SAND98-0599C
SAND--98-0599C

SURETY APPLICATIONS IN TRANSPORTATION

CONF-980132--

by
Rudolph V. Matalucci and Dennis S. Miyoshi
Security Systems and Technology Center 5800
Sandia National Laboratories
Albuquerque, New Mexico 87185-0761

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.

Presented January 5, 1998 at the
THIRTY-FIFTH PAVING AND TRANSPORTATION CONFERENCE
Cosponsored by the Department of Civil Engineering and the ATR Institute of The University of New Mexico

RECEIVED
MAR 17 1998
OSTI

ABSTRACT

Infrastructure surety can make a valuable contribution to the transportation engineering industry. The lessons learned at Sandia National Laboratories in developing surety principles and technologies for the nuclear weapons complex and the nuclear power industry hold direct applications to the safety, security, and reliability of our critical infrastructure. This presentation introduces the concepts of infrastructure surety, including identification of the normal, abnormal, and malevolent threats to the transportation infrastructure. National problems are identified and examples of failures and successes in response to environmental loads and other structural and systemic vulnerabilities are presented. The infrastructure surety principles developed at Sandia National Laboratories are described. Currently available technologies including a) three-dimensional computer-assisted drawing packages interactively combined with virtual reality systems, b) the complex calculational and computational modeling and code-coupling capabilities associated with the new generation of supercomputers, and c) risk-management methodologies with application to solving the national problems associated with threats to the critical transportation infrastructure are discussed.

19980420 018

The Challenge

The new and emerging threats to the critical transportation infrastructure faced by today's engineering design and facility management community demand innovative solutions that are increasingly based on risk management approaches. In the wake of the World Trade Center, Oklahoma City, and Saudi Arabian bombings; global civil and ethnic unrest; criminal and political terrorism; the Chunnel fire; recent natural disasters; and other indicators of a rapidly transforming social world, there is a growing awareness of public vulnerability. This awareness leads to increased expectations and responsibilities for the infrastructure design, engineering, and construction professionals. The destruction that follows such natural disasters as hurricanes, tornadoes, floods, and earthquakes also underscores the need for enhanced transportation system and structural safety, security, and reliability to protect the public

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

MASTER

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

from potential injuries, death, and heavy property losses. A multidisciplinary risk-management-based program has been developed at Sandia National Laboratories to address many of these critical national issues in this area by applying appropriately selected surety concepts, procedures, and technologies that were developed to support the safety, security and reliability of the nuclear weapons programs.

Infrastructure Surety Concepts

Infrastructure surety is a risk-management approach to providing

- SAFETY in response to abnormal threats
- SECURITY in response to malevolent threats
- RELIABILITY in response to normal threats

Figure 1 depicts this definition graphically. All three elements must be addressed in surety consideration. However, as illustrated in Figure 1, one element predominates for each of the threat conditions indicated.

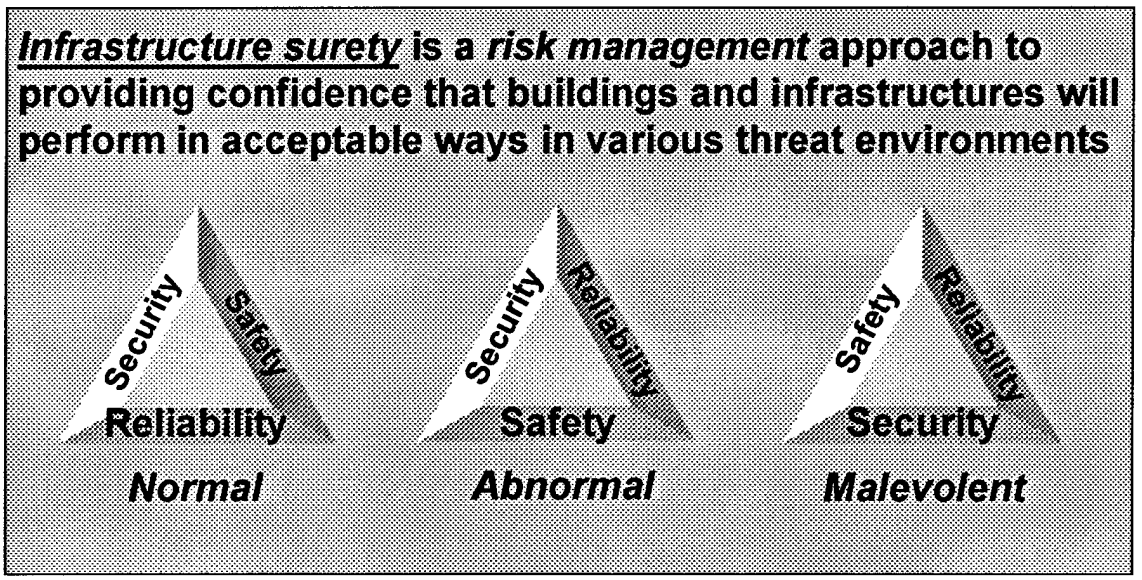

Figure 1. Infrastructure Surety Threat Diagram

The goals of infrastructure surety are to enhance public safety and security, ensure the reliability and quality of our critical infrastructure elements (including but not limited to transportation systems and structures), and increase public awareness of the benefits of applying surety principles to the design or retrofit of public, commercial, and private systems, facilities and structures. The program at Sandia National Laboratories is

organized into four major elements to better provide the necessary technologies for an integrated approach to addressing the national surety issues and needs (Figure 2).

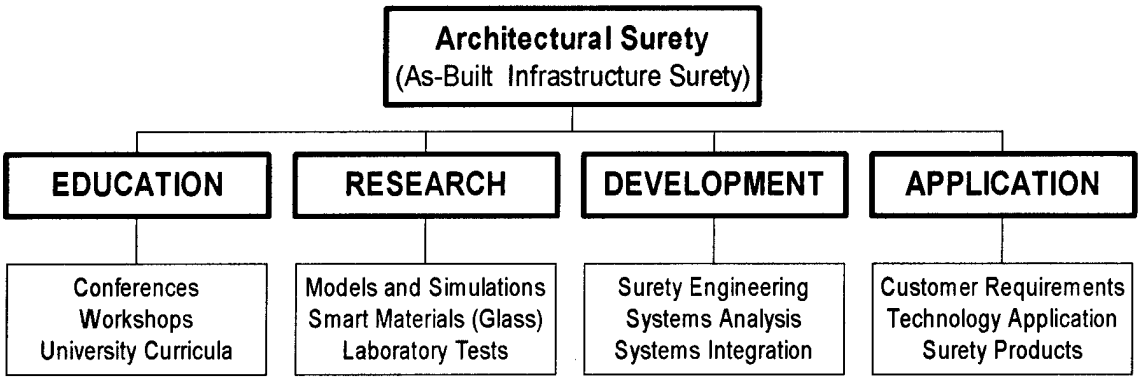

Figure 2. Infrastructure Surety Program at Sandia National Laboratories

Conference presentations such as this one are a part of the education outreach effort. Objectives include applying surety principles to national problems, gaining consensus within technical communities, impacting change to engineering curricula, and creating a national constituency. The research, development, and application efforts are equally necessary to ensure that the most appropriate technologies are made available for the identified problems of national significance. (See References 1 and 2 for additional information.)

National Problems

Threat environments for infrastructure elements, such as transportation systems and facilities, can be identified as normal, abnormal, and malevolent. Normal threats to the built environment are those that are considered to be usual insults to the structure and operation of a structure or system, such as aging, weathering, and other easily predicted, naturally occurring, or manmade loads. Abnormal threats include catastrophic natural disasters, such as Hurricane Andrew in 1992, the 1994 Northridge Earthquake, or the recent flooding along the Red River in North Dakota. Malevolent threats are deliberate acts in nature, resulting from terrorist activities or other intentional human-induced damage to the as-built infrastructure.

Normal Threats

Urban decay, the aging and deterioration of the urban infrastructure, is a normal threat to transportation and other urban infrastructure systems. For example, the "Woodrow Wilson Bridge in the Washington, DC area is a critical link in the Interstate 95 corridor,

used by hundreds of thousands of people on a daily basis. It is quite literally falling apart . . . " according to Congressman Bud Shuster, Chairman, House Transportation and Infrastructure Committee. Rodney Haraga of the City of Los Angeles Bureau of Engineering reports that "Los Angeles has over 7000 miles of streets in need of resurfacing, yet the city budget limits repaving to only 150 miles annually." Concerns about our crumbling cities are voiced by national politicians and local officials alike.

Accidents, usually caused by human error, are normal threats to the environment. Tacoma's Galloping Gertie bridge collapse, the sinking of the Titanic, the Challenger disaster, and the fire in the Chunnel are just a few of the spectacular failures that provided lessons for future structures. Failures are likely to result from such situations as designing a bridge to carry 70,000 cars per day and allowing it to carry 170,000 vehicles per day, 17,000 of which are heavy trucks (Woodrow Wilson Bridge). Building roads for a 20-year design life and using them for 50 years with minimal maintenance (the City of Los Angeles) is another example of current use exceeding the original design criterion.

Abnormal Threats

Abnormal threats include natural disasters that cause severe consequences. Predicting 100-year-floods or the probability of an earthquake of a particular magnitude occurring in a specific earthquake zone or the peak quartering winds likely during hurricane season are well within our capabilities. However, applying this information to the design and retrofit of existing transportation and other critical infrastructure systems is frequently a post-disaster exercise. The principles of infrastructure surety can identify risks before the problems occur and provide for an appropriate level of protection for risk reduction. For example, the City of Los Angeles has bridges spanning the flood control channel that were built by the WPA in the 1930s. Should a major earthquake render these aging major bridges impassable, 4 million residents would be trapped with only the Ventura Freeway to the northwest available for egress, according to Rodney Haraga of the City of Los Angeles, Bureau of Engineering. Similarly, the City of Tampa is vulnerable to being isolated by hurricane or flood, and wind damage to or destruction of its bay bridge.

From the Kobe Earthquake, EQE International learned a great deal about the vulnerabilities of the Japanese transportation system. The collapse of the Hanshin Expressway showed us what worked (steel-jacketed columns and lighter steel framing) and what didn't (unreinforced supports and heavier concrete framing) (Figure 3). Inadequate supports left a new bridge just a few inches and a few seconds away from collapsing into Osaka Bay (Figure 4). In retrospect, there is some indication that these problems might have been foreseen or prevented if vulnerability assessments were made as a routine precaution.

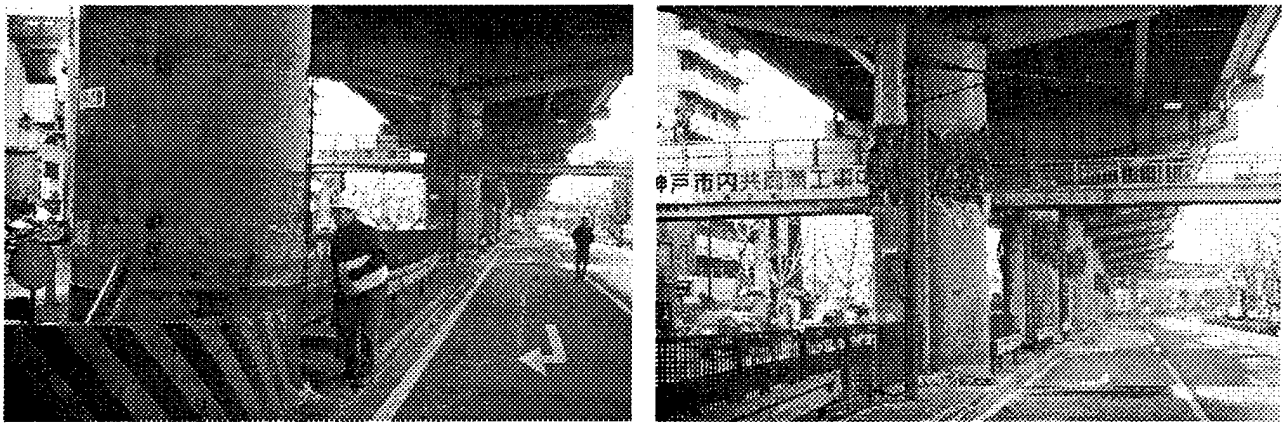

Figure 3. Portions of the Hanshin Expressway That Withstood (left) and Collapsed (right) During the Kobe Earthquake (courtesy of EQE International, Inc.)

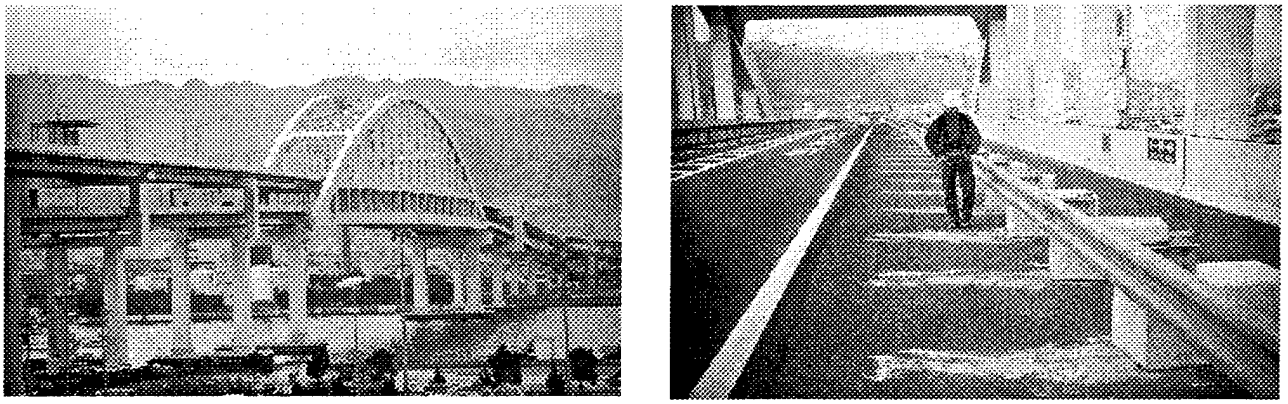

Figure 4. Bridge Over Osaka Bay (left) and Inadequate Supports (right) (courtesy of EQE International, Inc.)

Malevolent Threats

Malevolent threats are intentional human attacks upon the infrastructure. Acts of terrorism, such as the Sarin gas attack in a busy Tokyo subway station or the World Trade Center, Oklahoma City Federal Building, and Khobar Towers bombings, are among the well-known malevolent threats to our infrastructure. Any use of weapons of mass destruction, whether chemical, biological, or radiological, could severely impact our transportation systems, anywhere and at anytime.

Transportation facilities and structures, such as airports, bridges, freeways, tunnels, trams, are equally vulnerable to explosive attacks or other criminal or political acts of terrorism. The economic and political consequences of disrupting our nation's

transportation systems are obvious, and the impact caused by a long recovery period may be even more costly than the act itself.

Considering these threats at all points in the life-cycle of a project is one of the methods the infrastructure surety program recommends to reduce risk, thereby enhancing the safety, security, and reliability of the system or structure under development. Figure 5 shows the life cycle of a construction project. Surety has an important role in each of these stages. Surety plans developed for each stage highlight system shortcomings and provide insight to the owners concerning risks that can be minimized through appropriate actions.

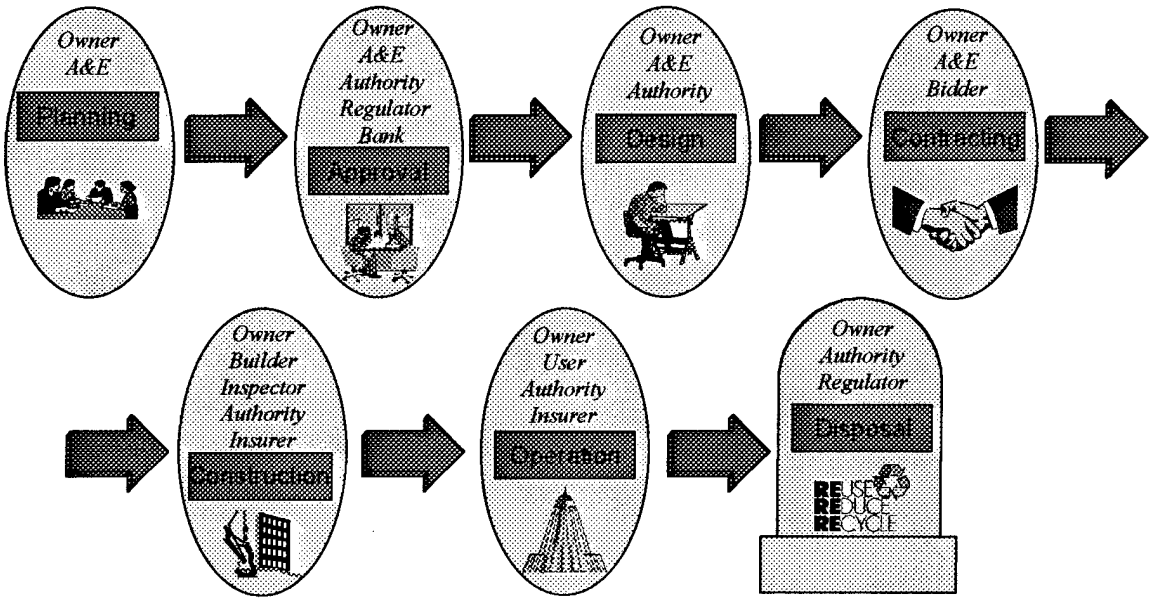

Figure 5. Life-Cycle Sustainable Development

Available Technologies

Normal, abnormal, and malevolent threats to our critical transportation infrastructure create national problems that can be addressed using surety products. Sandia's core competencies in structural and constitutive modeling, computational simulations, material properties and behavior, risk management, and systems analysis are applied to develop infrastructure surety analysis tools and other surety products. These technologies, including methodologies, procedures, tools, and products, can be adapted to address the requirements specified by the customer for a particular or general engineering, architectural, or construction application. A brief description of some of these available surety products follows.

Three-Dimensional Computer-Aided Drawing and Virtual Reality Capabilities

Application of virtual reality capabilities to the infrastructure would include easily applied, three-dimensional, interactive visualization developed from three-dimensional computer aided design (CAD) and computational files, including simulated effects of proposed mitigation measures. This capability permits virtual reality evaluation of antiterrorist measures (e.g., security devices) prior to the construction or retrofit of structures and transportation systems. In addition, a realistic virtual environment for the planning and training of emergency, disaster, and counter-terrorism responses, including law enforcement, search-and-rescue, and medical first-responder personnel, would be a boon to designers of vulnerable transportation systems and facilities.

Recent news reports describe the cost savings the Minnesota Department of Transportation expect to achieve by using a "virtual highway" developed at the University of Minnesota's Human Factors Research Laboratory to design a rebuild of a section of Minnesota Highway 61 through Tofte, MN. The design was tested before it was constructed, and unanticipated problems were identified and corrected on line.

As a further example, an interactive visualization of an airport or a freeway interchange could provide:

- Threat assessment and surety evaluation
- Evaluations of possible mitigation measures
- Finite-element analysis of structural integrity
- Simulation models for law-enforcement analysis, load effects and responses, and event scenarios in real time

Computational Simulation

The "Revolution in Engineering" afforded by new supercomputing capabilities (Figure 6) opens new calculational modeling and simulation opportunities. Sandia's teraflops (1.8 *trillion* floating operation points per second) computer, developed with Intel, enables complex calculations to be performed very quickly. Potential applications of this supercomputer (as powerful as 81 Pentium PCs) include:

- Model codes can be coupled (structural and blast effects)
- Innovations can be validated before construction
- Materials performance can be evaluated
- Life-cycle performance can be predicted and analyzed

Risk-Management Technologies

Another infrastructure surety application of Sandia technology is the performance of risk analyses including probabilistic risk assessments (PRAs) that have been

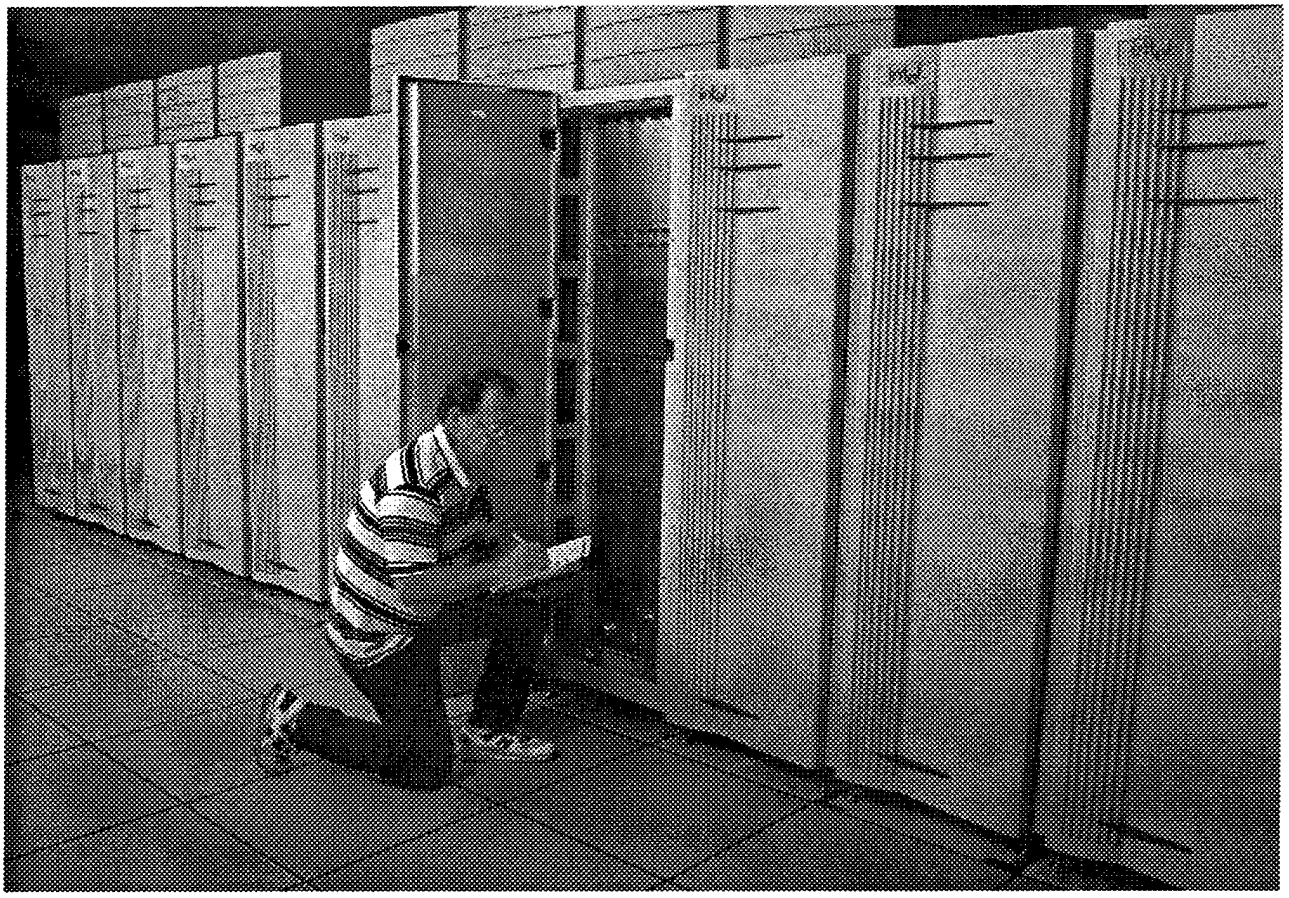

Figure 6. The Teraflops Supercomputer at Sandia National Laboratories

developed through nuclear weapons and power plant design programs. These procedures can evaluate the impact of proposed design, construction, and mitigation and remediation actions upon structural and system response to explosions, earthquakes, windstorms, floods, and fires. Design professionals can use a PRA-based methodology to uncover previously unidentified vulnerabilities and unexpected consequences. Such information enables the science-based evaluation of mitigation measures for known vulnerabilities to defined threat scenarios. PRA includes threat analysis and accident sequence analysis.

Reliability predictions are performed by screening models and developing prioritization analyses. They can be used to make important decisions involving design tradeoffs by providing a framework for systematically evaluating the conceptual model, physical process models, and other available information. Reliability prediction also includes data uncertainty analysis that enhances the design robustness and identifies information needs. By comparing the results to the performance objective, informed decisions can be made at customer-determined acceptable risk levels.

Software development is another important available tool. Personal computer software can be adapted to perform probabilistic risk assessments for the evaluation of threats to infrastructure elements such as roads and bridges. Such software can:

- Assess vulnerability to environmental effects, loads, and malevolent threats
- Use the probabilistic risk assessment methodology to uncover previously unidentified threats and unintended consequences
- Evaluate benefits of mitigation measures
- Perform cost-benefit analyses

Figure 7 illustrates the experience, diversity, and capabilities of the risk management programs at Sandia.

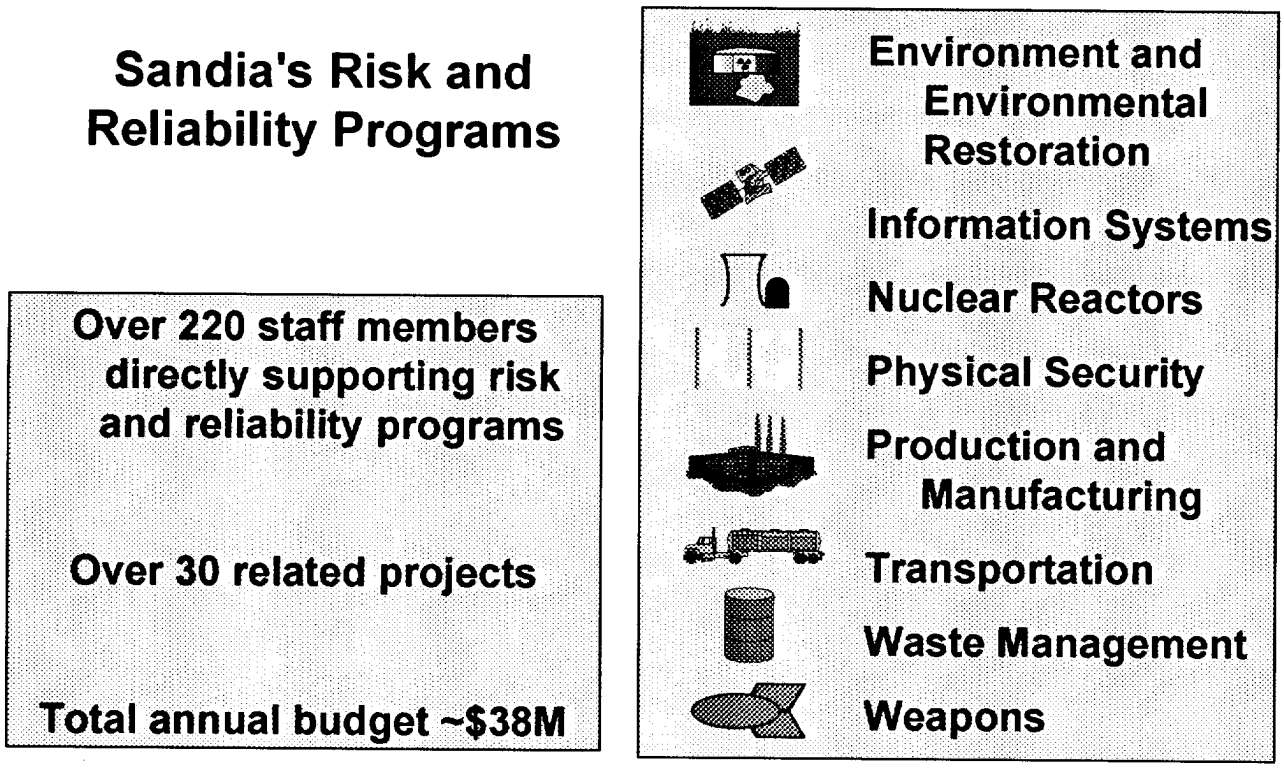

Figure 7. Risk and Reliability Expertise at Sandia National Laboratories

Sandia scientists and engineers are working with design and construction professionals to develop a technical approach and process for determining the level of threat and risk attached to a particular facility, system, or structure. The goal of this work is to assist architects, engineers, and other design professionals in designing for risk reduction through application of infrastructure surety concepts.

Summary

The critical transportation infrastructure is subject to normal, abnormal, and malevolent threats. Technologies are available to identify and assess these vulnerabilities, and to manage these inherent risks. Application of these technologies and the surety principles can improve the safety, security, and reliability of our nation's transportation infrastructure.

References

1. Security Systems and Technology Center, *Proceedings of Assuring the Performance of Buildings and Infrastructures: A Conference on Architectural Surety,* held in Albuquerque, NM, May 14-15, 1997. Sandia National Laboratories, Albuquerque, NM, 1997. (Portions of these proceedings are available on the Internet. Please see http://www.sandia.gov/archsur)

2. R. V. Matalucci, D. S. Miyoshi, and S. L. O'Connor, *A Curriculum for Infrastructure and Architectural Surety*, SAND98-TBD. Sandia National Laboratories, Albuquerque, NM, 1998 (in draft).

ABOUT THE AUTHORS

Rudolph V. Matalucci, Presenter - Rudy Matalucci is a Senior Member of the Technical Staff at Sandia National Laboratories, where he has been employed since 1980 after retiring from military service with the United States Air Force. While serving in the Air Force, he directed R&D programs for architectural and engineering design, construction, experimental testing, and evaluation of hardened facilities for missile systems, fighter aircraft, and underground command centers. Since joining Sandia, he has been the project leader and principal investigator for projects, concerning underground nuclear waste repository testing and evaluation, underground oil storage investigations, environmental site remediation and restoration, and advanced nuclear weapons storage and handling complexes. Rudy is currently the project leader for the Architectural and Infrastructure Surety program at Sandia. He holds three degrees in civil engineering: a BS from the University of New Hampshire and an MS and a Ph.D. from Oklahoma State University.

Dennis S. Miyoshi, Co-author - Dennis Miyoshi has been employed at Sandia National Laboratories since 1969. He holds a B.S. in physics from Stanford University and a Ph.D. in experimental physics from Cornell University. His early work included upper atmospheric studies of the earth's magnetic field, underwater studies of bioluminescence and other optical phenomena, and research into the properties of ultraviolet and infrared detectors. In the mid-1970s he joined the Nuclear Security Systems Directorate that had just been formed in response to the terrorist threat exhibited at the Munich Olympics. He had been responsible for automated inventory systems for nuclear material, for R&D in security technologies, and for developing security systems principles. He brought this experience and talent to his new assignments.

He is presently director of the Security Systems and Technology Center, a Sandia National Laboratories organization of more than 140 security staff members experienced in systems analysis, security technologies, and systems integration and implementation. His current interests include applying security concepts and technologies developed for the Department of Energy to the security problems of our citizens, including the mitigation of crime, fraud, and theft.

M98002803

Report Number (14) SAND--98-0599C
CONF-980132--

Publ. Date (11) 199801
Sponsor Code (18) DOE/DP, XF
UC Category (19) UC-700, DOE/ER

DOE