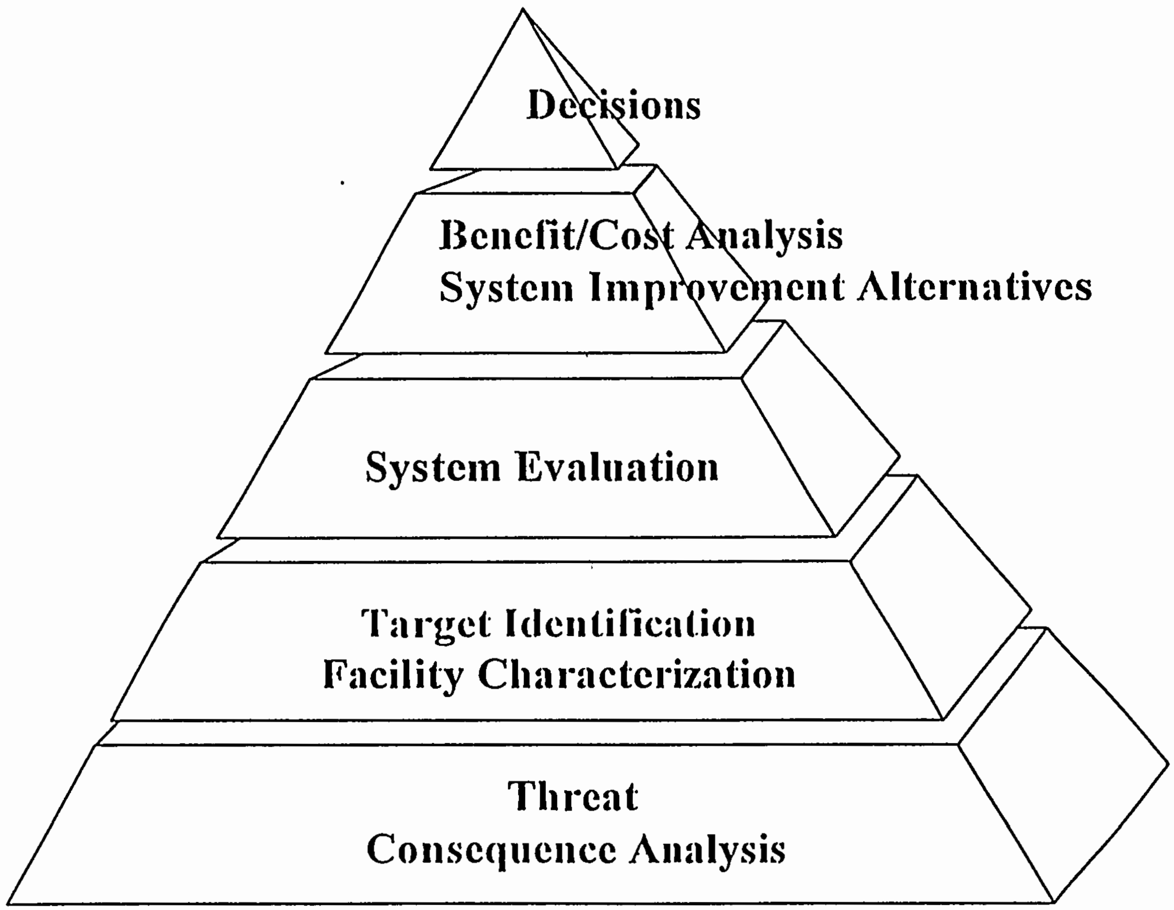
- decide which risks to mitigate, which risks to accept
- select the improvement option
- document the process and the rationale for the decision
- implement the decision

The EnSURE methodology provides....

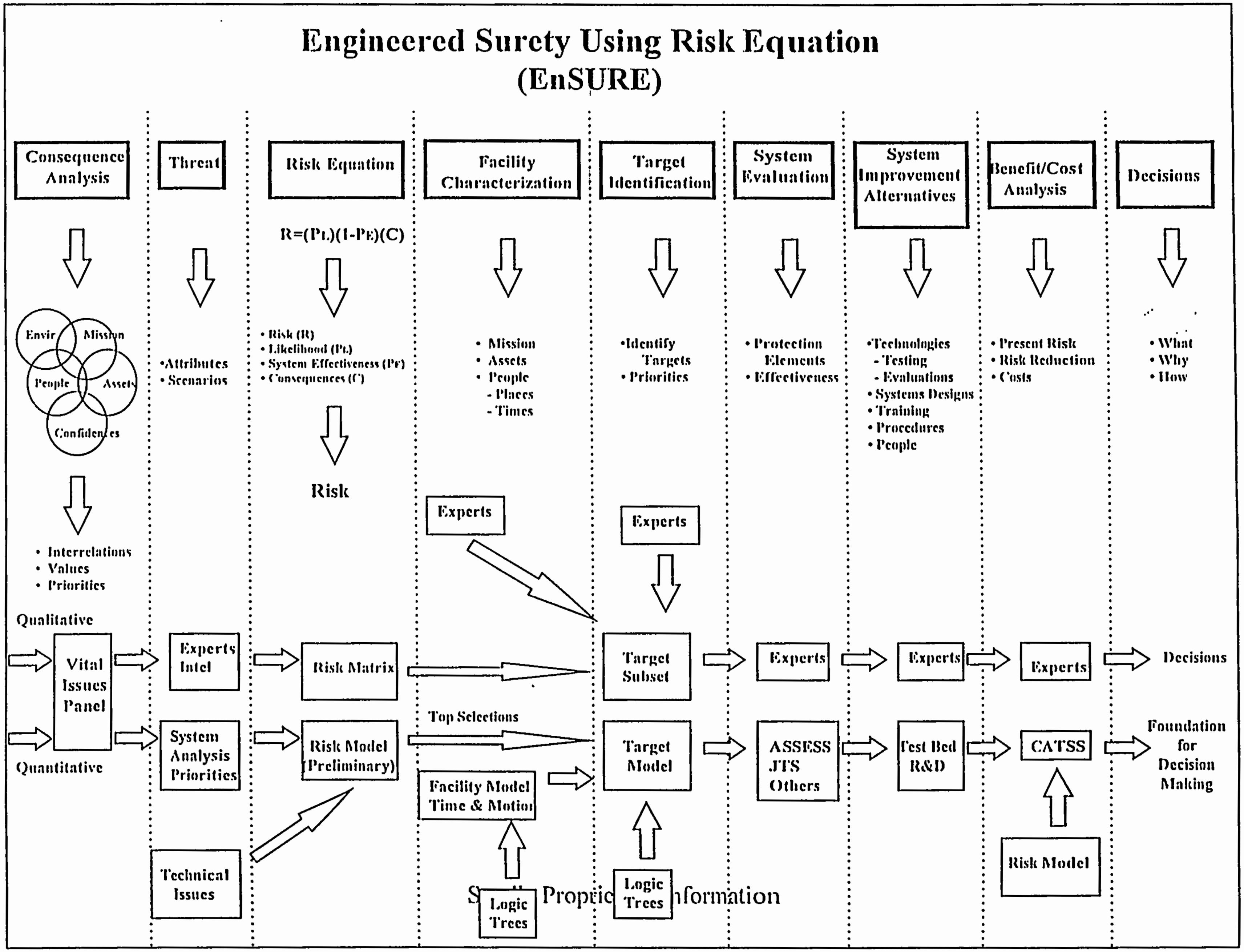
- the risk equation for evaluating diverse factors and values
- a rigorous foundation of knowledge for decision making
- the ability to do sensitivity analysis and evaluations of improvement options

Sandia Proprietary Information

Engineered Surety Using Risk Equation (EnSURE)



Sandia Proprietary Information


Engineered Surety Using Risk Equation
(EnSURE)
Consequence Analysis
Threat
Risk Equation
Facility Characterization
Target Identification
System Evaluation
System Improvement Alternatives
Benefit/Cost Analysis
Decisions
R=(PL)(1-PE)(C)
Envir
Mission
People
Assets
Confidences
• Interrelations
• Values
• Priorities
•Attributes
•Scenarios
• Risk (R)
• Likelihood (PL)
• System Effectiveness (PE)
• Consequences (C)
Risk
• Mission
• Assets
• People
- Places
- Times
•Identify Targets
• Priorities
• Protection Elements
• Effectiveness
•Technologies
- Testing
- Evaluations
• Systems Designs
• Training
• Procedures
• People
• Present Risk
• Risk Reduction
• Costs
• What
• Why
• How
Experts
Experts
Qualitative
Vital Issues Panel
Quantitative
Experts Intel
System Analysis Priorities
Technical Issues
Risk Matrix
Risk Model (Preliminary)
Top Selections
Facility Model Time & Motion
Logic Trees
Target Subset
Target Model
Logic Trees
Experts
ASSESS JTS Others
Experts
Test Bed R&D
Experts
CATSS
Risk Model
Decisions
Foundation for Decision Making

Risk Methods and Supporting Activities; Decision Support

Paul Davis, Manager
Environmental Risk and Decision Analysis Department

Environmental Risk Assessment at Sandia National Laboratories

- Methods -

Paul Davis
Ken Sorenson
Mert Fewell

July 2, 1997

Applications of Environmental Risk Assessment at Sandia

- **Post-Closure Assessment of Radioactive Waste Disposal Sites**
- **Environmental Restoration**

Approach to this Presentation

Since the basic methods behind these programs are the same or similar

– we will attempt to use a common framework for discussing the basic methods used in all environmental risk and decision analysis programs -

Common Framework

- The Ordered Triplet -

- **What can happen?**
- **How likely is it?**
- **What are the consequences?**

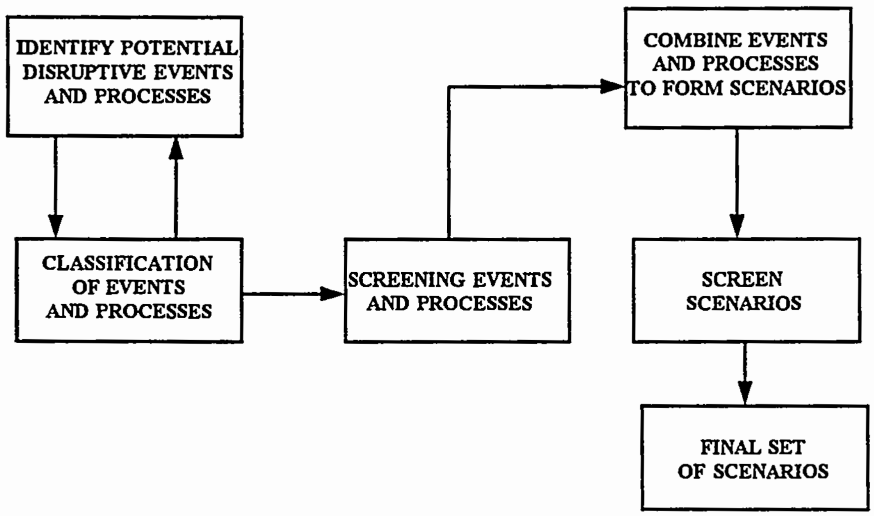
- Plus Decision Analysis -

- **Now What?**
  - **Is the risk acceptable?**
  - **If not, then what?**
    - **reduce uncertainty?**
    - **redesign/remediate?**

TRU and High-Level Waste Disposal

What Could Happen?	How Likely is it?	What are the consequences?
All adverse natural and human-induced scenarios	All scenarios assigned probabilities	Integrated release and/or dose simulated using models of release and transport phenomena Explicit treatment of uncertainty required

TRU and High-Level Waste Disposal
- What can happen? -



TRU and High-Level Waste Disposal
- How Likely is it? -

Probabilities of Scenarios Estimated Through:
- **Frequency Data (ex. recurrence intervals)**
- **Models of physical processes**
- **Formal Elicitation of Expert Judgment**

TRU and High-Level Waste Disposal
- What are the consequences? -

- **Estimates of Consequences are a combination of simulation results and parameter (and model) uncertainty where:**
  - **Simulations are based on models of physical processes of contaminate release and transport**
  - **Parameter uncertainty is propagated via Monte Carlo methods**
  - **Multiple approaches to the treatment of model uncertainty are being tried**

Processes for which Models have been Developed and/or Modified

- Density dependent brine transport
- Rock deformation including salt creep and formation fracturing
- Gas generation and gas phase transport
- Ground water flow and transport in:
  - Saturated and unsaturated media
  - Fractured and non-fractured media
- Direct releases due to drilling and volcanism
- Environmental Transport
  - surface-water transport
  - air transport
  - plant and animal uptake (including eco-risk)
  - direct and indirect human exposure

Examples of Codes Developed at Sandia for Environmental Risk Assessment

TOSPAC	LHS	CAMCON
NEFTRAN (I&II)	STEPWISE	SEDSS
BRAGFLOW	GEOINVS	CURE
SANTOS	SWIFT (I &II)	DANDD
SECOFL2D	PRECIS	PAGAN
SECOTP2D	GANT	DCM3D
PANEL/NUTS	GENII-S	GRASP-INV
CUTTINGS	OPTIMUS	BOSS

Treatment of Parameter Uncertainty

- Use representative, unbiased probability density functions (Pdfs) based on both existing information recognizing that:
  - Pdfs used in risk assessment usually include information about uncertainty as well as natural variability
  - It is difficult to separate parameter uncertainty from model uncertainty (includes distribution models and process models)
- Incorporate correlation between and among parameters (geostatistics)
- Propagate parameter uncertainty using a Monte Carlo method - Latin Hypercube Sampling
- Use intermediate measures of system performance to reduce uncertainty in parameter variability

LATIN HYPERCUBE SAMPLING (LHS)

- Divide distribution into equally probable intervals
- Sample a value from each interval
- Each parameter value from a given sample is randomly paired to values from other parameters in the sample

Treatment of Parameter Correlation

- Rank correlation based on empirical evidence or expert judgment (i.e., porosity & permeability)
- Spatial correlation
  - kriging
  - co-kriging (with and without process modeling)
  - geostatistical simulation
  - geologic simulation

Use of Intermediate Measures to Reduce Uncertainty in Parameter Variability

No measured values of consequences (dose, integrated release, etc.) are available but measurements of indirect model outputs are available and are used to condition model input, for example:

- measured hydraulic heads (static and stress-induced) are used in inverse procedures
- isotopic age dating is used to condition advective velocity estimates

Treatment of Model Uncertainty

- **Model "Validation"**
  - International Studies (INTRACOIN, HYDROCOIN, INTRAVAL)
  - Site Specific Model Testing
- **Probabilistic weighting of multiple conceptual models**
- **Process based approaches** (SEDSS, initial version of SPM)
  - Premise - "all models are wrong some are useful"
  - Develop models in the context of the decision to be made
  - Analyze all models that can be defended using existing information
  - Focus resources on models that cause regulatory violations

NRC Dose Assessments

- Low-Level Waste and Decontamination and Decommissioning -

What Could Happen?	How Likely is it?	What are the consequences?
Pre-Defined Generic Scenarios	*Probability Assumed = 1*	*Pre-Defined Generic Pathways (and Parameters)* Simulations of dose performed using process models of release and transport Uncertainty in models and parameters are addressed

NRC Dose Assessments

- Low-Level Waste and Decontamination and Decommissioning -

- **Process models developed for TRU and HLW disposal modified first for LLW and then further modified for D&D**
- **New models developed and/or modified for surface processes and biosphere transport**
- **Methods developed for TRU and HLW disposal for treating parameter uncertainty used directly in LLW and modified for D&D**

EPA Risk Assessments

What Could Happen?	How Likely is it?	What are the consequences?
Generic "Land Use" Scenarios negiotiated between the regulator, owner/operator, and the public	*Probability Assumed = 1*	*Pre-Defined Generic Pathways which may be modified with site data* Simulations of exposure performed using process models of release and transport Uncertainty in models and parameters may be addressed

EPA Risk Assessments

- Process models and methods for treating parameter uncertainty developed for TRU and HLW disposal used directly for simulating transport along pre-defined pathways
- New models developed for probabilistic treatment of biosphere transport and eco-risk
- Assumption-based modeling being developed for treating model uncertainty

EPA Assessments
- "Clean Up Levels" -

What Could Happen?	How Likely is it?	What are the consequences?
Pre-Defined and Analyzed Generic Scenarios	*Probability Assumed = 1*	*Pre-Defined and Analyzed Generic Pathways and Parameters* some allowance for "natural attenuation" being considered Uncertainty in extent and nature of the contamination is addressed

EPA Assessments
- "Clean Up Levels" -

- Natural Attenuation is an inherent part of consequence modeling used in TRU, HLW, LLW, and D&D
- New process model developed for the treatment of dense non-aqueous phase liquids (DNAPLS)
- Methods developed for addressing spatial correlation of parameters modified to minimize costs of site characterization and clean up

Decision Analysis for Waste Management and Environmental Restoration Problems

What Type of Decisions?

Three Primary Questions:

- Is the Site Safe?
- What Remedial Approach or Design Change Should Be Implemented?
- When Is the Remediation Complete?

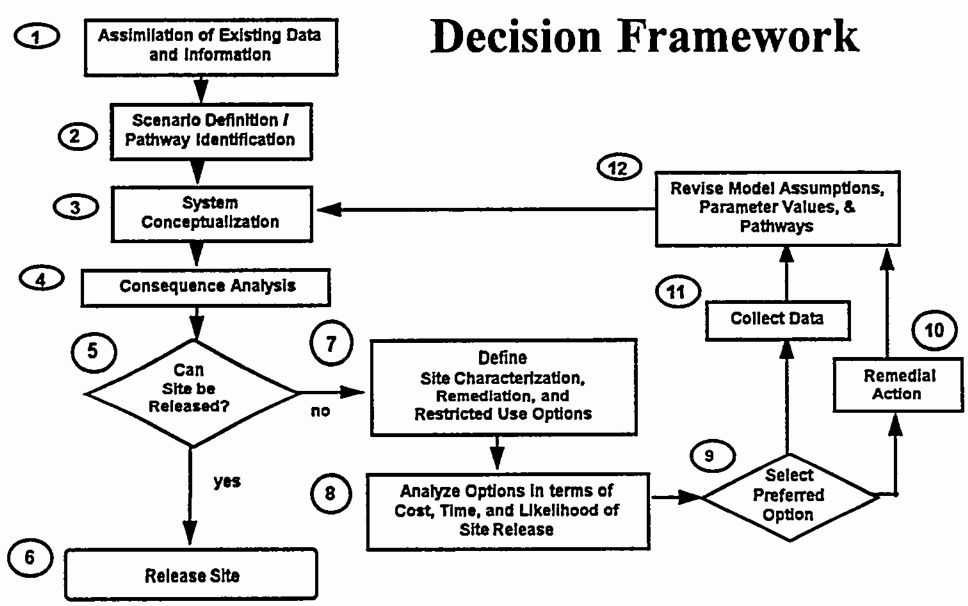
Secondary Question:

Is a Monitoring Program Adequate to Detect a Release?

While Making These Decisions, We Ask ...

Do We Need More Data, How Much, and Where Do We Collect it?

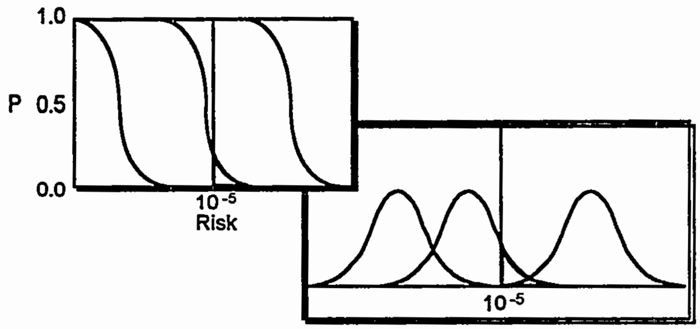
Decision Framework



Evaluation of Results

SNL has developed graphical and analytical approaches to addressing the following questions:

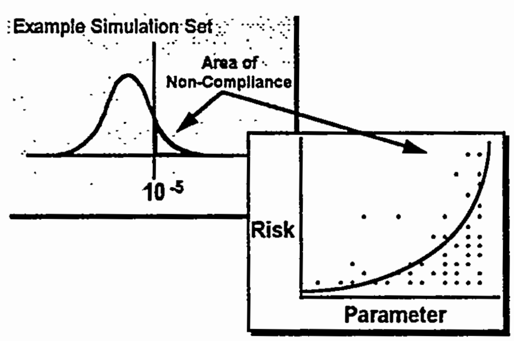
- **Is the answer unambiguous? (Red or Yellow Curves)**
- **Is more information needed to make a decision? (Purple Curve)**



SENSITIVITY ANALYSIS

Purpose: Determine which input parameter distributions/values have the most impact on the output distribution and which lead to potential non-compliance.

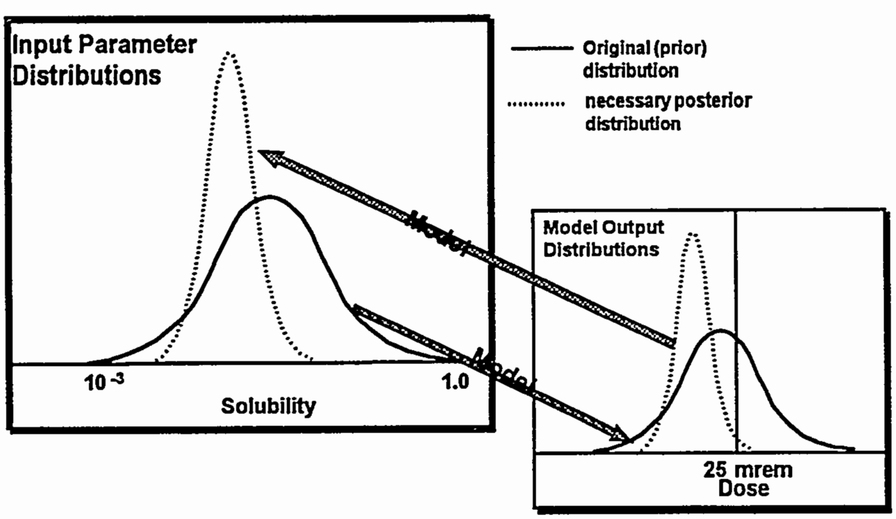
SNL Approaches: Graphical and analytical approaches have been developed including stepwise regression of ranked data, scatter plots, and interactive sensitivity analysis.



Data Worth

- Sensitivity analysis relates model input to model output and is used as a screening tool for data worth
- Data worth is focused on the allocation of resources and therefore considers the additional factors of:
  - how likely is that data collection activities will change input pdfs enough to change a decisions and
  - what is the cost associated with data collection

Updating Parameter Distributions and Determining Likelihood of Success

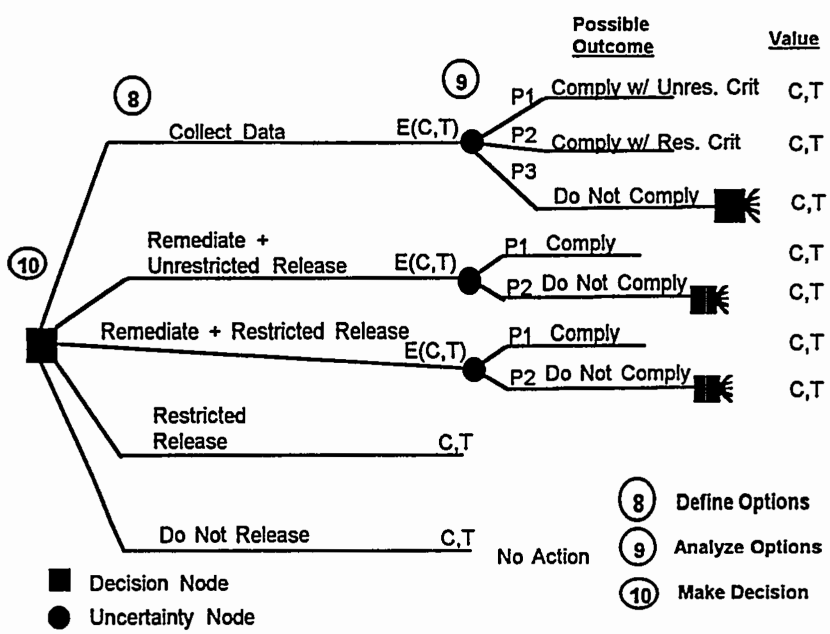


DATA WORTH / COST ANALYSIS

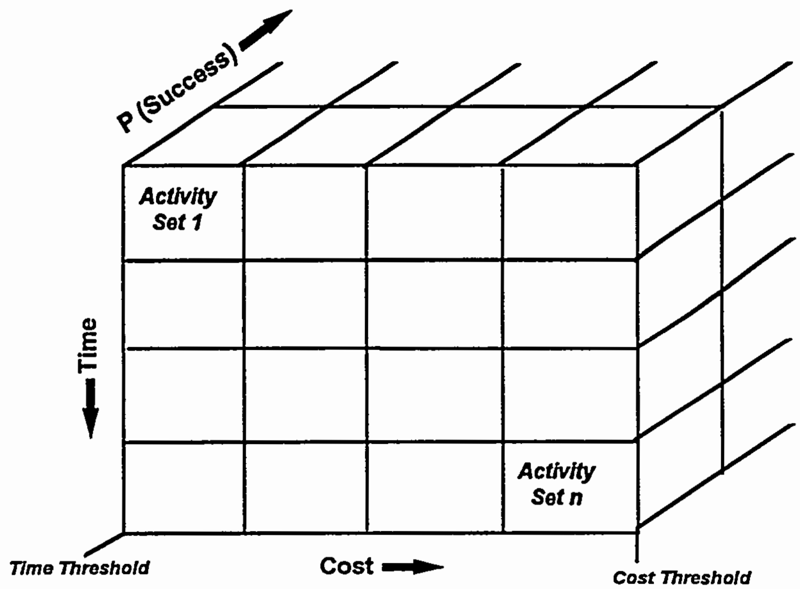
- **Various forms of decision trees and applications of multi-attribute theory have been developed and/or modified to support decision makers in making informed decisions. These approaches analyze the potential benefits of:**
  - **system design change or remedial alternative**
  - **decreasing the input parameter uncertainty through additional site characterization**
  - **the cost of additional data collection versus design changes or remediation**

  and in some cases address the uncertainty in costs of remedial alternatives

GENERIC DECISION TREE EXAMPLE



EXAMPLE DECISION OPTIONS MATRIX



Site Characterization

•Geostatistical methods developed for TRU and HLW combined with data worth analysis are used to define where to collect additional data

Monitoring

•Process models and uncertainty analysis methods developed for waste disposal and ER are used to produce multiple possible realizations of plume locations

• Cost-benefit analysis combined with optimization routines are then used to locate potential monitoring locations

SUMMARY

Over the past 20 years Sandia Labs has successfully developed an extensive capability to perform environmental risk assessment beginning with the National problems of HLW,LLW, and TRU waste disposal and extending those capabilities to the National environmental clean up programs of DOE, NRC, and EPA

Future Applications

Ken Sorenson, Manager
Environmental Risk Assessment &
Regulatory Analysis Department

SANDIA NATIONAL LABORATORIES

Risk Panel Meeting

Potential Applications in Environmental Programs

156

Paul Davis, Nuclear Energy Technology Center, 6400
Ken Sorenson, Environmental Technologies &
Applications Center, 6600
Mert Fewell, Nuclear Waste Management Programs Center, 6800

July 2, 1997
Albuquerque, New Mexico

Sandia
National
Laboratories

Potential Applications

The Environmental Programs risk assessment work addresses potential new applications in four important ways:

1. Training users of developed codes and methodologies.
2. Enhancement to existing tools.
3. Decision tool applications for large-scale programs.
4. Providing support to the regulatory process.

Sandia National Laboratories

Potential Applications

1. Training users of developed codes and methodologies.

- Implementation of any given methodology will require:
  - Training the customer to use the tool, or
  - Supporting the customer to understand the technical basis, analyses, and results, and/or
  - Supporting the regulator in interpreting results and in performing independent analyses, if necessary.

Sandia National Laboratories

Potential Applications

Example 1:

– NCART will provide site specific programmatic decision analysis support to the DOE National Spent Nuclear Fuel Program and to the individual sites. Sandia can provide specific analyses or the sites can perform their own analyses.

Potential Applications

Example 2:

– The WIPP team is supporting EPA's independent confirmatory analysis for the review of the WIPP compliance application.

Sandia National Laboratories

Potential Applications

2. Enhancement of existing tools

- Code sets and methodologies can be enhanced to reflect technical advances, regulatory changes, or customer requirements.

Potential Applications

<u>Example 1</u>:

- As desktop computer capability continues to expand, decision tool methodologies become increasingly comprehensive and user friendly. Protocol for the SEDSS framework is evolving to the point where the decision as to what specific code within the framework to use for a particular problem is transparent to the analyst.

Potential Applications

<u>Example 2</u>:

– DOE sites are beginning to address environmental risk. It will be necessary to incorporate environmental risk analysis capabilities into existing and developing risk assessment and decision-aiding tool frameworks.

Sandia National Laboratories

Potential Applications

3. Decision tool applications to large-scale programs

- For large-scale programs of national significance, existing or developing decision-aiding methodologies will need to be customized.

Sandia National Laboratories

Potential Applications

<u>Example 1</u>:

– D&D of nuclear facilities will require assessment of additional regulations, future land use issues, commingling of facilities and sites, etc. While methodologies developed for repository or nuclear power plant assessments may be applicable, they will need to be customized to address important issues specific to the application.

Potential Applications

Example 2:

– Water resource management and surety of water supply systems is an area of national and international significance that can benefit from Sandia's expertise in programmatic risk assessment and decision-aiding tools framework development. As with D&D, these tools can be customized to address issues specific to water resource management.

Sandia National Laboratories

Potential Applications

4. Provide support to the regulatory process.

- Development and application of risk assessment tools strengthen the technical justification for risk-based environmental remediation and restoration.

Potential Applications

<u>Example 1</u>:

- Sandia is providing technical support to DOE in its interactions with EPA with regard to the Hazardous Waste Identification Rule (HWIR) . Risk assessments provide technical justification to recommended regulatory changes that will substantially reduce costs without compromising public health and safety.

Potential Applications

<u>Example 2</u>:

– As both the NRC and EPA evolve to a PRA approach to compliance, Sandia's expertise and tools provide the means for credible PRA analyses. For example, the NRC and EPA share in the funding of the SEDSS development and EPA has requested Sandia support in the review of the WIPP compliance application.

Information Systems

Sharon Chapa, Manager
Decision Support Systems Software
Engineering Department

Information System Risk

Presentation to the
Risk Program Review Committee
July 2, 1997

presented by Sharon K. Chapa

Broad Definition of Information System Risk

❖anything that makes the system "misbehave"
❖failures stem from myriad causes
❖poorly characterized
❖complex internal structure
❖complex coupling to environment
❖failure space not modeled

Examples of Software Failures and Their Consequences

- a medical delivery system
- a telecommunications infrastructure
- a reactor design

Why Sandia Cares About Information System Risk

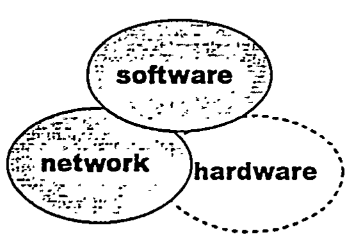
- build critical software
  - analyze weapons
  - control weapons & robots
  - 7x24 situation awareness monitoring
  - environmental decisions
- assessments for others
  - critical infrastructures
  - control systems, eg. nuclear power plants

Information System Risk Program

- no formal program across Sandia specific to information system risk
- related programs and activities
  - Strategic Surety Backbone
  - Reliability Science & Engineering Council
  - LDRD areas: Risk & Reliability, Info Systems
  - work going on within real programs
- total on the order of: $3M, 20 FTE

A View of IS Risk

- project risk - cost, schedule, performance
- technical risk - reliability, safety, security



How We Address Project Risk

- ❖project management tools
- ❖reviews
- ❖assessments
  - ➢SEI CMM
  - ➢SEI risk assessment
- ❖cost & schedule estimation tools

How We Address Technical Risk

- ❖improve best practices
  - ➢primarily driven by needs of real programs
  - ➢some research dollars
- ❖seek analytic basis to assess failures
  - ➢some research dollars

Improving Best Practices (examples)

- design
  - limit complexity
- testing
  - robotics: simulating hazardous test situations
  - 7x24 monitoring: simulating scenarios
  - WR qualification: formal planning & tracing
  - business: load & performance testing

Improving Best Practices (examples, continued)

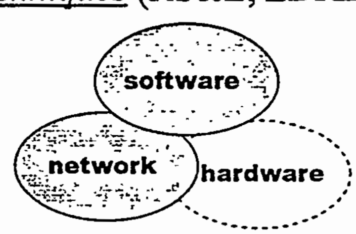
- usability
  - capturing scripts of actual usage for study
  - work processes drive design
- safety
  - weapons: safety in spite of software
  - robotics: software's role in safety
- security
  - security policies for mutual distrust

Improving Best Practices (examples, continued)

- code generation
  - using 4GLs
  - provably correct translator research
- self monitoring systems
  - 7x24: state of health expert systems
  - path expression research
  - multi-factor qualification research proposals

A View of IS Risk

- risk = undesired behavior
- project risk - cost, schedule, performance
- technical risk - reliability, safety, security
  - best practices (programs, SSB)
  - *analytic techniques* (RS&E, LDRD)



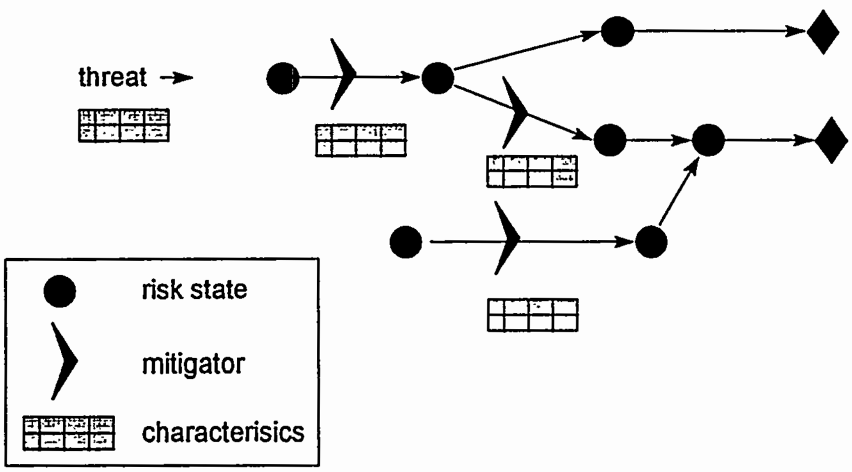
Developing Analytic Techniques

- ❖modeling failure space
  - ➢complex systems (organized complexity)
  - ➢multiple dimensions (safety, security, reliability)
  - ➢software, networks
- ❖building tools to apply new understanding
  - ➢data collection
  - ➢analysis

Reliability Science & Engineering Roadmap

Elements ↓	Reliability Engineering Tools	Scientific Understanding	New Paradigms
Reliability Modeling	Data collection tools: static & dynamic observations of the software product Analysis tools: deriving a reliability assessment from the observations	Models relating observables to reliability properties Fragility model: how reliability degrades with maintenance	Science-based measurement, analysis, prediction of software reliability Monitoring observables; ongoing assessment of fragility & degradation
Lifecycle	Simulations, "executable" specs CASE tools & process data collection tools Compensating for low quality parts of process	Understand coupling between processes & reliability properties of the software product	Design for maintainability Assess impacts prior to changes Upgrading in-place
Quali-fication	Multi-factor reliability measurement Operational surveillance of fragility	Couple (product measurables + test + simulation + process) to a reliability rating	Explicitly satisfying surety, quality, reliability requirements Deliver a reliability rating with the software product

LDRD #1
Surety Analysis Graph

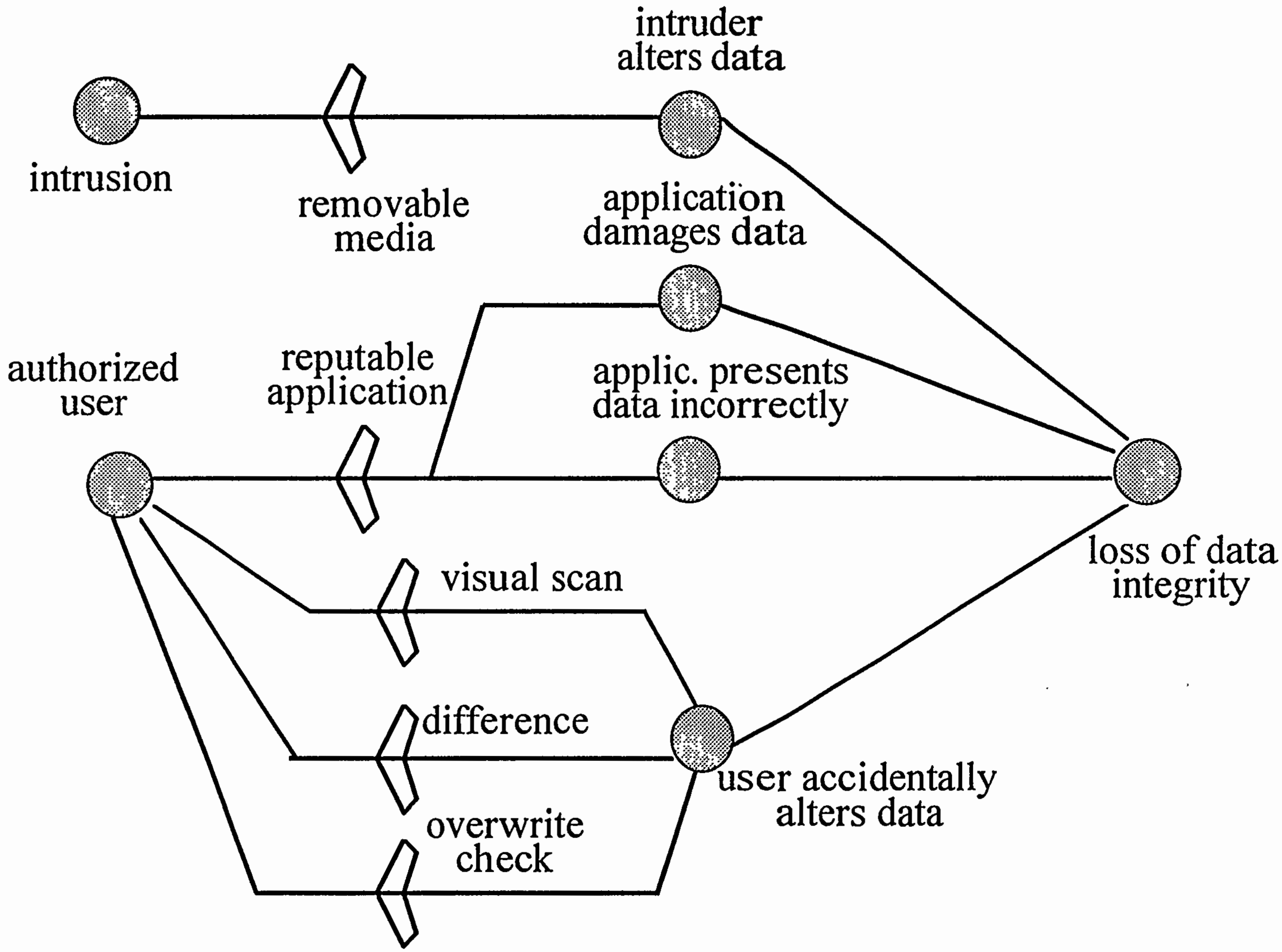


LDRD #1

Consequences

	Information	Processes/ Transactions	System Composition	System State Changes	Interfaces
Access Control		• authentication failure • spoof			
Integrity	• intruder alters • user alters • bad application				
Utility				• shutdown-startup not synchronized	
Availability			• single p.o.f. • unreliable network		
Safety					• harmful output • operator error • out of toleranc

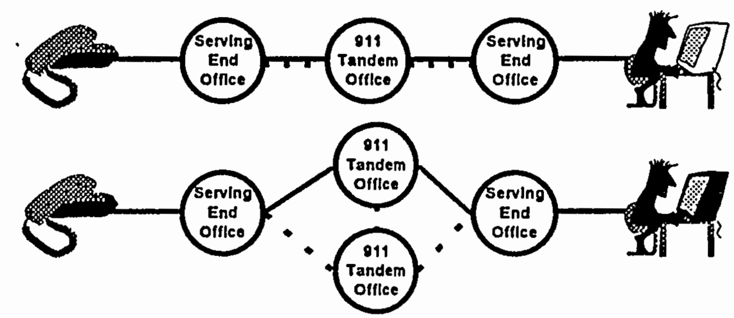
LDRD #1



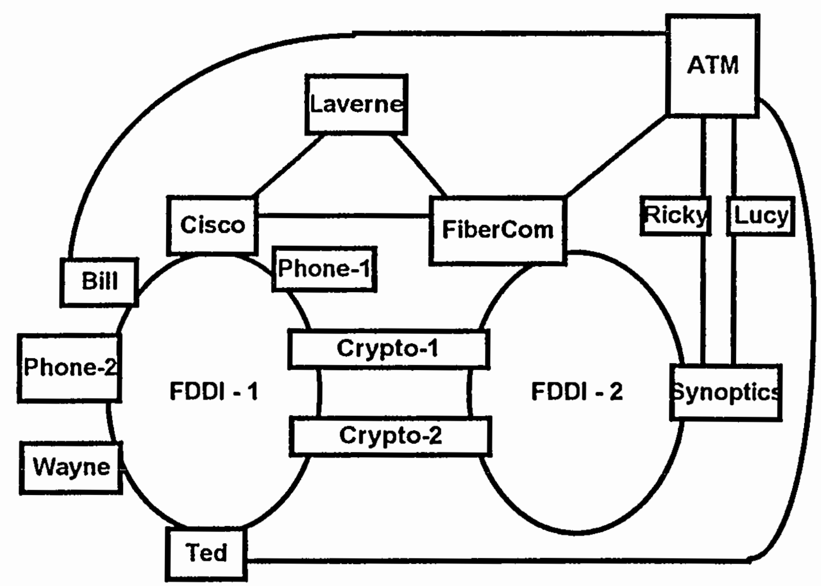
intruder alters data
intrusion
removable media
application damages data
authorized user
reputable application
applic. presents data incorrectly
loss of data integrity
visual scan
difference
user accidentally alters data
overwrite check

LDRD #2
Communications Network Reliability

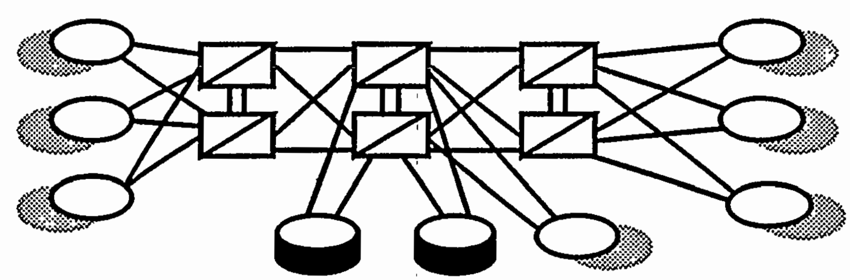
Example 911 Service Architectures



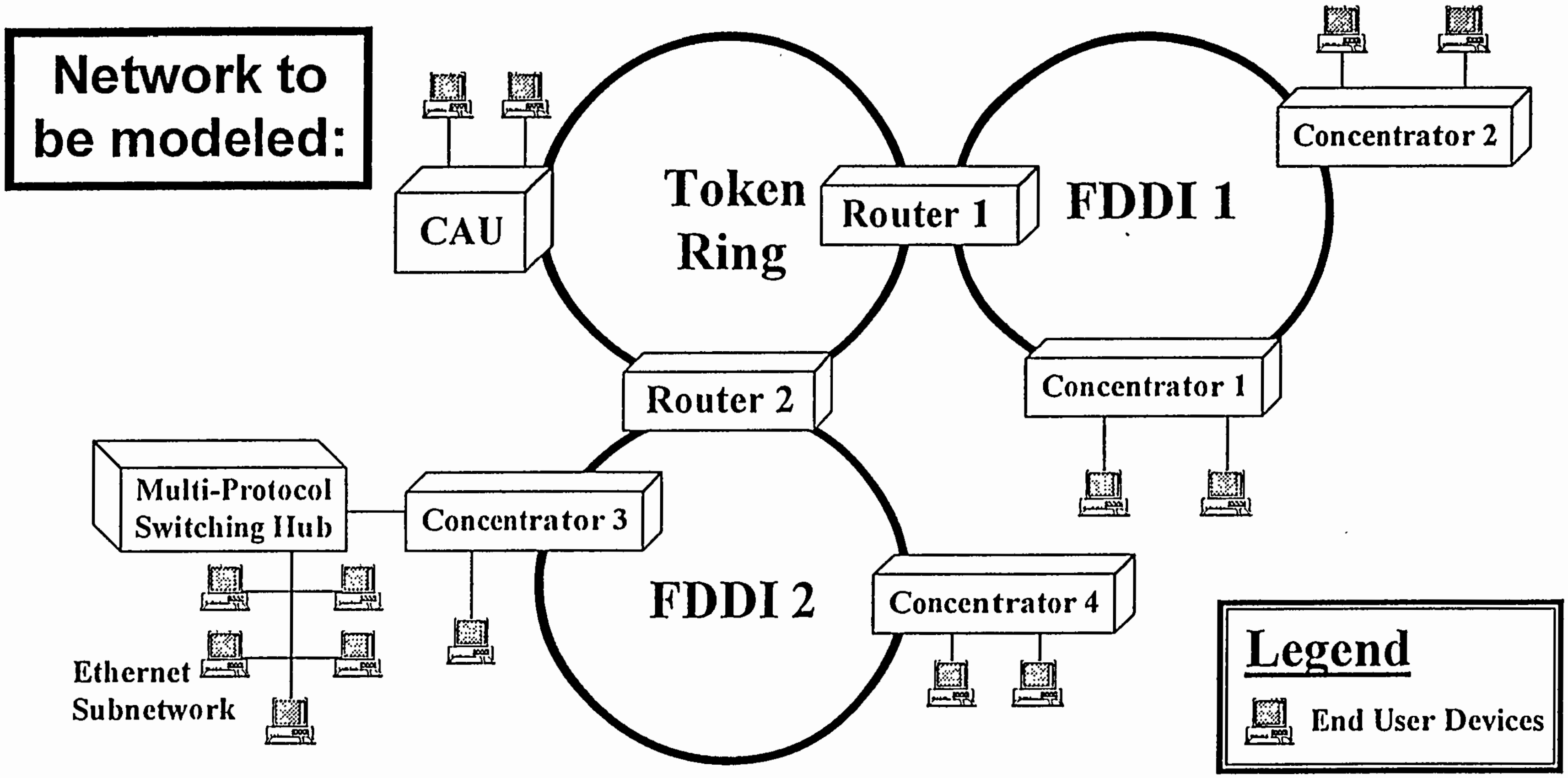
Example Data Network Architecture



Example Telephone Signaling Network Architecture

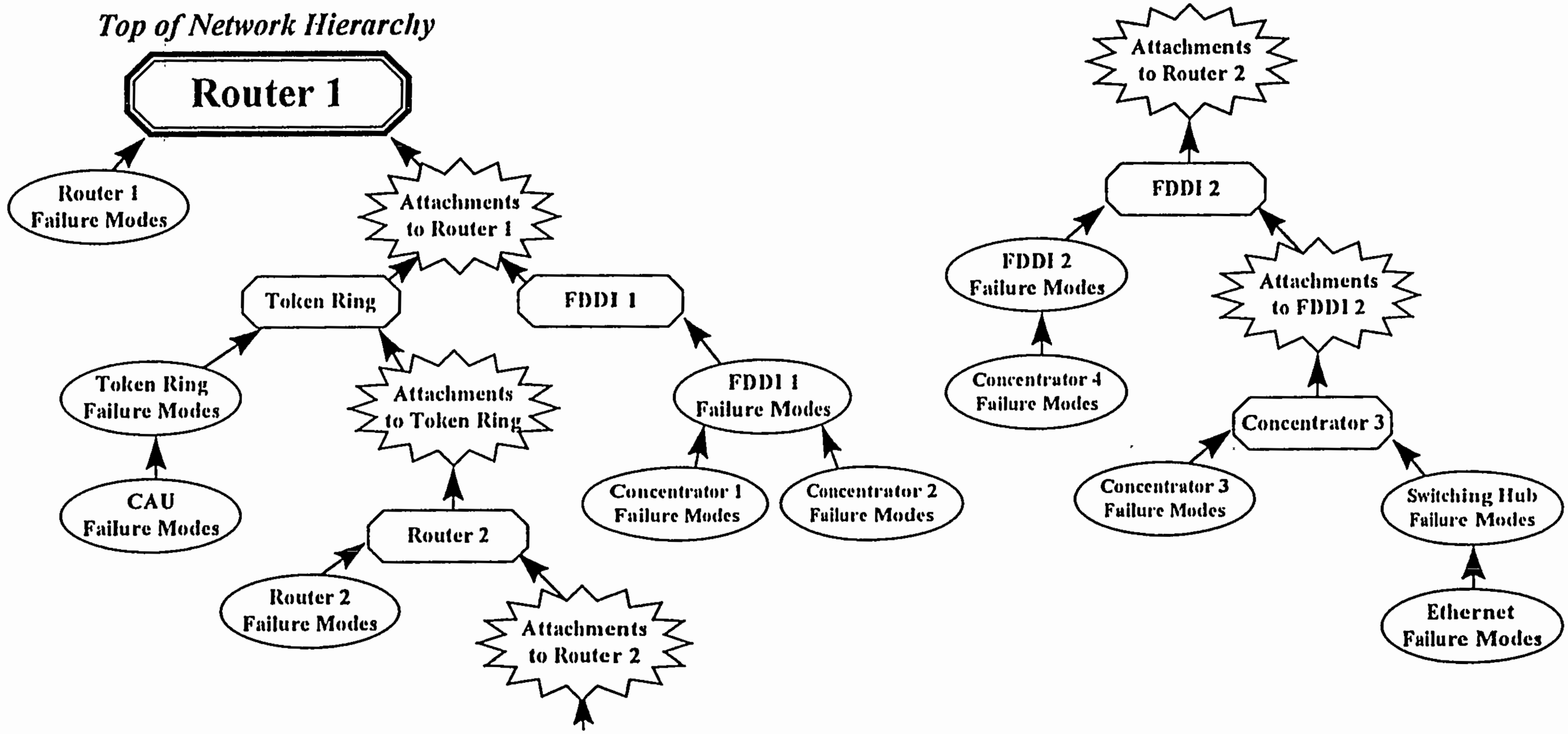


LDRD #2


Network to be modeled:
CAU
Token Ring
Router 1
FDDI 1
Concentrator 2
Concentrator 1
Router 2
Multi-Protocol Switching Hub
Concentrator 3
FDDI 2
Concentrator 4
Ethernet Subnetwork
Legend
End User Devices

LDRD #2

How fault tree modules can be assembled in the "Plug-and-Play" method.



LDRD #2

- Risk-based network analysis techniques have been developed for hierarchical and non-hierarchical networks.
  - *<u>Hierarchical</u>*: "Plug-and-Play" Fault Tree Analysis Method
  - *<u>Non-Hierarchical</u>*: Efficient Network Search Algorithm enables the use of cut sets rather than path sets
  - These methods can be "married" for hybrid networks
- Models can be extended to model network services and classes of network traffic

Summary
Information System Risk

- We address project risks and technical risks.
- We continually improve our best practices.
- We seek a better analytic basis, but face challenges in the modeling of software and network failure spaces.

Some Future Research Directions

Greg Wyss
Risk Assessment & Systems Modeling
Department

Committee to Evaluate Sandia's Risk Expertise
July 1-2, 1997

Looking Forward:
A Sampling of Methodological Research Programs at Sandia

Gregory D. Wyss, Ph.D.
Risk Assessment and Systems Modeling Department 6412
Sandia National Laboratories
Albuquerque, NM 87185-0747

(505) 844-5893 gdwyss@sandia.gov

Sandia National Laboratories

97-11-1

Outline

Looking Forward: A Sampling of Methodological Research Programs at Sandia

- Computational
  - High-Performance Computing for Uncertainty Analysis
- Methodological
  - Effects of Aging on Reliability
  - Risk-Based Network Vulnerability Analysis
  - Fuzzy and Hybrid Number Algebra for Risk Assessment
  - Object-Oriented Risk and Reliability Assessment
- Summary

Sandia National Laboratories

97-11-2

Laboratory-Directed R&D

Sandia has a significant internally-funded R&D program to push the state-of-the-art.

- All aspects of risk and reliability analysis
  - Innovative technical methods
  - Defining failure modes
  - Understanding aging effects
  - Designing for reliability
  - Critical National Infrastructures Risk and Reliability
- Funds awarded by competition
  - Projects can last from 1 to 3 years
  - $1.3M in FY-97; 2.7M in FY-98 (incl. multi-year $)

Sandia National Laboratories

97-11-3

Laboratory-Directed R&D (cont.)

Projects funded in FY-97 include:

- Reliability Degradation Due to Stockpile Aging
- Integrated Approach to Develop Micro-Electrical-Mechanical System (MEMS)
- Precursors to Failure of Oxides and Metal Lines in CMOS Technology
- An Extensible Object-Oriented Framework for Risk & Reliability Analysis
- Risk-Based Characterization of Network Vulnerability
- Enhancing Risk Analysis Using New Mathematical Structures

Sandia National Laboratories

97-11-4

LDRD is Multi-Disciplinary

The LDRD program selection criteria encourage inter-disciplinary cooperation.

- Teams are sought from across organizational and technological boundaries
- Technologies and results should be useful to multiple applications and customers

Objective: Bring together diverse methods to solve challenging problems in the forefront of science and technology.

Sandia National Laboratories

97-11-5

Uncertainty Quantification

The Problem:

- Properly accounting for uncertainties in risk and reliability assessments is extremely computer-intensive.
  - Can require thousands or millions of evaluations of individual probabilistic or deterministic models.
- Situation is complicated by the "state explosion" that occurs in many models, *e.g.*,
  - End states in event tree models
  - Weather trials in consequence assessments

Sandia National Laboratories

97-11-6

Uncertainty Quantification (cont.)

Technologies and Benefits

- Advances in desktop computing enable many uncertainty studies that were not previously possible.
  - More detailed computations using existing methods
- High performance computing enables cutting edge research in this area.
  - Parallelization of assessment software
  - Teraflop computing increases throughput -- makes it possible to consider methods that would have previously been intractable

Sandia National Laboratories

97-11-7

Effects of Aging

The Problem:

- Anticipating potential stockpile aging problems has traditionally been based on testing and deterministic engineering analyses.

Project Objectives:

- Identify and prioritize potential aging issues using reliability analysis techniques.
- Help engineers understand impacts of new materials, components, etc., on system reliability *given limited testing.*

Sandia National Laboratories

97-11-8

Effects of Aging (cont.)

Technologies and Benefits

- Uncertainty engines
  - LHS & Adaptive importance sampling
  - First order / second order / likelihood reliability methods
  - Genetic algorithms & neural networks
- Wraps around existing design & analysis tools
  - Stress voiding and electromigration in IC's
  - Thermo-mechanical fatigue of solder joints
- Effectively uses data from a variety of sources
  - Flight tests; storage inspections; expert judgment

Network Vulnerability Analysis

The Problem: Apply risk assessment techniques to network security analysis.

- Many individual component vulnerabilities are known, but their security implications, *when taken together*, are unknown.

Project Objective: Develop a methodology that enables an inexperienced analyst to:

- Identify how an adversary might exploit known weaknesses to gain access to a system, and
- Determine what undesirable activities they could perform after gaining access.

Network Vulnerability Analysis (cont.)

Technologies and Benefits

- Directed graph model based on network topology and generic known vulnerabilities
  - Collected from CERT, etc.
  - Varies by type of machine, level of access, etc.
- Solution algorithms seeks to find the highest probability or lowest "cost" attack path
  - Shortest path algorithms
  - Simulation (represent the real behavior of attacker, attacker learning, and dynamics of attacks)
  - Selective pruning of exhaustive paths to determine importance of particular vulnerabilities

Sandia National Laboratories

97-11-11

Enhanced Mathematics for PRA

__The Problem:__ It is suspected that traditional probabilistic uncertainty assessment methods may overstate our confidence in the limit of very sparse data.

- Central Limit Theorem causes the results to tend toward a central value – probabilistically correct, *but*,
- Is "uncertain data" (in the limit of extremely sparse data) *really* probabilistic? Or might it be more accurately represented by fuzzy and/or possibilistic algebra?
- And, how do we combine data that is *known* to be probabilistic with data that might be fuzzy or possibilistic?

__Project Objective:__ Develop the mathematics to address these issues and appropriate software to implement it.

Sandia National Laboratories

97-11-12

Enhanced Mathematics for PRA (cont.)

Technologies and Benefits

- Research into the nature of mathematical models for uncertainty analyses.
- *Example:* Quantification of risk assessment results using hybrid numbers.
  - Similar to complex numbers, except that each value is composed of fuzzy, possibilistic and probabilistic parts
  - Incorporates a "degree of belief" to establish a relative weighting of the fuzzy and probabilistic parts.
- Software is being developed to enable hybrid quantification of cut sets.

Sandia National Laboratories

97-11-13

Object-Oriented Risk Assessment

The Problem: Risk analysis is very labor-intensive.

- Requires a specialist with a breadth and depth of expertise that is rarely embodied in a single individual
- Teaming between risk and system personnel is difficult -- no common tool set or knowledge base.

Project Objectives: Deliver a tool set that:

- Enables rapid creation of risk models by casual analysts,
- Helps the analyst manage the large volume of information that supports these models, and
- Facilitates teaming between risk analysts and engineers [illegible] across the laboratory.

Sandia National Laboratories

97-11-14

Object-Oriented Risk Assessment (cont.)

Technologies and Benefits

- Object-oriented analysis methods from computer science
  - Objects encapsulate domain and risk knowledge to represent a real-world entity (e.g., a computer)
  - Objects operate as "black boxes" -- communicate with each other through standardized interfaces
- Traditional risk assessment methods
  - Risk sub-models built into objects
  - Deterministic and probabilistic risks considered
  - Both inductive and deductive risk models supported

Sandia National Laboratories

97-11-15

Summary

Sandia is developing new risk assessment methods for widely varying applications.

- Research encompasses many areas of important to risk and reliability
  - Analysis methods
  - Effects of Aging
  - Defining failure modes
  - Design for Reliability
- Research teams cross traditional disciplinary boundaries to find novel solutions.
- Internal research funds are targeted to problems of national significance with target customers.

Sandia National Laboratories

97-11-15

POSTER PRESENTATATIONS

WinR^{TM}
(Reliability Analysis Software)

WinR™ Training Course

Sandia offers a 3-4 day training course on reliability analysis using WinR™.

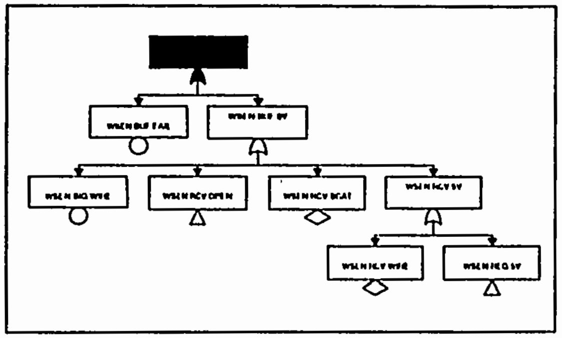
Course topics include:

- Fault tree development
- Root cause analysis
- Repairable systems analysis
- Nonrepairable systems analysis
- Reliability allocation
- Reliability optimization
- Maintenance cost analysis
- Field failure data analysis
- Sensitivity and uncertainty analysis

Course participants use WinR™ to gain practical, hands-on experience in real-world applications. There are also a variety of class exercises designed to reinforce the material being presented. Students leave with a comprehensive set of course materials and a copy of the WinR™ software.

The first offerings of the WinR™ training course will begin in the fourth quarter of 1996. Courses will be taught at Sandia and can also be given at your facility.

Center for System Reliability



For more information contact:

Dr. James E. Campbell
Systems Reliability Department
Sandia National Laboratories
P.O. Box 5800, MS 0746
Albuquerque, NM 87185-0746
(505) 844-5644 / fax: (505) 844-3321
email: jecampb@sandia.gov

or

Dr. Laura Painton
Systems Reliability Department
Sandia National Laboratories
P.O. Box 5800, MS 0746
Albuquerque, NM 87185-0746
(505) 844-8093 / fax: (505) 844-3321
email: lapaint@sandia.gov

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94A:85000

LOCKHEED MARTIN

SAND No. 97-1306

Center for System Reliability

Introduces

WinR™

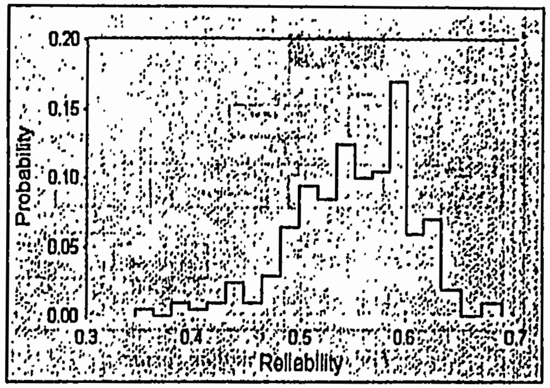
Reliability Analysis Software for Windows

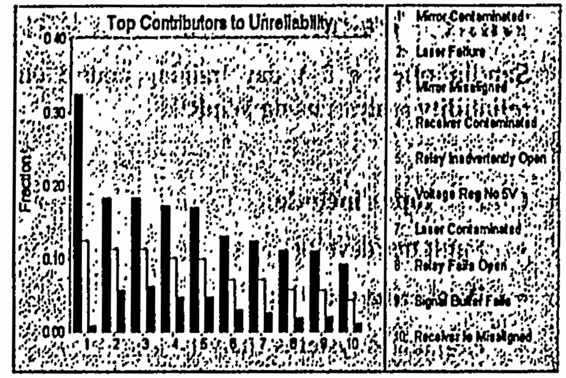
Sandia National Laboratories

"...exceptional service in the national interest."

Overview

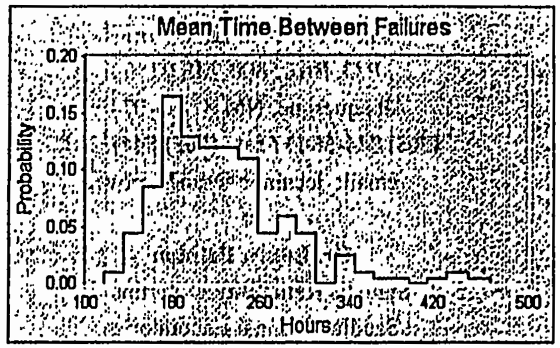
WinR™ is a PC-based reliability modeling software system typically used as a design-for-reliability tool. The software is unique in its ability to analyze uncertainty and unit-to-unit variability. This analysis capability is supported by fully integrated systems for data management and for graphics results presentation.





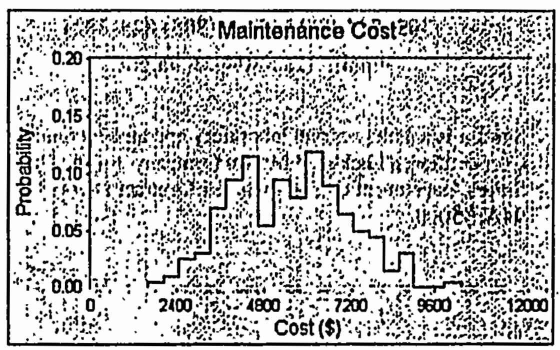
Typical analyses performed with WinR™ include:

- Optimal reliability allocation
- Fault tree and root-cause analysis
- Reliability optimization
- Field failure data analysis
- Trade-off and cost-benefit studies
- Maintenance cost analysis
- Cost minimization
- Spares optimization



The following figure shows results from a WinR™ reliability optimization study. The baseline column shows the MTBF, availability and maintenance cost for a machine prior to any reliability upgrades. The last column shows the estimated performance if all potential improvements were made to the machine. The middle column shows results when WinR™ was used to select the best combination of improvements.

The next three figures show typical outputs of reliability, MTBF, and cost. Notice the variability shown in these results. The fourth figure shows the top contributors to unreliability. Such sensitivity results are available for all WinR™ outputs.



	Baseline	Optimal	All Improvements
MTBF	72 hours	146 hours	154 hours
Maintenance Cost	$115,600	$44,000	$42,700
Availability	0.78	0.904	0.907
Improvement Cost	$0	$21,850	$86,350

National Machine Tool Partnership
and

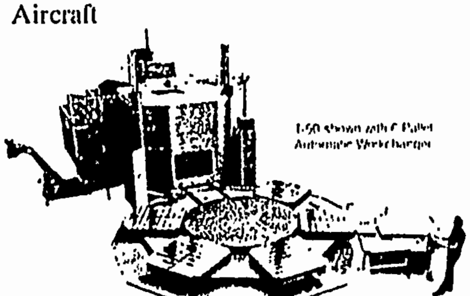
CST *Center for System Reliability*

can assist your organization with:

- System reliability analyses
- Optimal maintenance and spares strategies
- Predictive maintenance
- Design trade-off and cost-benefit analyses

We have extensive experience working with industry!

- Semiconductor
- Machine tool
- Automotive
- Medical
- Textile
- Aircraft



Horizontal CNC Machining Center

Call to see how we can help you maximize your equipment availability and minimize maintenance costs!

For more information contact:

Robert M. Cranwell, manager
Systems Reliability Dept.
Sandia National Laboratories
P.O. Box 5800, MS 0746
Albuquerque, NM 87185-0746

(505) 844-8368/fax: (505) 844-3321
email: rmcranw@sandia.gov

or

Donald L. Plymale
Product Realization Integration Dept.
Sandia National Laboratories
P.O. Box 5800, MS 0961
Albuquerque, NM 87185-0961

(505)845-9203/fax: (505)844-5589
email: dlplyma@sandia.gov

Sandia National Laboratories

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

LOCKHEED MARTIN

Sand No. 97-1308

National Machine Tool Partnership
and

CST *Center for System Reliability*

Introduce the

WinR-PdM™ Predictive Maintenance System

A systems approach to improving availability and reducing costs

Sandia National Laboratories

WinR-PdM™

A New Concept for Predictive Maintenance!

Sandia National Laboratories has recently coupled its reliability modeling and prediction capabilities with its sensor technology to develop the *WinR-PdM™* predictive maintenance system.

Tired of interpreting sensor data and trend functions?

WinR-PdM™ eliminates much of the guess-work that is typically encountered in processing and interpreting trend functions and sensor data.

Key features of WinR-PdM™ include:

- ***Ease of data interpretation*** - Data are presented in terms of easily interpreted probability of failure curves, Pareto charts, dials and gauges.
- ***Utilization of all data*** - Historical failure data are combined with real-time sensor data to provide an accurate up-to-date status of the system.
- ***Early detection*** - Reliability models of the system are utilized to estimate probability of failure in advance of an actual failure

User Friendly, Fully Integrated Windows Environment System!

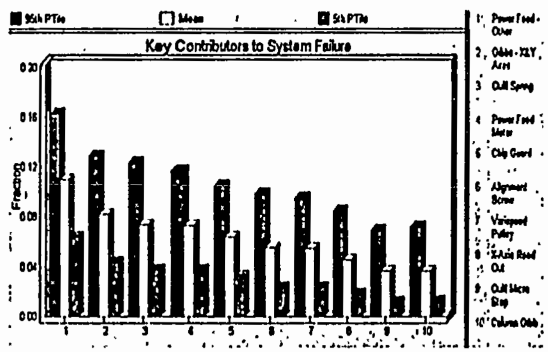
WinR-PdM™ is an integrated system coupling sensor data with the unique *WinR™* software developed at Sandia National Laboratories.

WinR™ is a PC-based, Windows environment software package with capabilities in:

- Reliability Modeling & Prediction
- Optimization Analyses
- Maintenance & Spares Analyses
- Trade-Off & Cost-Benefit Analyses
- Sensitivity & Uncertainty Analyses

Easily identifiable failure modes!

Through its ***reliability modeling and sensitivity analysis capabilities, WinR™*** can be used to identify key contributors to system failure.

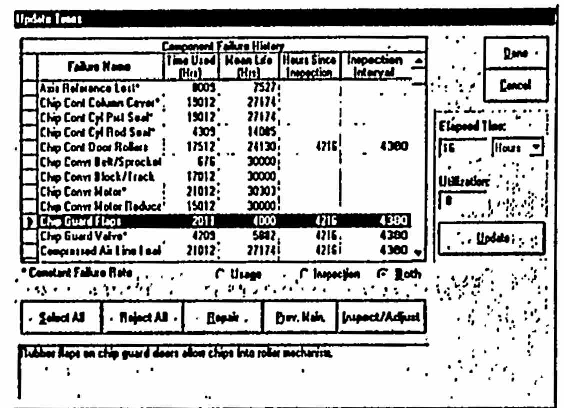


Key Contributors to System Failure

Understanding root causes of failures allows the selection of appropriate sensors for monitoring relevant system components.

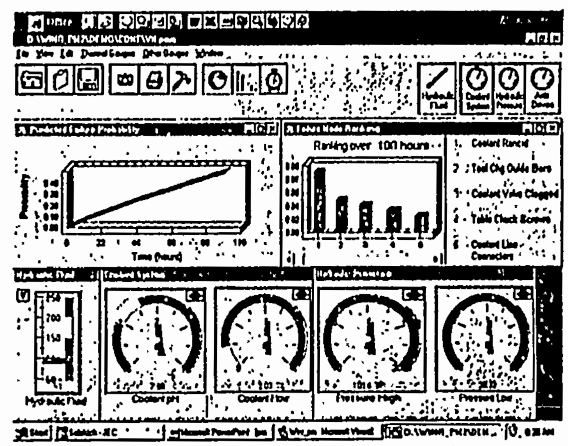
Easily Interpreted System Status!

Real-time sensor data is combined with historical failure data in *WinR™* to continually update the system status.



Current System Component Status

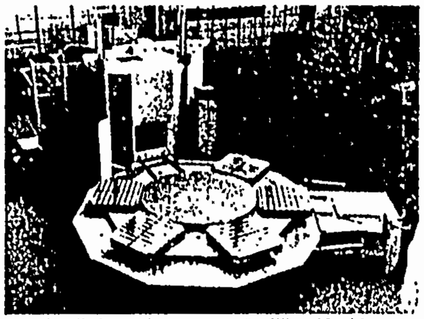
WinR™ ***reliability models*** are used to estimate the probability of system failure over time and provide a ranking of the most probable failure modes.



System Failure Probability & Key Contributors

Predictive Maintenance

CST has recently coupled its reliability modeling and prediction capabilities with sensor technologies from within Sandia National Laboratories as part of a pilot predictive maintenance project with a major U.S. aircraft company. This has led to the start of an advanced pilot effort on a machine tool within Sandia.

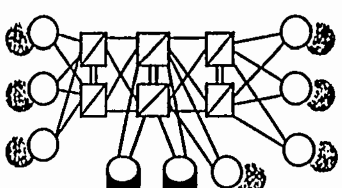


Predictive Maintenance of Milling Machine

Communications Network Reliability

CST has developed new reliability modeling methods that can be applied during both network design and operations phases to:

- Provide reliable network design
- Prioritize network monitoring & maintenance
- Optimize network improvements



Simplified Telephone Common-Channel Signaling Network

For more information contact:

Robert M. Cranwell, manager
Systems Reliability Department
Sandia National Laboratories
P.O. Box 5800, MS 0746
Albuquerque, NM 87175-0746

(505) 844-8368 fax: (505) 844-3321
email: rmcranw@sandia.gov

CST *Center for System Reliability*

Sandia National Laboratories

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

LOCKHEED MARTIN

Sand No. 97-1307

Center for System Reliability

Sandia National Laboratories

CST Center for System Reliability

Established to Meet the Needs of a
Changing Reliability Focus!

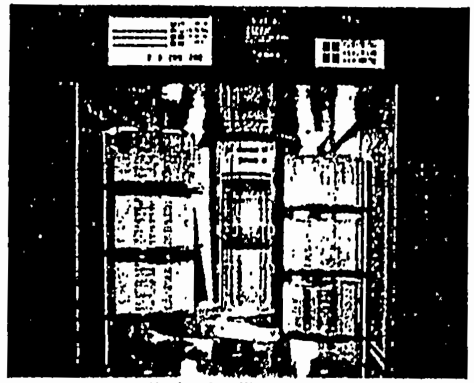
Field reliability data on complex systems indicate that the primary causes of failure ***are not components!*** Data indicate that part failures account for only about 15% of system failures; 85% are due to ***system-level*** problems associated with design and manufacturing.

Sandia National Laboratories has established a ***Center for System Reliability*** (CST) that can provide support in:

- Reliability modeling and prediction
- Sensitivity and uncertainty analyses
- Optimization analyses
- Predictive maintenance
- Communications network reliability
- Education & training.

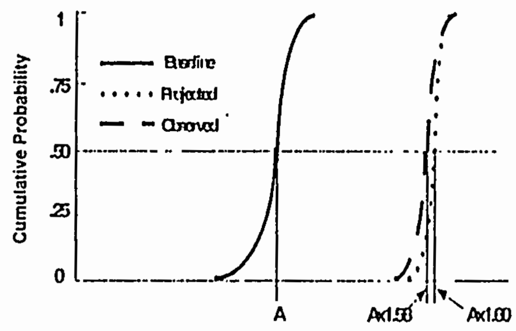
Reliability Modeling & Prediction

CST has developed the ***WinR***^{TM} PC-based, windows environment, reliability analysis software package. ***WinR***^{TM} is used in modeling and analyzing a product throughout its life cycle. It has been used to model complex semiconductor manufacturing equipment such as the pictured wafer handling system.



Wafer Handling System

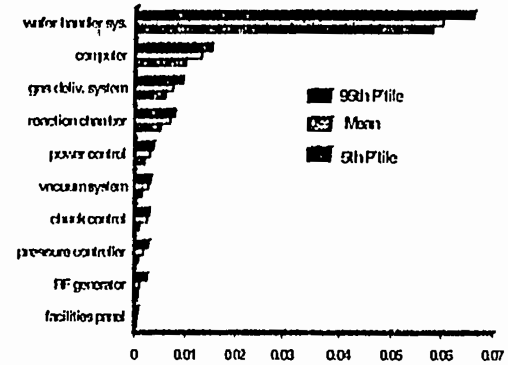
WinR^{TM} is especially powerful when used as a "design-for-reliability" tool to evaluate the reliability of a product early in design.



Observed vs Predicted Reliability of New Equipment Design

Sensitivity & Uncertainty Analyses

CST has extensive capabilities for analyzing the effects of parameter uncertainty and unit-to-unit variability. Sensitivity analyses can be performed to identify top contributors to system failure, unavailability, down time, costs, and uncertainty.

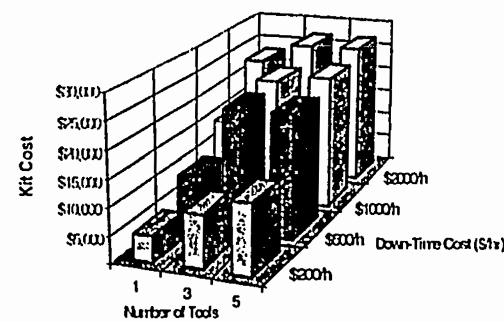


Key Contributors to System Failure for Semiconductor Manufacturing Equipment

Optimization Analyses

CST also has capabilities for performing *combinatorial optimization analyses.* This feature is being used in studies on:

- Design tradeoffs
- Equipment upgrades
- Reliability allocation
- Spares inventory



Cost of Optimized Spares Kit

Reactor Risk Assessment at Sandia

Reactor Risk Assessment

at

Sandia National Laboratories

Poster Session

for

Committee to Evaluate Sandia's Risk Expertise

July 1, 1997

Donnie W. Whitehead

Phone No. (505)-844-2632

email: dwwhite@sandia.gov

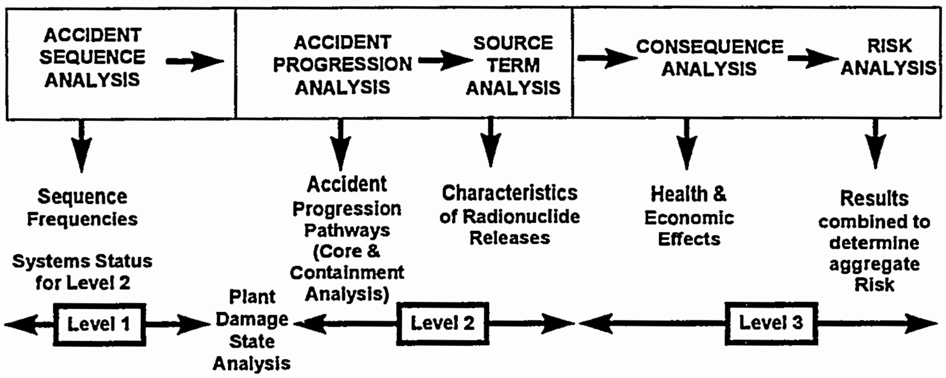
Reactor Risk Assessment at Sandia National Laboratories

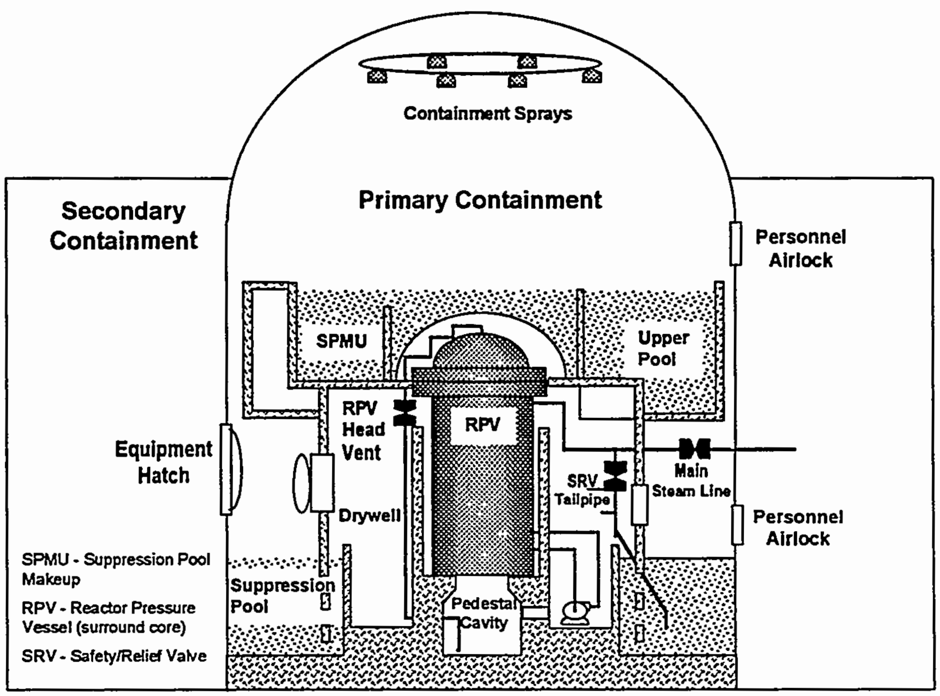
The probabilistic risk assessment (PRA) process can be applied to complex structures. Examples include:

- Nuclear power plants
- Weapons
- Chemical processing plants
- Infrastructures
  - Telecommunication
  - Transportation
- Aircraft

Sandia is expanding the use of PRA. As an example, consider nuclear power plants.

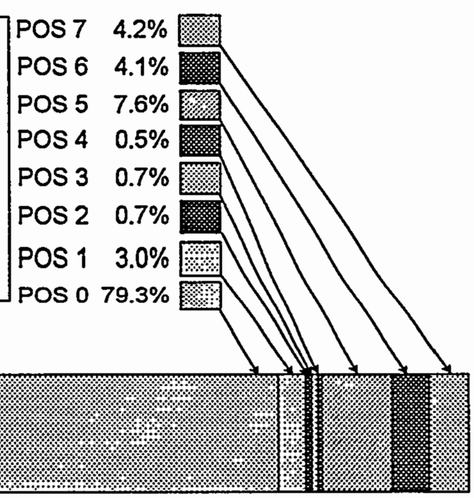
PRA Process for Nuclear Power Plants





Traditionally, nuclear power plant PRAs have focused on full-power operations. However, other operational states exist.

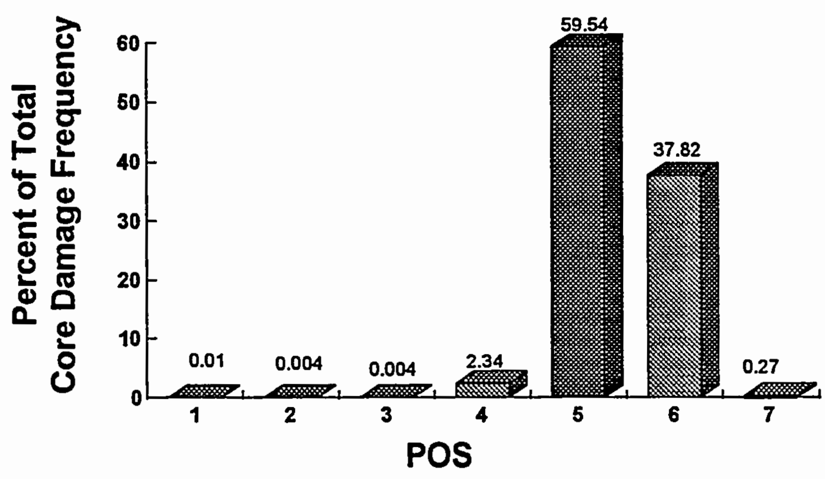
Fraction of Time Spent in Each Plant Operational State (POS)



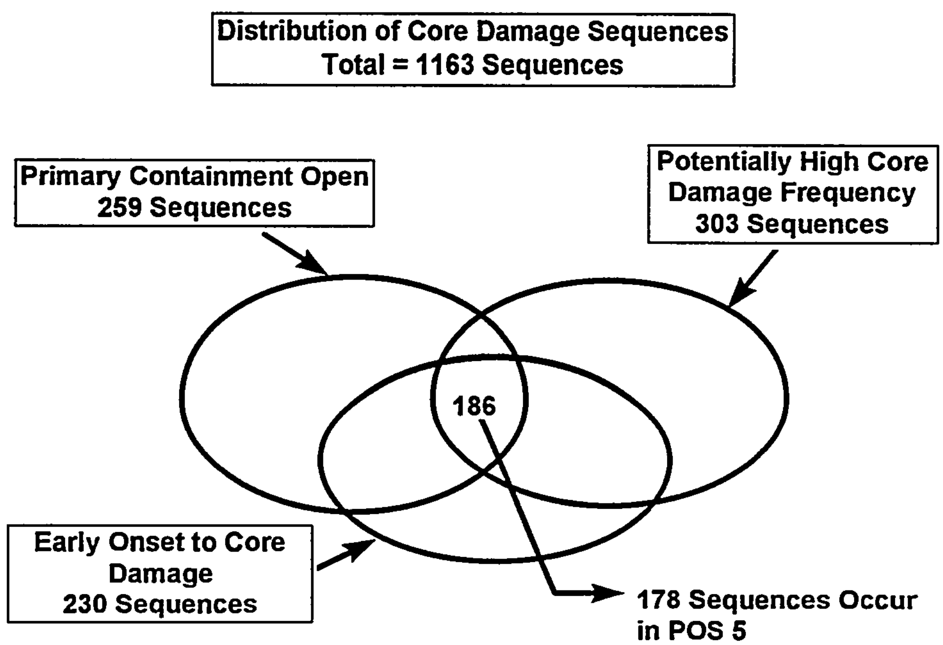
POS 0: Power
POS 1: Startup
POSs 2 - 4: Hot Shutdown
(Three POSs defined by pressure and temperature differences.)
POS 5: Cold Shutdown
POSs 6 & 7: Refueling
(Two POSs with different water levels.)

Screening analyses indicated that two POSs--POS 5 and POS 6--are the largest contributors to total core damage frequency (CDF).

Importance of Plant Operational States

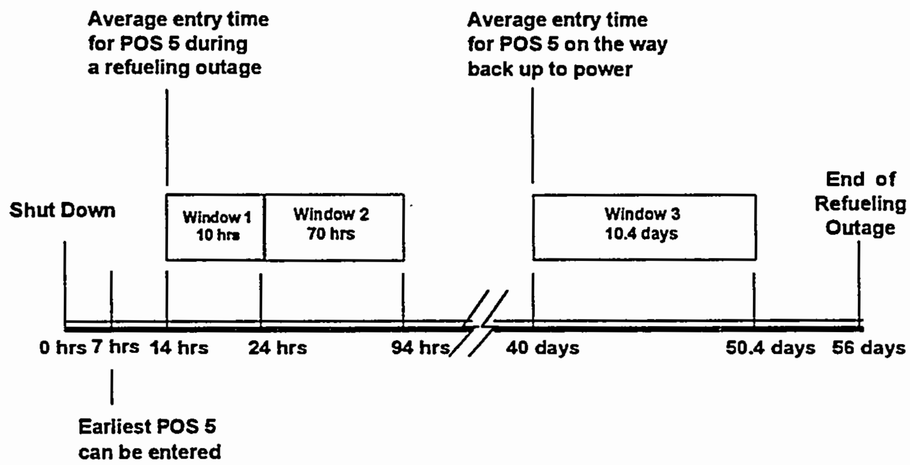


Considering factors important to both core damage frequency and risk, POS 5 was selected for detailed analysis.

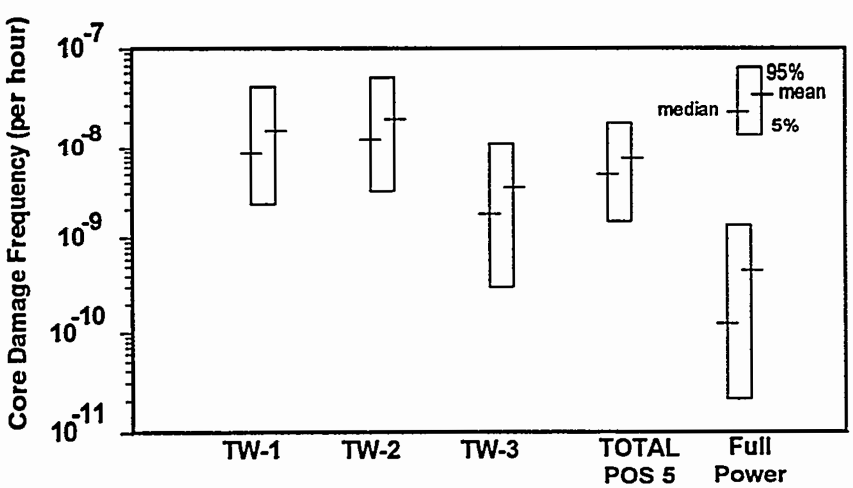


To account for thermal-hydraulic and radionuclide differences, POS 5 was divided into three time windows.

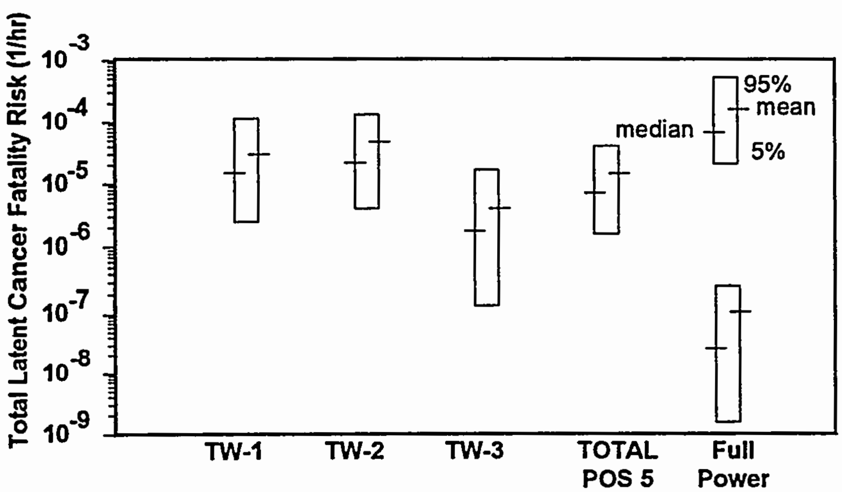
POS 5 TIME LINE



Results indicate that on a per hour basis, POS 5 has the potential to be at least as great a contributor to core damage and risk as full-power.

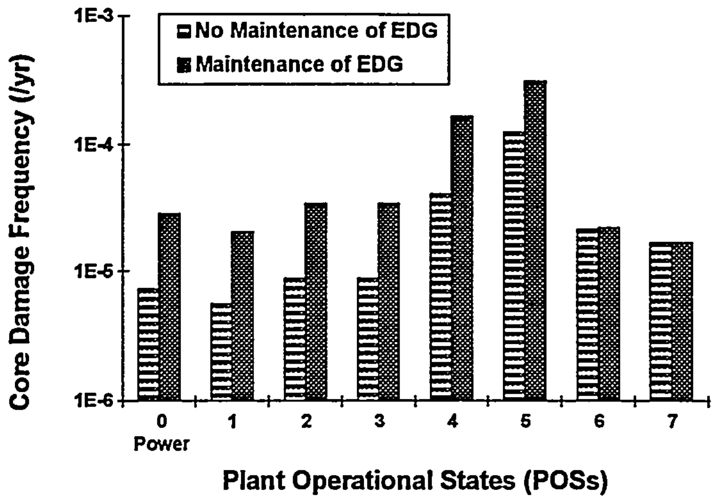


TW - Time Window



TW - Time Window

Using models for all plant operational states, risk-informed decisions can be made on when to perform maintenance or test activities. For example, in POSs 6 and 7 the CDF associated with maintenance on an emergency diesel generator (EDG) is similar to the CDF for no maintenance.



EDG - Emergency Diesel Generator

Risk and Reliability Assessment for Telecommunications Networks

Probabilistic Safety Assessment '96
Park City, Utah September 29-October 3, 1996

RISK AND RELIABILITY ASSESSMENT FOR TELECOMMUNICATIONS NETWORKS

Presented by: Gregory D. Wyss, Ph.D.

Authors

G.D. Wyss & H.K. Schriner, Risk Assessment & Systems Modeling Dept.

T.R. Gaylor, Data Transport & Network Design Dept.

Sandia National Laboratories
Albuquerque, NM 87185-0747

☎ (505) 844-5893 gdwyss@sandia.gov

Sandia National Laboratories

96-13-1

Outline

Risk and Reliability Assessment for Telecommunications Network

- Introduction
- Network Cut Sets: Modeling Connectivity
  - Models of Hierarchical Networks: Fault Tree Analysis
  - Models of Non-Hierarchical Networks: Directed Search
- Modeling User Perceptions of Network Performance
- Summary

Sandia National Laboratories

96-13-2

Introduction

It is possible to have a network system with zero risk ... but it's not very useful ...

Sandia National Laboratories

96-13-3

Surety is a Balancing Act

"Surety" balances access control, integrity, safety, functionality and reliability.

Assure Against Unauthorized Use — **of** — **Assure Safe & Authorized Use**

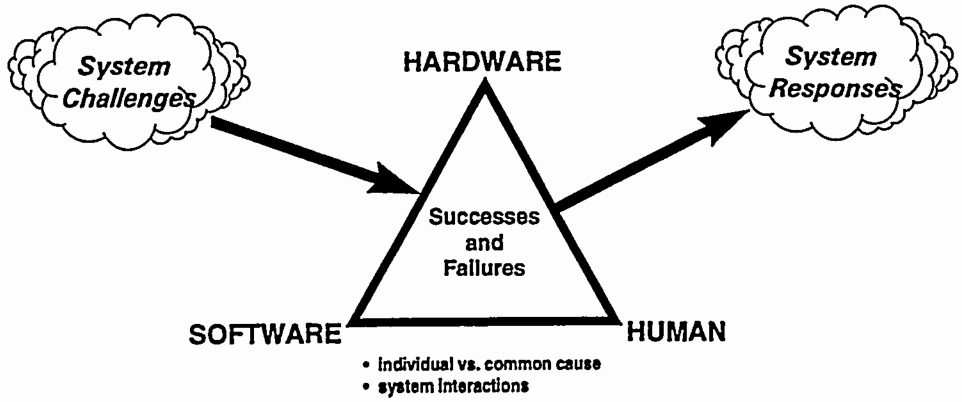
Information and Systems

Sandia National Laboratories

96-13-4

Sources of Risk for Complex Interconnected Systems

Risk assessment considers the ***combined*** response of hardware, software, and humans to potential system challenges.



Sandia National Laboratories

96-13-5

Generalized Network Analysis Methods

Sandia has invested internal R&D funds to develop network surety analysis methods.

- **Quickly found that fault trees work well for hierarchical networks but fail for non-hierarchical** *(to be discussed later)*
- **Objectives:**
  - **develop and validate a *quantitative* risk and reliability analysis method for data networks**
  - **make fault tree modeling of hierarchical networks faster and less labor intensive**
  - **make fault tree modeling accessible to persons who are network experts but not risk analysis experts**
  - **model network connectivity as well as network performance aspects (network services, classes of traffic, etc.)**

Sandia National Laboratories

96-13-6

Hierarchical Networks

Fault tree analysis (FTA) often works well for modeling hierarchical networks.

- A network is hierarchical if the address space or the network architecture enforce a hierarchy.
  - Many current-generation networks behave hierarchically.
  - Typically only a few paths from one node to another.
- Fault tree modeling is straightforward
  - Top node in the hierarchy is the top event in the fault tree
  - Global connectivity is modeled by expanding the fault tree towards the end user nodes
  - Fault trees can be extended to model particular failure modes within individual nodes and links

Sandia National Laboratories

96-13-7

"Plug-and-Play" Fault Tree Strategy

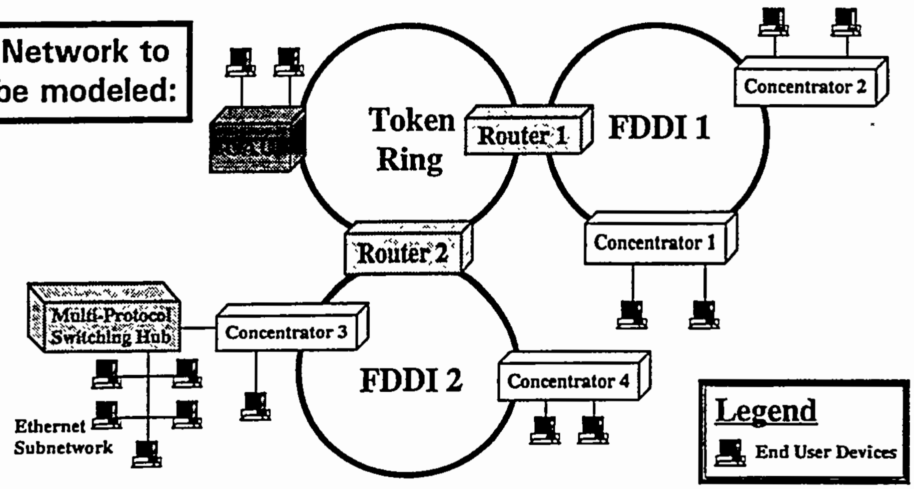
- Build fault tree "modules" for each class of network and type of network entity *(topology, node, link, element, etc.)*
  - Module models the basic failure modes for that entity
  - Module contains "plugs" to which additional fault tree modules can be "attached" to expand the fault tree model
    - → support services (power, HVAC, maintenance, etc.)
    - → other network entities to which this one is attached
- "Plug" the modules together following simple rules to obtain a fault tree for the entire network
  - Start at the top of the hierarchy, and assume network failure if any node cannot talk to the top of the hierarchy
  - Follow the network diagram until all entities included in FT
  - Trim off any "plugs" that don't connect to anything
  - Solve the resulting model as a traditional fault tree

Sandia National Laboratories

96-13-8

Example "Plug-and-Play" Model

Network to be modeled:

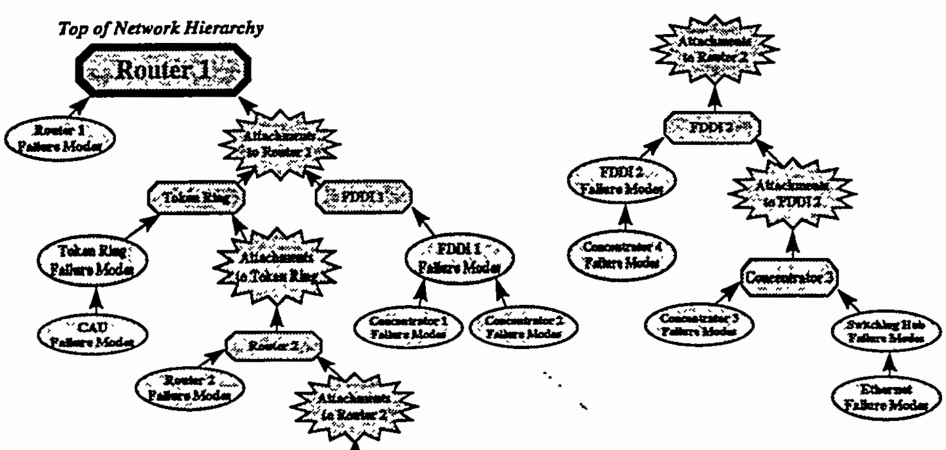


Sandia National Laboratories

96-13-9

Example "Plug-and-Play" Model (cont.)

How fault tree modules can be assembled in the "Plug-and-Play" method.



Sandia National Laboratories

96-13-10

Modeling Quality of Service

To a user, the network "works" when their traffic can get through *and* needed services are available.

- Modeling network services:
  - A typical service is successful if *all* users can access one or more of the server machines that provide this service.
  - Full connectivity *and* an appropriate servers are running. This is the top event for a service fault tree model.
- Modeling classes of network traffic:
  - Definition of "network success" is somewhat subjective.
  - To first order, we can assume any link or network element that cannot support the required network characteristics is "failed" and simply requantify the connectivity cut sets.

Sandia National Laboratories

96-13-11

Non-Hierarchical Networks

Previous reliability models for non-hierarchical networks have used path set theory.

- Path sets are an efficient way to look at reliability between two well-defined endpoints in a network. But...
- "Connectivity" is achieved only when "everyone can talk to everyone else." We want to model this condition.
  - This requires that we find path sets for *all pairwise combinations of endpoints*.
- Path sets cannot show component importance the way cut sets can.
  - It is mathematically difficult and computationally expensive to obtain cut sets from path sets.

Sandia National Laboratories

96-13-12

Non-Hierarchical Networks (cont.)

It is difficult to find cut sets for networks.

- Fault tree analysis methods fail for non-hierarchical networks.
  - To model "everyone can talk to everyone" can require one or more fault trees for *each node in the network!*
  - These fault trees are very difficult to construct because there is clear directionality to follow in the network
  - The problem can become ~combinatorial
- *Huge* numbers of cut sets - even for small networks.
  - Must consider combinations of link and node failures
  - Greater redundancy → more failure combinations to look at

Sandia National Laboratories

96-13-13

Network Solution Strategy

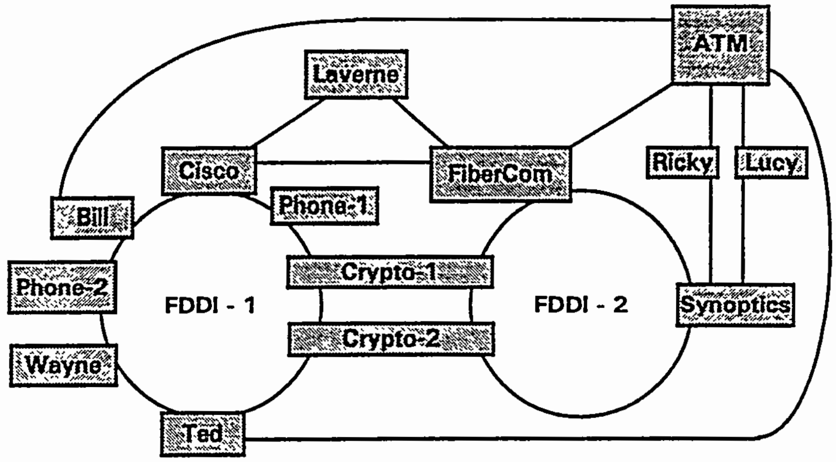
Our method uses several approaches to minimize computational effort for solving networks.

- Simplify the network before solving it (automated and visual simplification)
- Reduce the number of cut sets to be generated
  - Build cut sets based only on link failures (*functional* model)
  - Infer (but do not construct) all cut sets that contain *combinations* of link and node failures
- Efficient cut set search algorithm
  - Developed under Sandia's internal R&D program.
  - Cut sets are found directly from the network architecture connectivity diagram (no FT model construction needed)

Sandia National Laboratories

96-13-14

One "Arbitrarily-Connected" Network Used to Test Our New Methods



Sandia National Laboratories

96-13-15

Building Cut Sets for a Functional Network Model

<u>Objective</u>: reduce the number of cut sets that we have to find directly from the network.

- **Searching the network for cut sets is the most computationally expensive part of the analysis**
- **Strategy to reduce computational effort:**
  - Find the cut sets for a *functional* network model (contain only failures of functional network routes -- look like links)
  - *Infer* the existence of cut sets containing combinations of link and node failures from the functional cut sets.
  - The functional cut sets are to be found by direct search of the network connectivity diagram.

Sandia National Laboratories

96-13-16

Infer Physical Model Cut Sets

A link cannot carry traffic if either the link itself fails *or* the node on either end of the link fails.

- An n-link cut set can give 3^n sets of link and node failures
  - We would have to expand, build and reduce these 3^n cut sets
- Better strategy: Build the build the physical model cut sets in a minimal factored form
  - Essentially all redundant cut sets are generated, so no need to perform the expansion or Boolean reduction
  - We can get by with only two (2) cut set formulae per network division instead of 3^n.
  - This formulation is compatible with quantitative evaluation *and* all cut set and event importance measures.

Sandia National Laboratories

96-13-17

Hybrid Networks

Many networks contain both hierarchical and non-hierarchical sections.

- Example: the telephone network
  - Communication between switches is non-hierarchical, but distribution to end customers ("local loop") is hierarchical.
- We can "marry" fault tree solutions to non-hierarchical solutions to solve hybrid networks.
  - Solve each "level" of the network separately using the most appropriate technique
  - Combine the cut sets to form a global network solution
  - All component importance computations can be performed based on these results

Sandia National Laboratories

96-13-18

Extracting Information From Cut Sets

Cut sets provide a doorway for understanding many aspects of system behavior.

However, the information must be extracted from the cut sets by mathematical manipulation.

- Identify important network failure modes
- Use event importance measures to identify individual components or groups of components that:
  - must be protected to preserve system reliability (RI)
  - are the best candidates for upgrade to obtain the greatest reliability improvement for the money spent (RR)
  - should be monitored as indicators of system risk (FV/PD)
- Discrete optimization techniques (e.g., genetic algorithms) can select the most cost effective system improvements.

Sandia National Laboratories

96-13-19

Potential Applications

Assumptions inherent in the method:

- Each link supports traffic in both directions when it succeeds, and in neither direction when it fails
- If a node fails, it cannot transport data on any link to which it is attached

Applications:

- Data networks (e.g., ATM), Telephone networks
- These methods can also be used to model network-like architectures in non-communications industries.
- Infrastructure (utility distribution systems, etc.)

Sandia National Laboratories

96-13-20

Summary

- Risk-based network analysis techniques have been developed for hierarchical and non-hierarchical networks.
  - *Hierarchical*: "Plug-and-Play" Fault Tree Analysis Method
  - *Non-Hierarchical*: Efficient Network Search Algorithm enables the use of cut sets rather than path sets
  - These methods can be "married" for hybrid networks
- Models can be extended to model network services and classes of network traffic
- These techniques can be used with other systems that utilize network-like architectures.

Acknowledgment: This work was sponsored by the Laboratory-Directed Research and Development Program at Sandia National Laboratories.

Sandia National Laboratories

96-13-21

Point of Contact

For further information on this work, contact

Gregory D. Wyss
Senior Member of Technical Staff
Risk Assessment and Systems Modeling Department
Sandia National Laboratories
P.O. Box 5800, MS 0747
Albuquerque, NM 87185-0747

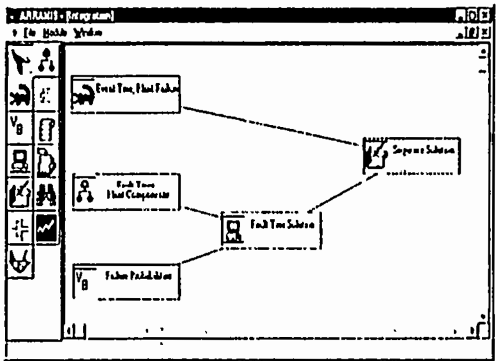
Phone: 505-844-5893
Email: gdwyss@sandia.gov

Sandia National Laboratories

96-13-22

ARRAMIS
(Integrated Risk and Reliability Software)

ARRAMIS



Analysis "Building Blocks" can be assembled in any order using a flow chart paradigm. The most flexible and powerful PRA tool ever!

"Connect the dots" data transfer

Includes analysis integrity security system

Complete **Plug-N-Play** capabilities

PC/Windows 95/NT driven

For more information contact:

Kelly M. Hays
Risk Assessment and Systems Modeling Department
Sandia National Laboratories
P. O. Box 5800, MS 0747
Albuquerque, NM 87185-0747

(505) 844-0547 fax: (505) 844-3321
email: kmhays@sandia.gov
or
arramis@sandia.gov

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

Sandia National Laboratories

"...exceptional service in the national interest."

SAND97-1391

ARRAMIS

Advanced Risk & Reliability Assessment Model Integration Software

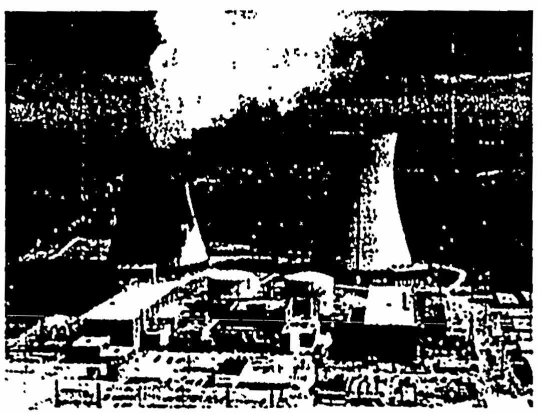
The high consequence surety software package that gives mainframe power on a desktop.

Sandia National Laboratories

ARRAMIS

Incorporates established Sandia PRA Software representing three decades of code development for solving the largest PRA analyses.

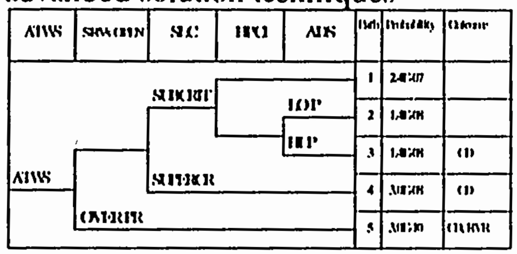
Single package for an entire PRA for high consequence systems such as nuclear reactors, nuclear weapons, telecommunications, aircraft, and infrastructure surety.



Key features of ARRAMIS include:

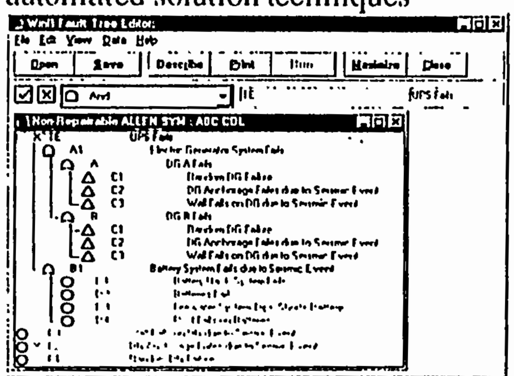
- **Complete event tree analysis**

  Graphical event tree creation and advanced solution techniques



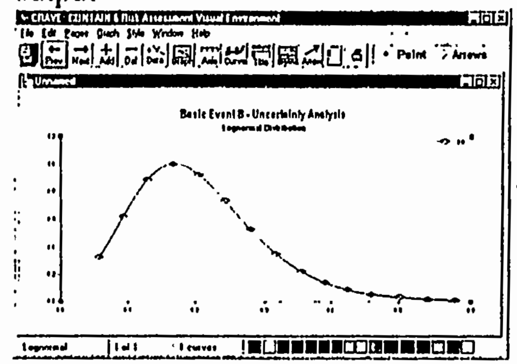
- **Complete fault tree analysis**

  Graphical fault tree creation and automated solution techniques



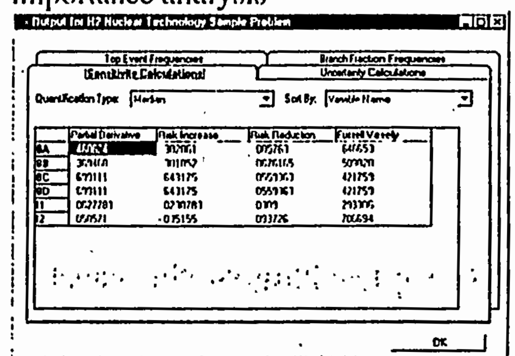
- **State of the art uncertainty analysis**

  Uncertainty data sampling, stratified sampling, and user friendly graphical output



- **Importance analysis**

  State of the art sensitivity and importance analysis



Cassini Fireball Safety Analysis

Probabilistic Safety Assessment '96
Park City, Utah September 29-October 3, 1996

AN OVERVIEW OF THE RISK UNCERTAINTY ASSESSMENT PROCESS FOR THE CASSINI SPACE MISSION

Gregory D. Wyss, Ph.D.
Risk Assessment and Systems Modeling Department 6412
Sandia National Laboratories
Albuquerque, NM 87185-0747

(505) 844-5893 gdwyss@sandia.gov

Sandia National Laboratories

96-14-1

Outline

An Overview of the Risk Uncertainty Assessment Process for the Cassini Space Mission

- Overview of the Cassini Mission and Approval Process
- Tools and Methods for Computing Risk
- Separation of Variability and Uncertainty
- Uncertainty Analysis Computational Process
- Summary

Sandia National Laboratories

96-14-2

The Cassini Mission

Profile:

- Deep space probe to explore Saturn and its moons
  - Anticipated launch: late 1997, to arrive Saturn in 2004
  - Flight path includes gravity assist rendezvous with Venus (2x), Earth and Jupiter to pick up speed
- Carries 3 Radioisotope Thermoelectric Generators (RTGs)

Safety Review and Approval Process:

- Spacecraft design team (LMC) conducts safety analysis
- Reviewed by the Interagency Nuclear Safety Review Panel
- Launch decision made by the Executive Office of the President of the United States.

Sandia National Laboratories

96-14-3

INSRP

The Interagency Nuclear Safety Review Panel (INSRP) reviews all aspects of mission safety.

- Experts include spacecraft breakup, re-entry, meteorology, biological effects of radiation, and uncertainty
- Review the SAR, perform independent confirmatory computations, and make launch recommendations

INSRP mandated the Cassini uncertainty analysis

- Previous launches considered mainly separate effects sensitivity studies with estimates of uncertain ranges
- Panel wants integrated uncertainty analysis with separation of variability from uncertainty

Sandia National Laboratories

96-14-4

Computation of Risk

There are many parallels between the Cassini spacecraft PRA and traditional reactor PRA studies

Cassini Risk Analysis	Reactor PRA Parallel
Probability and characteristics of launch vehicle failures that can jeopardize the space probe (*i.e.*, create the *potential* for radioactive release)	Level I Core Damage Sequence Analysis
Conditional probability that a release occurs given a launch vehicle failure, and characteristics of that release	Level II Accident Progression / Source Term Analysis
Consequences of a radiological release (atmospheric transport, deposition, health effects, contaminated areas, etc.)	Level III Accident Consequence Analysis

Sandia National Laboratories

96-14-5

Computation of Risk (cont.)

Characterization of Launch Vehicle (LV) Failure

- LV failure "Data Book" generated by LV manufacturer
- Taken as "given" for this analysis

Accident Progression and Source Term: LASEP-T Code

- Performs *Monte Carlo* simulation of data book scenarios
  - "Flies" LV fragment field - evaluates impacts on spacecraft
  - Tracks spacecraft parts through reentry to ground impact
- Classifies individual simulations according to "end states"
  - Point estimate of trial's conditional probability of release
  - Discrete distribution of the radiological mass releases
  - Other important source term characteristics (e.g., altitudes)

Sandia National Laboratories

96-14-6

Computation of Risk (cont.)

The SPARRC radiological consequence model depends on release location and characteristics

- Surface impact -- during ascent -- high altitude during reentry
- Impact location characteristics: Rock - Soil - Water
- With or without a propellant fireball
- Radiological mass particle size distribution
- Not many isotopes -- vast majority of the inventory is PU-238

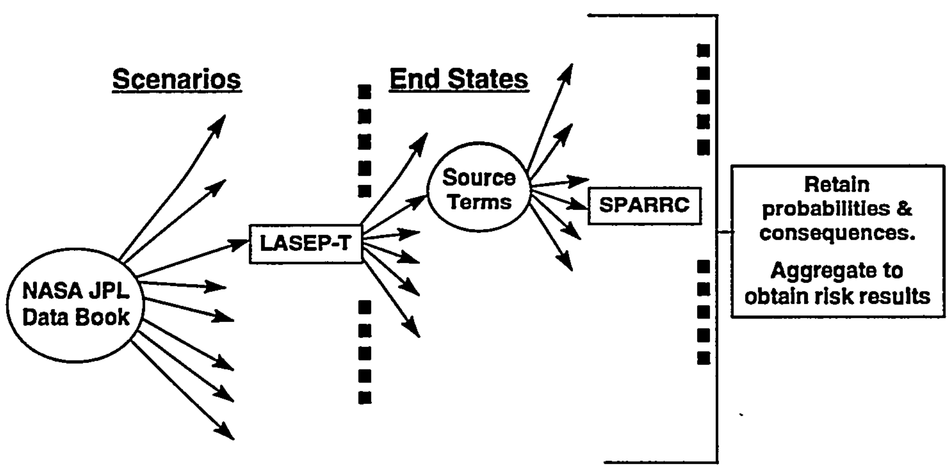
Large number of source terms requires simplification

- Binning of releases with similar characteristics and expected consequences (mass, scenario including altitude, etc.)
- Binning of weather

Sandia National Laboratories

96-14-7

Computation of Risk (cont.)



Sandia National Laboratories

96-14-8

Variability Versus Uncertainty

INSRP wanted the Cassini analysis to attempt to distinguish between variability and uncertainty.

- **Stochastic Variability - The natural variation of system paths and outcomes due to variations in:**
  - **inherently stochastic physical processes, or**
  - **unobserved, unobservable, uncontrolled, or uncontrollable parameters**
- **Knowledge Uncertainty - The uncertainty in system behavior that is due to inadequate understanding of how it is affected by observable or controllable parameters**
- ***Uncertainty* can be reduced if better information can be gained about the physical process itself and/or its root causes. *Variability* cannot be reduced no matter how much we know about the process and its root causes.**

Sandia National Laboratories

96-14-9

Variability Versus Uncertainty (cont.)

Most issues have both uncertainty and variability contributors.

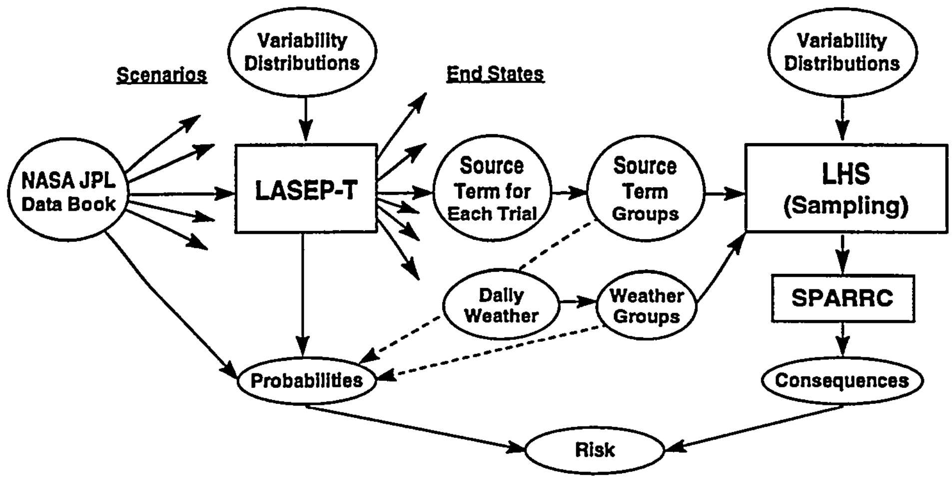
- **It is very difficult to determine the *relative* contributions of uncertainty and variability to a particular issue.**
  - **Often a subject of great controversy**
  - **Still an open research subject -- beyond current state of the art**
- **Therefore, for this analysis, each issue was categorized as either *entirely* "variability" or *entirely* "uncertainty" based on which one "dominates" that issue.**
  - **Only variability (variables) changed for initial risk estimates -- uncertain parameters held as constants to represent a "single world view"**
  - **Both variables and parameters changed during uncertainty analysis**
- ***Note:* We must use the entire range of possibility for every issue regardless of whether it's due to uncertainty or variability.**

Sandia National Laboratories

96-14-10

Variability Analysis Method

(Computes Initial Risk Estimates)



Sandia National Laboratories

96-14-11

Uncertainty Assessment Process

- Ideal Approach:
  - Wrap the risk computation in a Monte Carlo/LHS shell
  - Not feasible because LASEP-T is already a Monte Carlo code
- Practical Approach #1: Direct Substitution Method
  - Run a complete risk analysis similar to variability assessment
  - View each LASEP-T end state as variability, with individual LASEP-T trials as uncertainty for each end state
  - View weather as variable - all other consequence model parameters as uncertainty
  - Mixes variability and uncertainty, but doable without new research
- Practical Approach #2: Mathematical Deconvolution
  - Theory presented on the following slides
  - Can be done using same code runs needed for direct substitution method

Sandia National Laboratories

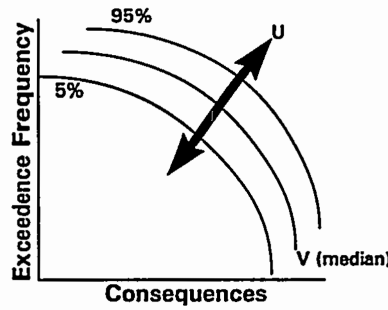
96-14-12

Deconvolution

Basic approach:

- Obtain a distribution for risk based solely on variability (V)
- Obtain a second distribution for risk (R) based on intermingling all uncertainty and variability
- *Assume* there exists a distribution for the effect of uncertainty by itself (U) which, when convolved with V, produces R.
- Use Laplace or Fourier transforms to obtain U.

- Use U to "shift" V to obtain estimates of confidence for risk uncertainty



Each curve is V, shifted based on values from U. The family of curves represents the risk uncertainty.

Sandia National Laboratories

96-14-13

Deconvolution (cont.)

Deconvolution Theory

- Recall: under both Laplace and Fourier transforms, a convolution operation is transformed to multiplication.

$$V^* \bullet U^* = R^*$$

- We have computed V and R explicitly.
  - Transform V and R to Fourier space
  - Divide the transforms to obtain U^*
  - Invert the transform to obtain a representation of U *(not always an easy task)*
- This practice is common in electrical engineering signal analysis. Software is available.

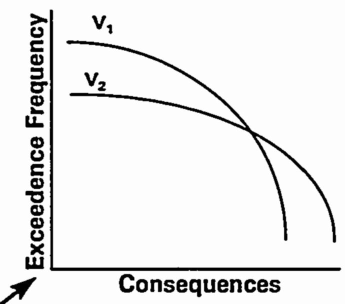
Sandia National Laboratories

96-14-14

Deconvolution (cont.)

Limitations of the Method

- For mathematical rigor, this process only applies to linear transfer functions.
  - Our transfer function (composed of LASEP-T, SPARRC, etc.) is clearly *not* linear. However....
  - Tests of the method with several non-linear transfer functions have still produced reasonable results.
- Under this method, U is simply applied as a factor to shift V.
  - Suppose varying the uncertain parameters would, in reality, cause crossing risk curves. *Deconvolution cannot find this behavior!*

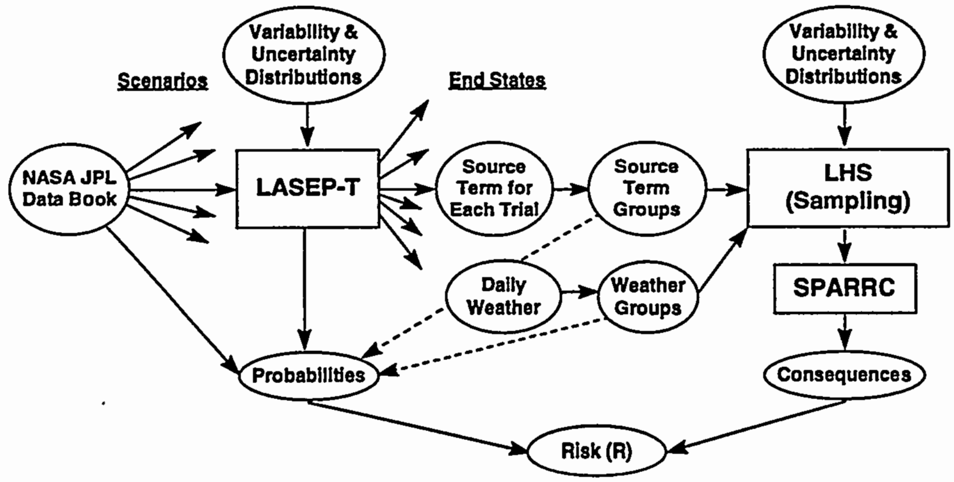


Sandia National Laboratories

96-14-15

Uncertainty Analysis Method

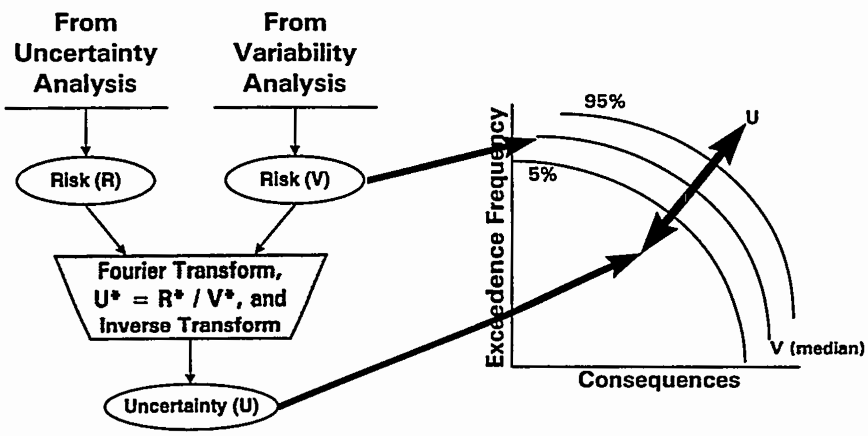
(Computation is Virtually Identical to the Variability Analysis)



Sandia National Laboratories

96-14-15

Deconvolution Process



Sandia National Laboratories

96-14-17

Summary

The Cassini variability and uncertainty analysis is a dramatic step forward from previous launch analyses.

- **Uncertainty Analysis**
  - **Separation of variability and uncertainty**
  - **Same computations can be used with either Direct Substitution or Deconvolution**
- **New Method: Deconvolution**
  - **Produces a family of risk distributions**
  - **Uncertainty distribution (derived from Fourier transform) shifts the variability distribution to find full picture of risk**
  - **Provides a "pure" separation of variability and uncertainty**

Sandia National Laboratories

96-14-18

KBERT/CONTAIN
(Integrated Tool for Facility Safety Hazard Analysis)

CONTAIN / KBERT

An Integrated Analysis Tool to Assess Consequences of Dispersal of Hazardous Agents in Facilities

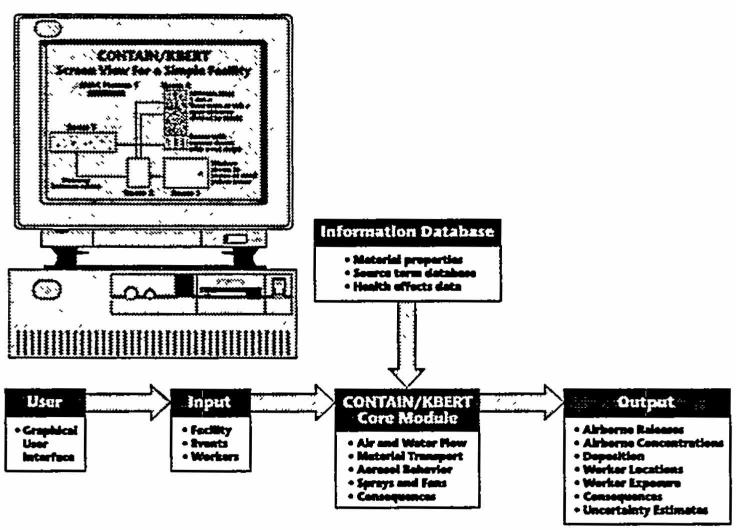
Richard O. Griffith
John E. Brockmann
Daniel J. Rader
Ken E. Washington

Sandia National Laboratories
Albuquerque, NM

6421-RG-5/15/97-1-0

Sandia National Laboratories

CONTAIN / KBERT Concept



6421-RG-5/15/97-2-0

Sandia National Laboratories

CONTAIN / KBERT Overview

- **Role of CONTAIN / KBERT**
  - A knowledge-based computer tool designed to be routinely used in the safety analysis of facilities
  - More easily and more consistently apply existing material release and material properties databases
  - Leverage existing CONTAIN code capabilities for analyzing aerosol behavior and material transport in facilities
  - Evaluate exposures and consequences to personnel
  - Allow quantitative evaluation of uncertainties
- **Other Potential Applications**
  - Assist in building design
  - Evaluate and assess mitigation strategies
  - Assist in review and evaluation of safety analysis reports
  - Tool for conducting hazard assessments in DOE facilities
  - Evaluation of proposed new activities at existing facilities

6421-RG-5/15/97-3-0 Sandia National Laboratories

Interior Transport – The CONTAIN Code

- **CONTAIN:**
  - Developed at SNL for the USNRC to analyze nuclear reactor containment accidents and experimental facilities
  - Under continuous development and testing for over 15 years, and represents a total investment by the USNRC of approximately $20M
  - Being adopted as principal licensing tool for the USNRC
  - Substantial validation and assessment database: successfully completed a two-year external peer review to certify its modeling capabilities
  - Broadly used throughout the U.S. and the world by national laboratories, industry, contractors, and universities.

6421-RG-5/15/97-4-0 Sandia National Laboratories

CONTAIN Key Features and Capabilities

- Control volume approach, arbitrary network of volumes and structures
- CONTAIN can model
  - Gas thermodynamics and flow
  - Aerosol transport and deposition
  - Fans/ventilation systems
  - Fire system sprays
  - Walls, floors, ceilings
  - Airborne debris
  - Water pools
- Designed to support Probabilistic Risk Assessment *(PRA)* studies to evaluate trends and uncertainties in large complicated problems

6421-RG-5/15/97-5-0

Sandia National Laboratories

CONTAIN/KBERT Key Features
Facility Configuration

- Rooms
  - Basic building blocks for representing internal regions of a facility: offices, labs, hallways, etc.
  - Arbitrary number of rooms can be specified
- Structures
  - Represents aerosol deposition surfaces and heat sinks
  - Arbitrary number of structures can be specified
- Doorways
  - Can represent any opening: doors, windows, pipes, etc.
  - Arbitrary number of parallel or serial connections
- HVAC Ducts
  - Connects rooms to one or more HVAC systems
  - Inlets from environment or exhaust to environment
  - Filter can be placed in any flowpath

6421-RG-5/15/97-6-0

Sandia National Laboratories

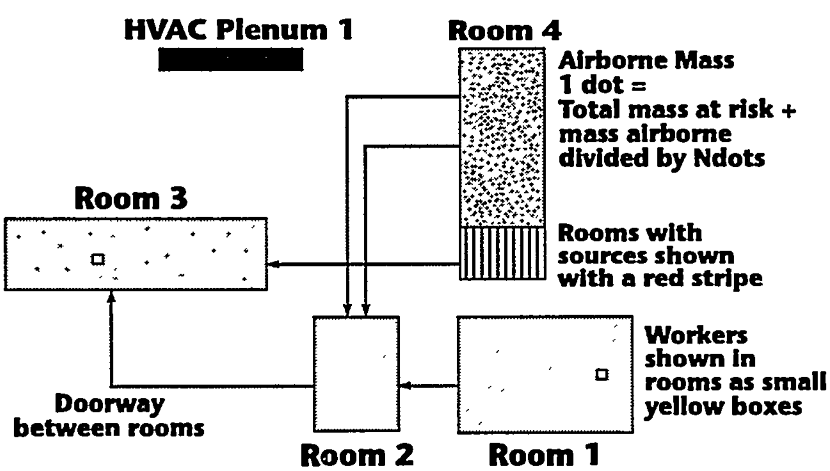
CONTAIN/KBERT Key Features
Personnel Treatment

- **Evacuation Plan Specified for each Worker**
  - Models movement of workers through facility
  - Rooms and delay times specified
  - Used to represent alarm response plan
- **Personnel Physical Parameters**
  - Breathing Rate *(affects inhalation dose)*
  - Skin Area *(affects deposition onto skin -- skin dose)*
- **Dose Shielding Factors**
  - Unprotected, Half-mask, Full-mask, SCBA
  - Inhalation Protection
  - Cloudshine Protection
  - Groundshine Protection
  - Skin Protection

6421-RG-5/15/97-7-0

Sandia National Laboratories

CONTAIN / KBERT
Screen View for a Simple Facility



6421-RG-5/15/97-8-0

Sandia National Laboratories

CONTAIN / KBERT Application Environment

- **Target Platform**
  - Desktop IBM-compatible personal computer
  - Microsoft Windows 95 operating system
- **Programming Language**
  - KBERT object-oriented design *(C++)* facilitates extensions
  - Transparently links to CONTAIN code in FORTRAN
- **Database Tools**
  - Microsoft Access relational database
  - Graphical front end for rapid database development
  - Database easily accessed from Visual C++ code
  - Easy to enable access of data across a network

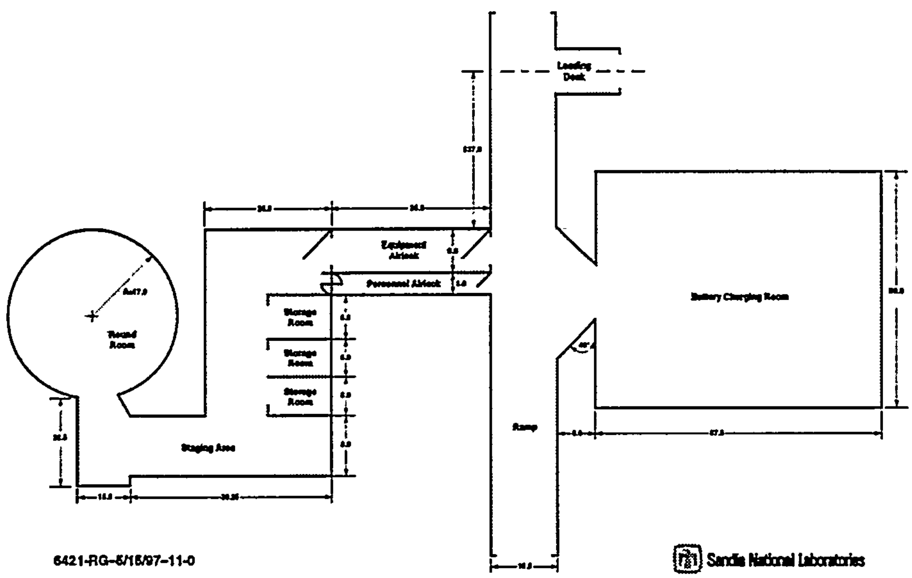
6421-RG-5/15/97-9-0 Sandia National Laboratories

Demonstration of Capabilities – Pantex

- December 1995: Urgent DOE need to assess radiological consequences of high explosives detonation in Pantex assembly cell
- DOE required credible estimates of exposures from release both on and off site for the Environmental Impact Statement
- SNL integrated existing codes and analysis capabilities to answer DOE questions and solve their problem
- July 1996: Letter of Commendation from DOE/AL head Bruce Twining to SNL executive VP John Crawford

6421-RG-5/15/97-10-0 Sandia National Laboratories

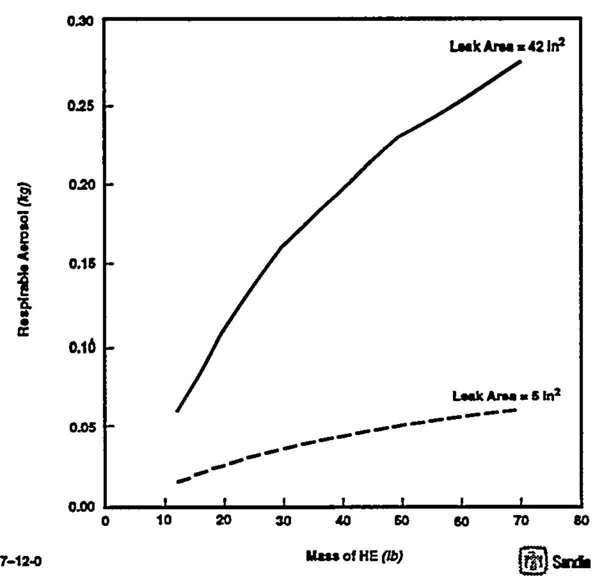
Pantex Assembly Cell



6421-RG-5/15/97-11-0

Sandia National Laboratories

Pantex Aerosol Release



6421-RG-5/15/97-12-0

Sandia National Laboratories

Distribution:

1 John Ahearne
102 Rose Lane
Chapel Hill, NC 27514

1 George Apostolakis
Room 24-221
77 Mass. Ave.
Cambridge, MA 02139-4307

1 John Garrick
4590 MacArthur Blvd.
Suite 400
Newport Beach, CA 92660-2027

1 Rush Inlow
US DOE Albququerque Operations Office
Pennsylvania at Henry Street
Albuquerque, NM 87116

1 Alan Moghissi
5457 Twin Knolls Rd.
Columbia, MD 21045

1 Frank Parker
400 24th Ave. South
Room 106 Jacobs Hall
Nashville, TN 37235

1 Evaristo Bonano
BETA Corporation International
6719-D Academy Road NE
Albuquerque, NM 87109

1 Mohemed El-Genk
University of New Mexico
Institute for Space and Nuclear Power Studies
Albuquerque, NM 87131-1341

1 Ahmed Hasan
University of New Mexico
School of Engineering
Albuquerque, NM 87131-1341

1 Yacov Haimes
University of Virginia
Center for Risk Management of Engineering Systems
Thornton Hall
Charlotteville, VA 22903

1 MS 0736 Nestor Ortiz, 6400
10 MS 0716 Evan Dudley, 6805
1 MS 0716 Regina Hunter, 6805
1 MS 0722 Ken Sorenson, 6804
1 MS 1139 Ken Reil, 6423
1 MS 0149 Dan Hartley, 4000
1 MS 0405 Todd Jones, 12333
1 MS 0747 Allen Camp, 6412
1 MS 0747 Vince Dandini, 6412
1 MS 0747 Greg Wyss, 6412
1 MS 0747 Donnie Whitehead, 6412
1 MS 0744 Mike Hessheimer, 6403
1 MS 0767 Fred Harper, 6314
1 MS 0769 Dennis Miyoshi, 5800
1 MS 1345 Paul Davis, 6416
1 MS 1138 Sharon Chapa, 6533
1 MS 0718 Sieglinde Neuhauser, 6314
1 MS 1337 Wendell Weart, 6000
1 MS 0744 Dana Powers, 6404
1 MS 0701 Richard Lynch, 6100
1 MS 1140 Jim Rice, 6000
1 MS 0405 Allan Benjamin, 6413
1 MS 0739 Ken Bergeron, 6421
1 MS 0742 John Kelly, 6414
1 MS 0718 Richard Yoshimura, 6641
1 MS 0746 Bob Cranwell, 6613
1 MS 1206 Kelly Hays, 6412
1 MS 1080 Jim Smith, 1325
1 MS 1137 Ken Washington, 6614
1 MS 1328 Mert Fewell, 6849

2	MS 0619	Review & Approval Desk, 12630 For DOE/OSTI
5	MS 0899	Technical Library, 4414
1	MS 9018	Central Technical Files, 8940-2