SANDIA REPORT

SAND98–2086
Unlimited Release
Printed September 1998

An Introduction to Architectural Surety[SM] Education

Rudolph V. Matalucci and Dennis S. Miyoshi
Security Systems and Technology Center

Sharon L. O'Connor
Tech Reps, Inc.

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 Depart-ment of Energy by Sandia Corporation.

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: A03
Microfiche copy: A01

SAND98-2086
Unlimited Release
Printed September 1998

An Introduction to Architectural Surety℠ Education

Rudolph V. Matalucci and Dennis S. Miyoshi
Security Systems and Technology Center
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0761

Sharon L. O'Connor
Tech Reps, Inc.
Albuquerque, NM 87110

Abstract

This report describes the Sandia National Laboratories (Sandia) educational outreach activities in the developing field of architectural and infrastructure surety, a risk management approach to enhancing the safety, security, and reliability of facilities, systems, and structures. It begins with a description of the field of architectural and infrastructure surety, including Sandia's historical expertise and experience in nuclear weapons surety. An overview of the 1996 Sandia Workshop on Architectural Surety℠ is then provided to reference the initiation of the various activities. This workshop established the need for a surety education program at the University level and recommended that Sandia develop the course material as soon as possible. Technical material was assembled and the course was offered at the University of New Mexico (UNM) during the 1997 spring semester. The bulk of this report accordingly summarizes the lecture material presented in this pioneering graduate-level course on Infrastructure Surety in the Civil Engineering Department at UNM. This groundbreaking class presented subject matter developed by experts from Sandia, and included additional information from guest lecturers from academia, government, and industry. Also included in this report are summaries of the term projects developed by the graduate students, an overview of the *1997 International Conference on Architectural Surety℠: Assuring the Performance of Buildings and Infrastructures* (co-sponsored by Sandia, the American Institute of Architects, and the American Society of Civil Engineers), and recommendations for further course work development. The U.S. Department of Energy provides support to this emerging field of architectural and infrastructure surety and recognizes its broad application to developing government, industry, and professional standards in the national interest.

Intentionally Left Blank

Acknowledgments

There are numerous people who have made significant contributions to the education element of the Architectural Surety℠ Program at Sandia. We acknowledge the following individuals for their contribution to this surety education development program:

Tom Baca, *Sandia National Laboratories*

Allen Camp, *Sandia National Laboratories*

Joel Carlson, *Sandia National Laboratories*

John Covan, *Sandia National Laboratories*

Robert Cranwell, *Sandia National Laboratories*

Lee Dickinson, *Failure Analysis Associates, PA*

Ray Finley, *Sandia National Laboratories*

Tobias Flatow, *Flatow, Moore, Shaffer, & McCabe, PA*

Mary Green, *Sandia National Laboratories*

Jerome Hall, *University of New Mexico*

Eve Hinman, *Hinman Consulting Engineers*

Richard Little, *National Research Council*

Lyman Sandy, *Miller, Stratvert, & Torgerson, PA*

Russell Skocypek, *Sandia National Laboratories*

The authors also acknowledge the unique contributions made by the first graduate students to attend an architectural surety℠ class. Their feedback has been invaluable. In addition, the support of our colleagues at Sandia National Laboratories, who endorsed the architectural surety℠ concept and inspired us to continue with the project, is deeply appreciated. Jamy Peevy of Sandia National Laboratories produced teaching aids, presentation materials, and course documentation, and her professionalism and dedication are gratefully acknowledged.

The major portion of this surety graduate education development project was funded directly by the Defense Programs of the U.S. Department of Energy.

Intentionally Left Blank

Contents

Intentionally Left Blank

Figures

Intentionally Left Blank

Tables

Intentionally Left Blank

Acronyms and Abbreviations

A/E	Architectural/Engineering
ADPA	American Defense Preparedness Association
AIA	American Institute of Architects
AISC	American Institute of Steel Construction
ASCE	American Society of Civil Engineers
ASCI	Accelerated Strategic Computing Initiative
ASD	Adversary Sequence Diagram
BE	Basic Event
CAD	Computer-Aided Design
CDF	Cumulative Distribution Function
CCDF	Complementary Cumulative Distribution Function
CCTV	Closed-Circuit Television
CE	Civil Engineering
CIA	Central Intelligence Agency
CPTED	Crime Prevention Through Environmental Design
DE	Developed Event
DoD	U.S. Department of Defense
DOE	U.S. Department of Energy
DSWA	Defense Special Weapons Agency
EE	External Event
EMI	Electromagnetic Interference
FaA	Failure Analysis Associates
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FMEA	Failure Modes and Effects Analysis
FMSM	Flatow, Moore, Shaffer, & McCabe, Inc.
FS	Factor of Safety
HAZOPS	Hazardous and Operability Study
IBC	International Building Code
ICBO	International Conference of Building Officials
IR	Infrared
LOS	Line-of-Sight
MIT	Massachusetts Institute of Technology
MSBLCE	Modeling and Simulation-Based Life-Cycle Engineering
MTBF	Mean Time Between Failures

MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
NBIS	National Bridge Inspection Standards
NCJRS	National Crime Justice Reference Service
NFPA	National Fire Protection Agency
NRC	National Research Council
NTSB	National Transportation Safety Board
NWC	Nuclear Weapon Complex
PIN	Personal Identification Number
PPS	Physical Protection System
PRA	Probabilistic Risk Assessment
S	Safety Margin
SCBA	Self-Contained Breathing Apparatus
SETS	Site Enforcement Tracking System
SFPE	Society of Fire Protection Engineers
SNL	Sandia National Laboratories
TG	Time to Goal
TR	Time to Respond
UE	Undeveloped Event
UNM	University of New Mexico
VA	Vulnerability Assessment
VMD	Video Motion Detectors

Definition

The Architectural Surety℠ program at Sandia National Laboratories is a science- and engineering-based risk management approach to improving the safety, security, and reliability of the as-built environment. Surety principles, processes, and technologies developed in the nuclear weapons and national security programs are applied to the design and retrofit of buildings, facilities, and systems to achieve a level of confidence that they will perform exactly as planned under both expected and unexpected circumstances.

Intentionally Left Blank

Section 1.0

Introduction

This section provides a brief introduction to Sandia's experience in nuclear weapon surety and the application of this experience to the emerging field of infrastructure and architectural surety℠. It addresses the changing responsibilities of design and construction professionals in light of the increased public awareness of structural vulnerabilities to normal, abnormal, and malevolent threats. A brief discussion of the educational and professional outreach program initiated by Sandia National Laboratories is presented. A description of selected technologies with strong potential for application to infrastructure and architectural surety℠ issues is also presented.

1.1 Architectural Surety℠

The new and emerging threats to the infrastructure faced by today's architectural and engineering design community demand a new approach and direction. The rise of domestic terrorism, the unpredictable and uninsurable losses from earthquakes, windstorms, fire, tornadoes, hurricanes, floods, and other hazards, and the aging of public buildings combine to change the way we think about the built environment. In the wake of the World Trade Center and Oklahoma City bombings, global civil and ethnic unrest, criminal and political terrorism, and other indicators of a rapidly transforming public world, a growing awareness of vulnerability leads to increased public expectations and responsibilities for the design, engineering, and construction professionals. The destruction that follows natural disasters underscores the need for structural safety, security, and reliability to protect the public from potential injuries, death, and property loss.

These escalating risks to the public and the infrastructure change the roles of designers, architects, planners, engineers, and builders by increasing the focus on the safety, security, and reliability of the built environment. Incorporating a systematic approach to surety in the design, engineering, and construction processes and the life cycle of the as-built infrastructure systems (buildings, bridges, tunnels, dams, airports, transportation systems) can save lives and significant costs. The principles of surety also support a risk management approach to this issue, that is, the process of identifying, assessing, and mitigating risks to the public and public structures. One of the major challenges is to achieve reduced risk with little additional cost, either initially or over the project's life cycle.

Threats

Environmental threats to buildings and facilities come in three forms: normal, abnormal, and malevolent. Normal threats are those that are the usual insults to the structure and operation of a building or facility, such as aging, weathering, and other predictable, climatically related impacts. Abnormal threats include naturally occurring disasters, such as Hurricane Andrew

in 1992, the Northridge Earthquake in 1994, or the recent flooding along the Red River in North Dakota. Malevolent threats include terrorist or other deliberate, human-induced damage to structures and facilities.

1.2 Nuclear Weapons Surety at Sandia

Nuclear weapons surety includes safety, reliability, use control, and security. The President of the United States, the Department of Energy (DOE), the Department of Defense (DoD), and the national laboratories and production agencies within the Nuclear Weapon Complex (NWC) all have responsibility for nuclear weapon surety. The primary responsibility for providing nuclear weapons surety has been held by Sandia National Laboratories since the 1940s. Sandia's nuclear surety responsibilities encompass nuclear safety, security, and use control aspects of nuclear weapon systems, nuclear weapons, nuclear weapon components, nuclear devices, and their associated operations, technologies, and auxiliary equipment. Included in this responsibility is the requirement for documentation of designs, performance validation and verification, independent assessments, and relevant emergency-response information.

Discharging these responsibilities throughout the life of a nuclear weapon involves an extensive array of programs, policies, and procedures - not to mention the ongoing need to maintain and develop knowledgeable, skilled, and dedicated staff. A high degree of formality in operations and oversight is required to ensure that proper surety requirements are established and fully implemented. Knowledgeable foresight is required to anticipate and offset threats to nuclear surety.

The Surety Assessment Center at Sandia National Laboratories performs assessments of the safety, security, use control, reliability, and quality attributes of nuclear weapons and weapons systems. A core function of the center is to evaluate these attributes and ensure that Sandia appropriately addresses the surety of nuclear weapons. An important ancillary role is working with weapons designers to ensure that modern safety features are incorporated into and maintained within the stockpile for its entire life span - from concept through retirement. The Center assists Sandia design teams not only in surety disciplines, but also in the realms of statistics, human factors, test equipment, and test operations. This inclusive set of disciplines interfaces extensively with research, development, and design teams across Sandia.

With the collapse of the former Soviet Union, the end of the cold war, the ban on underground testing, and the freeze on the development of new nuclear weapons, the focus of Sandia's surety programs has shifted to stockpile stewardship. The nuclear weapons in our nation's stockpile are aging, but the surety of these weapons must not be compromised. The two national security issues that continue to make nuclear weapon surety critical are:

- The extreme consequence associated with inadvertent or unauthorized nuclear weapon explosions or radioactive material dispersal, and
- The critical need to assure and preserve the high quality and reliability of the nation's nuclear deterrent.

Safety remains paramount in stockpile stewardship. Weapon system safety principles provide predictable, safe response at all times, even during and after unpredictable events, and is achieved through a combination of design features. The nuclear explosive, detonators, and other critical components of a warhead's electrical system are contained in an exclusion region isolated from power sources by physical barriers. The transfer of energy through the barriers for normal operation is guarded by strong-link components to ensure electrical isolation in abnormal environments. Other vital components, including those that enable transfer of energy, are designed as weak links that become irreversibly inoperable in accidents well below the projected failure levels for strong-link components.

Similarly, processes associated with all phases of a weapon's life must meet the highest standards of safety. Weapon safety is a critical area that includes transportation and handling, the logistics of retirement and dismantlement, and ongoing sensitivity to environment, safety, and health issues.

With the ban on underground testing, new methods must be developed to assess weapon surety. Sandia's probabilistic risk assessment technology development efforts will improve probabilistic risk assessment of nuclear weapons subjected to normal, abnormal, and malevolent environments. The ability to identify vulnerabilities in designs and set priorities in safety technology research and development will be improved by these methods.

Weapon use control and physical security are complementary measures contributing to weapon surety. Weapon use control features and use control ancillary equipment support the national nuclear command and control system and ensure that nuclear weapons can be used only when authorized by the President of the United States. A number of Sandia projects support DoD and DOE in accordance with the national nuclear command and control system as defined in the 1987 National Security Presidential Decision Directive. Sandia is the principal laboratory supporting DOE in fulfilling these responsibilities.

Weapon security protects against unauthorized access to nuclear weapons. Security systems include sensors, alarms, communications, and penalty responses integrated into weapon transportation systems and weapon storage installations. Sandia has the responsibility for developing systems that enhance the security of weapons in DOE custody during transportation, including the transporter that will be used for transporting weapons and weapon materials. Other areas of emphasis include advanced sensors, alarms, and communications for application to DOE fixed installations or (on a reimbursable basis) to DoD for military installations and deployable site security systems. Special weapon protection projects at Sandia develop security system concepts and applications to ensure nuclear weapon security and survivability in all phases of the life cycle.

Surety technologies and principles were therefore developed at Sandia to ensure the safety, security, reliability, and quality of nuclear weapons. There is no margin for error with nuclear weapons; zero tolerance is the only acceptable approach to nuclear risk. Sandia's contribution to architectural

surety℠ is to apply, where appropriate and at appropriate levels, these proven, fail-safe surety policies and procedures to public infrastructure. The technologies and principles of the zero-tolerance nuclear weapons surety program are expensive. Identifying the cost-benefit tradeoffs is a critical part of architectural surety℠.

1.3 Architectural Surety℠ Program

Objectives

The goals of the architectural surety℠ program are to enhance public safety and security, ensure the reliability and quality of buildings and facilities, and increase public awareness of the benefits of applying surety principles to the design or retrofit of public, commercial, and private structures. The success of this program depends upon gaining a consensus within the technical and design professional communities. Developing a clear vision of the benefits of applying architectural surety℠ principles and technologies to the design and construction of buildings and structures is the first step toward achieving these goals. Identifying the needs of the design community will assist in clarifying this vision. Once identified, the surety needs of the design community must be addressed.

The development of new technologies and the adaptation of currently available technologies are ways to address these needs. The challenge is to cost-effectively adapt the surety principles developed at Sandia in the nuclear weapons program to the design of structures. Educating architects, engineers, and other design professionals through the development of new course material is also an important segment of the architectural surety℠ program. The program was intended to create a national constituency that will foster the goals of the architectural surety℠ program and lend professional and financial support where needed.

Approach

As described earlier, changes in our society are impacting the safety, security, and reliability requirements of our structures. The increases in malevolent threats such as crime, violence, and terrorist attacks have increased public awareness of the vulnerability of buildings and facilities and created new demands on the design community. The destruction wrought by natural disasters continues to menace our citizens. The national infrastructure is aging through use and normal deterioration. Further deterioration and system failures due to the advanced age of structures are inevitable. Accidents and human error also contribute to failures that threaten the as-built environment. The increased public awareness of all these threats to our constructed world has correspondingly increased the demands upon the design profession. It is a national responsibility to mitigate the risks imposed by these newly identified and recognized threats.

There are a number of steps to be taken at the onset of such an architectural surety℠ program. Forming a partnership between academia and the practicing professional community is one such step. Professional exchange at conferences is another. Assisting with the integration of performance-based concepts into the existing prescriptive building codes would be another step. This integration would require development of verification testing and

modeling analysis for new designs before implementation of new techniques and systems. This step is expected to result in the application of innovation to the design process.

Cost-benefit analyses of surety evaluation plans are expected to provide confidence in the affordability and benefits of protecting life and investment. By networking with industries and building confidence through teaming, the architectural surety℠ process will demonstrate the feasibility of designing and constructing, safe, secure, and reliable structures at a reasonable cost. Such building and facility performance enhancements are in the national interest and are expected to be routinely included in the future.

Accepting the responsibility for improving structures requires a strong commitment from the design profession. Designers who accept this responsibility for surety must think outside the box of current standards and building codes, and use intuition, passion, innovation, and creativity during the full life-cycle process of a structural system. The growth in these attributes will assist planners, designers, and builders to achieve enhanced product realization and utilization for the public good.

Surety considerations must be addressed throughout the total life cycle of structures. The design professionals must be responsible for including the other team members in planning for the safety, security, and reliability of the structure. Costs associated with this additional effort should be considered beginning with the initial project concept.

Figure 1-1 illustrates the process involved in the total life cycle of a constructed project. Surety evaluations form an integral part of each stage of a structure's life cycle. For the adequate performance of a structure, it is critically important to have addressed surety issues at the early stages and have assured implementation of derived surety plans throughout the full life of the structure, through final disposition.

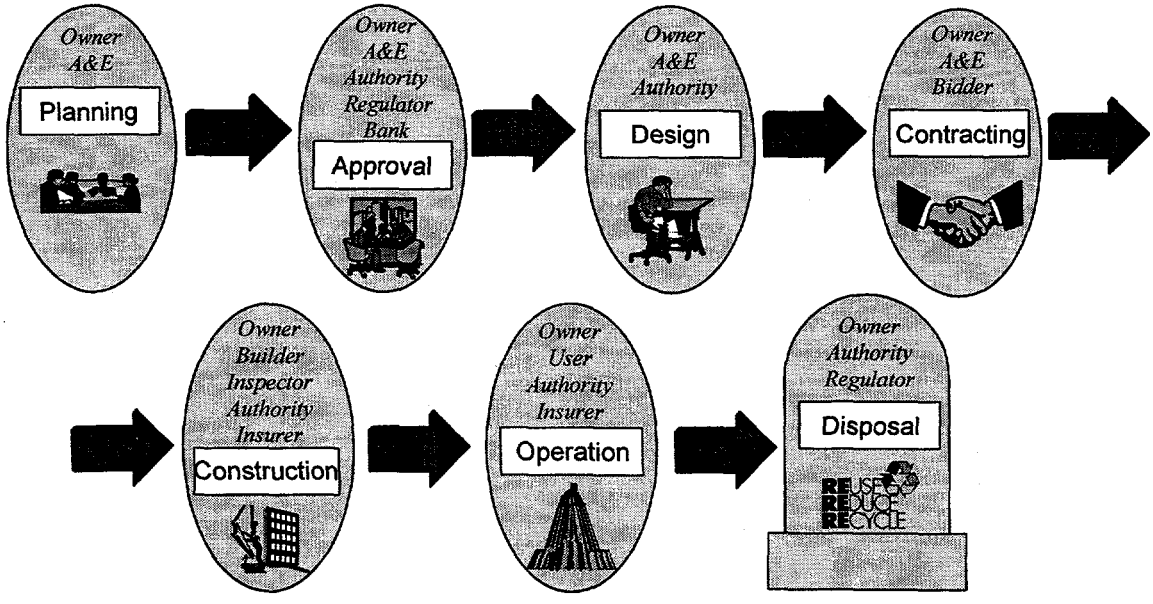


Figure 1-1. Life-Cycle Sustainable Development

Organization

The architectural surety℠ program at Sandia is organized into the following four major elements: education, research, development, and applications. These elements are defined and categorized to better provide the necessary technologies for a well-integrated approach to surety issues and needs. The combined results of work in all four elements are expected to result in (1) the evolution of training in surety principles and university curricula, (2) the demonstration of constitutive models and new materials, (3) the development of system models and computer simulation techniques, and (4) the ultimate provision of surety products to the customer for application to real-world conditions. **Figure 1-2** shows the organization of the architectural surety℠ program at Sandia. Further detail is provided throughout this section.

Education

As part of the education effort, Sandia began to consider the feasibility of applying the surety principles developed in the nuclear weapons program to the design community. A workshop was organized to solicit the input of design professionals from government, industry, and academia. This workshop, held in March 1996, served to familiarize the participants with the principles of surety and to acquaint laboratory staff with the needs and requirements of the design profession. This first professional outreach effort hosted by Sandia yielded recommendations for the direction of the program and for addressing the educational requirements of the nation in this technology area.

One of these recommendations was that Sandia develop an interdisciplinary university seminar on Architectural Surety℠. To the dual purposes of educating practicing professionals on the subject of architectural and infrastructure surety and researching the needs of the profession, Sandia presented a spring semester (January–May 1997) graduate-level civil engineering course at the University of New Mexico. Students registering for this class were eligible for graduate credit and/or professional development hours. General topics discussed in the class included:

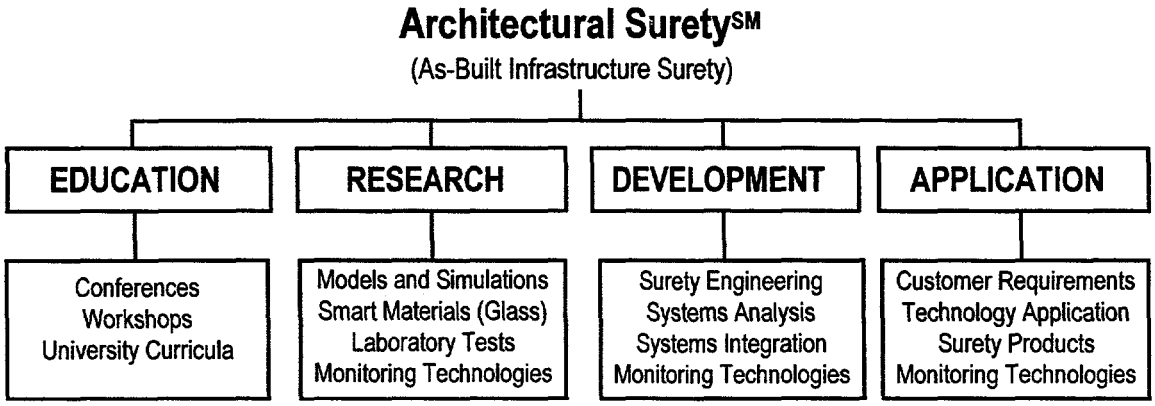


Figure 1-2. Sandia's Architectural Surety℠ Program

- Threat assessment
- Security
- Safety
- Reliability
- Risk management
- Modeling and simulation
- Project development and life-cycle engineering
- Performance codes and standards
- Ethics and legal issues
- Failure analysis and case histories

Another recommendation made at the March 1996 workshop was that Sandia host an annual or biannual international conference for design professionals on infrastructure and architectural surety℠. The exchange of information and refinement of identified needs were expected to be the driving force behind such a conference. With the co-sponsorship of the American Institute of Architects and the American Society of Civil Engineers, Sandia hosted the International Conference on Architectural Surety℠: *Assuring the Performance of Buildings and Infrastructures* in Albuquerque, New Mexico, on May 14 and 15, 1997.

Sandia engineers are working with design professionals to develop a process for determining the type and level of threat attached to particular structures. This process will assist architects, engineers, and other design professionals in designing for surety. Interactive workshops, graduate-level courses, seminars, and conferences are conducted by Sandia in conjunction with other interested professional organizations to assist in the definition of these threat parameters.

Research and Development Applications

Sandia is at the forefront of surety technology development and applications. Interaction with design professionals will enable the architectural surety℠ program at Sandia to guarantee that the surety needs of the engineering design community are met. Three obvious contributions Sandia can make to architectural surety℠ include (1) the application of currently available technologies in the national interest, (2) technology development programs to address the surety needs of structure and facility designers, and (3) implementation of developed technologies to meet building and infrastructure performance standards. Various technologies, several of which are discussed briefly below, show much promise for use in ensuring the safety, security, and reliability of the structures and facilities under design now and to be designed in the future.

Computational Simulation of Blast/Structure Interactions —These model simulations could be adapted to predict structural responses to blasts or other loads through the use of existing three-dimensional computer modeling capabilities, created for nuclear weapons development programs. Computational simulations and modeling can also be used to identify and evaluate potential new designs, building codes, and retrofits for hazard mitigation and to predict performance.

Sandia developed a computer code that evaluates the explosive conditions and couples it with the models that represent the structural and material response of buildings and structures under attack. This is done by coupling existing three-dimensional

hydrodynamic (explosive) computer codes with existing three-dimensional structural response computer codes. These coupled computer simulations of blast effects on structures and systems are to be verified through experimental test data. This can be accomplished through correlation with field test data on explosive mitigation systems such as barrier walls and enhanced multi-story structures using super-computer capabilities (Teraflops). These technologies can also be applied to dynamic structural interactions from ground motions caused by explosive blasts or earthquakes.

Window Glass Fragmentation Model—Computer simulations, models, and calculations at Sandia are being developed for modeling behavior and fracturing of window glass resulting from explosive blasts and other dynamic loads. These models will be used to predict the performance of effective glass and the applied protective and fracture mitigation measures (e.g., coatings, curtains, and lamination). This effort can ultimately provide the technical basis for glass protection standards including guidelines for anti-terrorism, public safety, and force protection applications.

The development of a glass fragmentation model that will help predict the fracturing response of window glass and the physical behavior of glass and frame assemblies to blast effects, as well as the associated human injury potential, is underway at Sandia. This will be accomplished by:

- Compiling and analyzing data from international glass breakage studies
- Extending existing capabilities in analyzing glass response (developed for nuclear weapons and adapted to modeling the effects of blast loads on window glass)
- Developing standardized test procedures and conducting tests to verify and improve window glass fragmentation and debris flow models
- Developing information for design guidelines and standards for retrofit and new projects

Instrumentation and Health Monitoring—The development of a relocatable instrument package for characterizing the environment to which a structure has been subjected and evaluating building response is a potential architectural surety℠ application of Sandia technology. This relocatable sensor package could be used at different sites to measure response of structures subjected to various threat conditions, such as blast and wind. The integrated sensor package would measure and record accelerations, strain, pressure, particle velocities, and displacements, and also provide health monitoring of structural systems throughout their life cycle. This relocatable instrument package, designed to measure dynamic blast and wind effects, could be trailer-mounted and applied for the test and evaluation of structures subjected to actual threat environments.

To develop this relocatable sensor package, Sandia can identify existing microsensors and data acquisition technologies that will best meet the needs of threat environments. A mobile monitoring system can be designed that integrates the microsensors and data acquisition technologies. A health monitoring system can be constructed and verified through testing and computer simulations. There are also many permanent sensor technologies

already developed and used by Sandia with application to structural surety.

Risk Management for Buildings and Infrastructure—Another potential application of Sandia technology to architectural surety℠ is the performance of probabilistic risk assessments (PRAs) for evaluating the effectiveness of proposed design, construction, and remediation actions upon structural response. Design professionals would be able to utilize a PRA-based methodology to uncover previously unidentified vulnerabilities and resulting consequences. This would allow them to evaluate the benefit of mitigation measures for known vulnerabilities to threat scenarios and to select alternatives that provide the most benefits.

Risk analysis studies can be accomplished by developing software that will perform risk assessments for the evaluation of explosives and other environmental threats to structures. This capability will involve adapting procedures to a known structural system, simplifying existing nuclear power plant PRA software (utilized by the NRC), incorporating existing physical protection analytical methods into simplified PRA software, and verifying methodologies with performance information.

Virtual Reality Visualization of Architectural Systems—Application of Sandia's virtual reality capabilities to architectural surety℠ would include three-dimensional, interactive visualization from three-dimensional CAD files, including simulated effects of proposed mitigation measures. This capability can permit virtual reality evaluation of anti-terrorist measures (e.g., security devices) prior to the construction or retrofit of structures. In addition, a realistic virtual environment for the planning and training of counter-terrorism activities would be a benefit to designers of vulnerable public and private buildings and facilities. This visualization capability would be useful for designers, engineers, and law enforcement, search-and-rescue, and medical first-responder personnel.

A virtual reality system will likely be based on software that creates virtual reality visualizations from three-dimensional CAD files and that evaluates security and safety measures. Existing capabilities will be expected in networked, multi-user virtual reality systems to develop interactive visualization systems. Other system capabilities include sensor and structural response visualizations and simulation models for force-on-force analysis. Virtual reality systems may also be used in finite-element analysis for structural integrity.

1.4 Documentation of Architectural Surety℠ Education

This report describes the Sandia National Laboratories' educational outreach activities in the developing field of architectural surety℠. In March 1996, Sandia hosted an Architectural Surety℠ Workshop in Albuquerque, NM, to initiate interaction with a select group of technical experts and representatives from industry, government, and academia. One of the strongest recommendations that emerged from the workshop was that Sandia conduct an experimental class in infrastructure surety to determine the applicability of Sandia's architectural surety℠ program to professional design and construction practices.

To this purpose, Sandia personnel with support from the University of New

Mexico's (UNM's) Civil Engineering (CE) Department developed and presented a graduate-level CE class in the Spring 1997 semester (January–May 1997). This course was approved by UNM to carry both graduate credit and professional development hours. Eight students, all of whom were practicing engineers or project managers, registered for and participated in the seminar-style course, and two UNM CE faculty members audited the class. The interdisciplinary and interactive approach of this course, which relied heavily on guest lecturers and student feedback, is described in this report.

Many of the lessons learned and concepts refined in the classroom were presented at the May 1997 International Conference on Architectural Surety℠: Assuring the Performance of Buildings and Infrastructures. This conference was cosponsored by Sandia, the Architectural Engineering Division of the American Society of Civil Engineers (ASCE), and the American Institute of Architects (AIA). This lively and exciting conference featured presentations by government, academic, and industry design and construction professionals during the plenary sessions and active participation during breakout sessions. New directions and national requirements were identified and discussed, and plans were made for further interaction.

The future of Sandia's architectural surety℠ program lies in continued awareness education and training, technology research and development, and applications of principles, processes, and technologies to government and industry needs. Sandia's position at the forefront of the ongoing revolution in the engineering sciences and our concern with the critical infrastructure problems facing our nation leaves Sandia uniquely qualified to serve as the leader of this architectural surety℠ program.

This report summarizes the highlights of the education component of Sandia's architectural surety℠ program. Further detail on individual lectures of the graduate level civil engineering class offered at UNM in the Spring 1997 semester is provided in the appendices. The lecture material from this pioneering class has been collected as the early draft of an architectural surety℠ textbook to be included in an educational outreach kit.

1.5 Summary

Infrastructure surety is a national concern. The concepts of architectural surety℠ are conveyed to design professionals through education, workshops, conferences, and publications. The development and application of surety technologies are a likely result of increased public and professional awareness and the development of professional networks and industrial partnerships.

The remainder of this report summarizes Sandia's educational outreach efforts in the developing field of architectural surety℠. Recommendations for evaluations of further education and training requirements are also presented.

1.6 Further Reading

Edwin K. Beauchamp and Rudolph V. Matalucci, *Dynamics of Window Glass Fracture in Explosions*, SAND98-0598. Sandia National Laboratories, Albuquerque, NM, May 1998.

A Conference on Architectural Surety℠: Assuring the Performance of Buildings

and Infrastructures Proceedings, Sandia National Laboratories, Albuquerque, NM, May 1997.

Rudolph V. Matalucci and Dominique Foley Wilson (eds.), *Architectural Surety℠ Workshop Summary Report.* Sandia National Laboratories, Albuquerque, NM, March 1996.

D. S. Preece, J. R. Weatherby, S. W. Attaway, J. W. Swegle, and R. V. Matalucci, *Computational Methods for Predicting the Response of Critical As-Build Infrastructure to Dynamic Loads (Architectural Surety℠)*, SAND98-1240. Sandia National Laboratories, Albuquerque, NM, June 1998.

Intentionally Left Blank

Section 2.0

Architectural Surety℠ Workshop

The specific objectives of the Architectural Surety℠ Workshop included:

- Identifying technical issues of national interest in architectural surety℠
- Recognizing and describing potential roadblocks (barriers to implementation)
- Developing national needs statements
- Recommending action items

This section describes the first professional outreach effort conducted by Sandia's Architectural Surety℠ Program. The Architectural Surety℠ Workshop, held at the Prairie Star Conference Center just outside Albuquerque, New Mexico, was the first exposure to surety principles for most invited participants. Under the direction of technical facilitators, the design professionals who attended the conference helped to identify the technical issues, potential roadblocks, national needs, and next steps for the architectural surety℠ program. This information was invaluable in guiding the development of the program.

2.1 Purpose

The purpose of the Architectural Surety℠ Workshop, conducted in March 1996, was to initiate interaction with a select group of technical experts from industry, government, and academia and to focus attention on the national requirements in the area of architectural surety℠. The participants were requested to give their attention to and reach consensus on architectural surety℠ issues including safety, security, reliability, and quality for the design, engineering, and construction of public buildings, facilities, and infrastructure systems.

2.2 Expectations

The workshop participants were instructed to consider normal, abnormal (natural disasters), and malevolent (terrorist attack) environment conditions as the basis for deliberations. The expectations of the workshop were that:

- An interactive group participation would evolve and lead to a prioritization of technical issues and needs at the national level
- A degree of group consensus and documentation of summary needs statements and recommended future actions would emerge
- An atmosphere of encouragement for innovative thinking "outside the box" would prevail to facilitate progress

2.3 Format

The workshop agenda was organized around a 1½-day interactive and

participative group program. The 31 participants and 10 Sandia support staff personnel were sequestered at a remote conference center. The conference format consisted of:

- One 4-hour plenary session
- One 1-hour brainstorming session
- Two 2-hour breakout sessions
- Two 1-hour summary sessions
- One 1-hour expert panel perspective session
- A wrap-up session during the second day luncheon

All information derived during the brainstorming and group breakout sessions was documented in real-time mode using a laptop database network system. This information was thus available for electronic projection during the group summary presentations.

The four breakout groups were divided into the following topical areas:

- Environment
- Engineering and construction
- Performance-based criteria
- Education and training

The participants were equally divided by their technical disciplines, expertise, and employment sectors into these four groups to ensure an appropriate balance of experience and interest in each group.

Through initial presentations by selected experts and subsequent breakout group discussions, a strawman outline of national issues, roadblocks (barriers), needs, and recommended actions was developed and summarized through facilitated group dynamics. The workshop was designed to surface national issues, problem areas, and potential conflicts, as well as to focus on the national perspective and mandate for architectural surety℠ requirements. The workshop approach was structured to emphasize which surety issues need to be addressed, what work needs to be accomplished, how the work might be pursued and effectively integrated, and how to minimize potential duplication of effort with similar ongoing activities by others (e.g., Government Services Agency, Defense Special Weapons Agency, National Science Foundation, the United Kingdom's Building Research Establishment, the Israeli International Congresses on Intelligent Buildings, and the like). The workshop participants and Sandia personnel also discussed and explored the benefits and possibilities for an International Architectural Surety℠ Conference in the future.

The breakout groups were given general instructions regarding their assigned tasks and proceeded under the guidance of a designated facilitator. The participants were left with unstructured parameters to inspire "out-of-the-box" thinking and interactions. The following guidelines and generic prompts were outlined for the facilitators of each group:

Environment

- Technical issues, needs, actions
- Definition of threats
- Risk management aspects
- National policies and/or barriers
- Public support and/or sentiments
- Information systems

Engineering and Construction

- Technical issues, needs, actions
- Processes and interfaces
- Liabilities and risks
- Schedules, budgets, profits
- CAD, shop drawings, procurement
- Environment, materials, useful life
- Quality, inspection, warranties

Performance-based Criteria

- Technical issues, needs, actions
- Guidelines, criteria, standards
- Compliance vs. performance
- Liability and litigation
- Cost effectiveness/advantages
- Implementation processes

Education and Training

- Technical issues, needs, actions
- Curriculum, degrees, departments
- Core competencies
- Approach and implementation
- Extension programs for industry
- On-the-job training
- Course outline and content

During the breakout sessions, a staff recorder provided a summary list of items raised. During the summary sessions, a spokesperson from each group presented the results. This information was used to prepare preliminary documentation of issues, roadblocks, needs, and future actions that were featured during the workshop, and was provided in hard copy form to each workshop participant.

At the conclusion of the workshop, a list of questions was given to each of the participants to determine the level of interest generated and to evaluate the overall workshop effectiveness. This survey was intended to provide guidance for future program activities.

2.4 Summary

The issues identified in the four brainstorming sessions were amorphous and vague by design. To encourage the workshop participants to range as widely as possible, the constraints on these sessions were few. The output of the brainstorming sessions, the identified issues and roadblocks, and the recommended action items are documented in the workshop summary report (SNL, 1996). The "next steps" identified by each group are briefly presented here.

The environment breakout group, which addressed both natural threats such as earthquakes and manmade threats such as bombs, recommended five action items directed toward developing a high-level, credible champion. These five "next steps" included:

- Developing a business case
- Cooperating and communicating
- Starting with government institutional support
- Hosting a technical conference
- Identifying other stakeholders for participation

The engineering and construction breakout group, which addressed both new facility and retrofit issues, identified seven recommended action items. The "next steps" from this group included:

- Introducing code changes at upper-level governing committees or agencies

- Developing and promulgating simple design guidelines, such as 3 to 5 psi blast pressure for surety considerations.
- Incorporating guidelines in codes without ignoring existing baseline codes such as security, fire, and the like
- Implementing new technologies, such as identifying and mitigating threats using probabilistic risk assessment techniques and methodologies
- Performing research and incorporating results in guidelines
- Performing research with a clear idea of goals, including research with short-term (<10 yr.) deliverables
- Establishing accountability by defining liability, enacting code enforcement, and pursuing non-limited markets

The performance-based criteria breakout group identified four "next steps" toward establishing national and international performance-based code standards that are unified and integrated. These steps included:

- Implementing continuing education and university curricula (perhaps via professional societies and groups to teach this team approach, awareness, design intent, crosstraining between the disciplines, and breaking the "cultural barrier" by assuming cross-disciplinary accountability in a systems approach)
- Demonstrating and proving this improved new paradigm
- Gaining support and endorsement from various professional societies, including AIA, ADPA, ASCE, ICBO, SFPE, DFPA, and the like
- Clarifying the applicability for performance-based codes versus prescriptive-based codes for architectural surety℠ (not necessarily an either/or situation)

The four "next step" recommendations that emerged from the education and training breakout group were all action items for Sandia, which included:

- Pilot testing an interdisciplinary class seminar and documenting who attends
- Developing a workshop for insurance companies
- Hosting courses for faculty from different universities
- Determining interest in offering classes in surety through professional associations and academic affiliations

While all of these recommended action items are the most concrete results of the workshop, the exchange of information, the contacts made, and the shared interest in developing a new paradigm are also significant outcomes. Numerous technical topics and experts in the area of architectural surety℠ were identified as potential participants and contributors for a follow-on International Architectural Surety℠ Conference. Furthermore, the noted state-of-the-art summary and status of some ongoing US and UK activities known by the workshop participants (involving industry, government agencies, national institutes, and academia) were highlighted informally during the workshop discussions. The importance of developing an architectural surety℠ network cannot be discounted.

2.5 Further Reading

Rudolph V. Matalucci and Dominique Foley Wilson (eds.), *Architectural Surety℠ Workshop Summary Report.* Sandia National Laboratories, Albuquerque, NM, March 1996.

Intentionally Left Blank

Section 3.0

Infrastructure Surety Class

The Architectural Surety℠ Workshop yielded recommendations for further action in several areas. The four "next step" recommendations from the group that addressed the education and training issues of architectural surety℠ were all action items for Sandia's program. This report discusses the activities undertaken by Sandia's architectural program in the education and training sector. The recommendations from the workshop education breakout group include:

- Pilot testing an interdisciplinary class seminar and noticing who attends
- Developing a workshop for insurance companies
- Hosting courses for faculty from different universities
- Pulsing interest in teaching classes in surety through professional associations and academic affiliations

Sandia architectural surety℠ program staff partnered with the University of New Mexico's (UNM's) Civil Engineering (CE) Department to offer a graduate-level class on Infrastructure Surety in the Spring 1997 semester (January - May 1997). Architectural and infrastructure surety is a new field of practice. The experimental class was designed to be interactive and flexible, allowing both students and instructors to discover, develop, and explore avenues of interest in the emerging subject of design surety. The course description presented to UNM for approval is presented as **Figure 3-1**.

This experimental course was approved by UNM to carry both graduate degree credit and professional development hours. The primary instructors were Rudolph V. Matalucci and Dennis S. Miyoshi of Sandia National Laboratories, who were ably guided in developing and presenting the course material by Professor Jerome Hall, the chair of UNM's CE Department and an enthusiastic workshop participant.

Eight students, all of whom were practicing engineers or project managers, registered for the seminar-style course, which met for three hours once a week during Spring 1997 semester. Two UNM CE faculty members audited the class and made valuable contributions. This section provides a brief summary of each class session. Further detail is provided in the Appendices.

The normal, abnormal, and malevolent threats to the infrastructure faced by today's civil engineers demand a new approach. In the wake of the Oklahoma City bombing, the Chunnel fire, seismic and climatic activity, global civil and ethnic unrest, criminal and political terrorism, and other indicators of a rapidly transforming public world, a growing awareness of vulnerability leads to increased expectations and responsibilities for the engineering profession. The escalating threats and risks to the public and the infrastructure change the roles of the designers, architects, planners, engineers, and builders. Incorporating surety in the engineering and construction process and the life cycle of the as-built infrastructure systems (buildings, bridges, tunnels, airports, transportation systems) can improve the safety, security, and reliability of the constructed environment. The principles of surety also serve risk management, the process of identifying, assessing, and mitigating risks.

Surety technologies and principles were developed to assure the safety, security, reliability, and quality of nuclear weapons. Nuclear surety in national security and national defense was the original total quality management program. There is no margin for error with nuclear weapons; zero tolerance is the only acceptable approach to nuclear risk. Appropriately applying these tried and true fail-safe surety policies and procedures to the constructed infrastructure is the core of this course.

The multidisciplinary approach presented in this course explores the application of surety experience and knowledge developed in the national laboratories environment to enhance the safety and security of the general public and the quality and reliability of the as-built infrastructure. Case histories, failure analyses, performance-based codes, the sustainable environment, risk management, ethics, litigation, cost-effective design, and a host of related surety issues are explored. Guest lecturers will illustrate the impact of surety issues on their particular areas of expertise. Including surety considerations at all phases of engineering and construction projects will improve the performance of the architecture and infrastructure by enabling designers, engineers, and builders to meet the challenge.

There are many other topics that will be discussed, ranging from far-reaching subjects such as human factors that impinge on surety and the changing requirements of the constructed environment to narrower, more specific items such as glass fracturing and new blast-resistant building materials. Research and development in the public and private sectors will be necessary to develop the new modeling and other tools required to incorporate surety into infrastructure planning and construction, but surety tools that engineers can use now to achieve high-quality, safe, secure, and reliable integrated designs will be presented.

Figure 3-1. Description of Proposed Infrastructure Surety Class Submitted to UNM

3.1 Introduction to Surety Principles

The first class session provided students with an introduction to the class, the instructors, and the unique role they would play as contributors to the development of the infrastructure surety body of knowledge. Students were introduced to the background, terminology, and concepts of infrastructure surety. Because this course was intentionally exploratory in nature, student participation at a high level was required.

3.1.1 *Obtain student buy-in*—The instructors were developing the course during the semester, and student feedback and suggestions would be critical in determining the approach to the course material. The course was to serve two purposes: (1) the students would be exposed to the tools and principles of surety developed in the nuclear weapons laboratories, and (2) these tools and principles would be adapted to the requirements of practicing civil engineers. Identifying the applicability of nuclear surety approaches to the design and engineering of structures would require extensive student involvement in the process. Obtaining a commitment from the students to participate actively in the goals of the class was a necessary first step.

3.1.2 *Identify the preliminary objectives of the class*—The objectives of the instructors were made clear to the students in the course description and in the introduction to the class. The students were expected to develop an understanding of surety principles and tools and assist in applying those tools and principles to civil engineering. A survey (**Figure 3-2**) completed by the

SURVEY FORM

Name: _____

Academic focus (Degree, major, concentration): _____

Special interests: _____

_____

Work history/experience: _____

_____

Significant projects: _____

_____

Class expectations: _____

_____

Figure 3-2. Survey Form to Identify Student Interests

students indicated both their backgrounds and their expectations of the course.

The results of this survey were compiled and distributed to students.

The survey showed the following group characteristics:

- All students have a full-time engineering-related job.
- All students had completed an undergraduate degree, and several have advanced degrees. Most are in Civil Engineering; Project Management and Architectural Engineering are also represented. Most concentrated in Structural work, with Risk, Transportation, and Construction Management specialties as secondary interests.
- Professional interests included structural and architectural design and construction, materials research, transportation systems, structural forensics, chaos theory, fuzzy logic, adaptive systems, infrastructure assessment, risk assessment, and environmental microscopy.
- Work experience was also broad and impressive, including commercial and public design and construction projects, concrete quality control, construction surveying, transportation projects, bridge design, explosives work, offshore oil pipeline systems, dam rehabilitation, and underwater work. Several had teaching experience.
- Projects ranged from schools, hospitals, and office buildings through head-on collision research to a new fuzzy logic textbook. Warehouses, intersections, residential subdivisions, bridges, dams, pipelines, underwater scouring systems, and materials and risk management research were also included.
- Expectations included quality and safety methods that could be economically applied to evaluate ongoing projects. Other general expectations included knowledge, references, case studies, and a new approach to research. One specific expectation was to meet the professional development hours requirement.
- Ongoing applications of surety included an interest in the new infrastructure thrust in engineering education, the special needs of underwater work and hotel building in high snow-load regions, a contract to upgrade federal facilities, traffic control and intersection design, drainage systems, research, schools and law enforcement and corrections facilities.

3.1.3 *Introduce students to the concepts of architectural and infrastructure surety*—The four significant areas of surety introduced for this course include:

- National needs
- Role of the national laboratories
- Input from industry and academia
- Motivation for teaching this course

The terminology of surety was introduced, and students were apprised of the general curriculum outline for the class.

The initial class session introduced students to the unusual expectations placed upon them to participate in this exploratory infrastructure surety course. They were asked to contribute to the emerging field, and they were surveyed to determine their interests and backgrounds. Their contributions were expected to effect the approach to the course material to be introduced.

Further detail of surety principles is provided in Appendix A.

3.2 Threats and Threat Environments

This class session was based on information developed in the Security Systems and Technology Center of Sandia National Laboratories. The presentation addressed the importance of including security planning in building design and engineering and discusses resources for determining specific threats, as well as the rationale for including the architectural client in the security planning phase.

3.2.1. *Define the criminal threat as an important factor in the planning and design of new structures or the remodel of existing structures*—While the science of physical protection has expanded as protected property has increased in value, the increasing sophistication of certain criminal elements has kept apace. The terrorist, the white-collar criminal, the hacker, and the industrial saboteur find new targets for crime in our increasingly complex world. This poses a challenge for the architect/engineer designing a security plan, who does not know the total threat or the nature of the threats to the facility or structure.

3.2.2 *Challenge the engineer and the architect to ask the appropriate questions and to require participation of the client in the planning process—thus assuring that threats to the property and the employees of the client are considered and incorporated*—A process to ensure that the security threat is completely explored and that the targets are identified should include the client and his representatives as well as the A/E staff. The formation of a threat evaluation team accomplishes several important functions, including a buy-in on the ultimate security system and a client-driven mechanism that places the requirement identification with the client. This A/E threat evaluation team would identify major security issues, define protection strategies, review and define threats versus security systems, determine impact of losses, and review the facility vulnerability assessment.

The team-generated threat assessment and the vulnerability assessment are likely to generate recommendations that the client will deem too expensive or beyond his willingness to incorporate. This decision on cost-benefit rightfully resides with the client, rather than the architect or engineer, and this process leaves the decision and the liability for that decision clearly with the client.

The architectural client understands his enterprise, his facility, his employees, and the dynamics of his business. In planning and designing a new or remodeled facility, the client must

identify, define, and communicate those factors, including security concerns, so that appropriate facility planning will be undertaken to meet the threat and frustrate potential adversaries from harming employees or damaging property. The architect or engineer must insist on the client's involvement and may have to assist the client in that task by assuring the client is able to make informed decisions.

Further detail of threats and threat environments is provided in Appendix B.

3.3 Security Concepts and Technology

This material, developed by the Security Systems and Technology Center of Sandia National Laboratories and adapted by the Architectural Surety℠ Program, was covered in two class sessions. Sandia's extensive experience in protecting nuclear weapons and nuclear weapons facilities is readily adaptable to architectural and infrastructure design applications. These lectures introduced the role that security plays in addressing the malevolent threats to structures, and how these human-induced threats may be thwarted or mitigated using security techniques.

3.3.1 *Understand the basic concepts of security*—There are two basic methods for preventing theft and sabotage. The first method involves deterring the adversary from attacking the target, such as a building, a bank vault, a computer, or a high-valve piece of equipment. This approach involves convincing the adversary that the cost of attacking the target is too high; either the task is too difficult or the likelihood of being apprehended is extremely high. This is a problematic approach, due to the difficulties of measuring system effectiveness and thus justifying the cost. The second method involves defeating an adversary attack using a physical protection system.

There are three major functions of a physical protection system ; detection, delay, and response. **Detection** is the ability of the system to notice an intrusion or other unwanted action, which is then communicated to the response force. **Delay** is the element that slows the adversary and prevents him from accomplishing his goal with the target (quickly walking away with a valuable or blowing up a bridge, for example), until the response force is able to intervene. **Response** can take the form of either a simple interruption or an actual neutralization of the adversary by an active police force.

3.3.2 *Understand the steps in designing a security system*—The design of an effective physical protection system is a cyclic process that begins with the definition of the objectives of the system. In performing this first step, the system designer must understand and characterize the facility's operations and conditions, define the threat (including the characteristics of the adversaries) to the facility, and identify the targets.

The second step is designing the system, based on the information gathered in the first step. The designed system combines such elements as fences, vaults, sensors, procedures, communication devices, and protective force personnel to achieve the protection objectives. The design should meet the these objectives within the

operational, safety, and economic constraints of the site.

The third step is analysis of the physical protection system design, checking for intrusion detection, entry control, access delay, responsive communications, protective force response, and other specialized features.

The system is then redesigned to improve weak or ineffective components. These last two steps are repeated as many times as necessary to meet protection objectives.

3.3.3 *Become familiar with the various security technologies on the market*—There are many security technologies available to support the detection, delay, and response components of physical protection. Detection technologies include exterior intrusion sensors, interior intrusion sensors, assessment tools, alarm communication and display, and entry control. Delay technologies, intended to increase the adversary task time following detection by introducing impediments along the path to the protected asset, are primarily barriers that slow the adversary and allow the response force time to arrive and react. In addition to traditional barriers, such as chain-link fences, locked doors, and grilled windows, dispensable or activated barriers can be employed to stop or delay an adversary from reaching his goal. A typical dispensable barrier system includes a way to determine activation, hardware to implement the activation decision, material that is dispensed to physically block access, hardware to dispense the material, and a protective force to respond. There are several materials, primarily foams developed by Sandia for nuclear weapon protection, that are used in dispensable barrier technologies.

This lecture described the goals and components of a physical protection system that provides detection, delay, and response features and discusses many of the technologies available to support the system. The process of incorporating these technologies into a system is an iterative process that requires complete understanding of the site and structural constraints. The appropriateness and cost-effectiveness for any particular application can vary widely.

Further detail of security concepts and technology is provided in Appendix C.

3.4 Safety Concepts and Technology

The material presented in this class session was developed by Sandia weapon safety engineers and adapted for the Architectural Surety℠ Program. The lecture addressed the importance of including safety planning in building design and engineering and proposes a systems-based process for including safety considerations in the design phase. Using a systems approach, designed-in safety can be maintained throughout the life of a structure.

3.4.1 *Learn safety vocabulary*—Safety is nested within hazards and dangers. To understand safety, a clear understanding of hazard and danger is necessary. A **hazard** is a source of danger, a chance event, or an accident. A **danger** is a liability to injury, pain, or loss. **Safety** is freedom from exposure to hazards. **Safety culture** is a paradigm for key players in a system to embed

predictable safety in an integrated fashion throughout the life cycle of the system. (For a structure, key players include A/Es, owners, fabricators, installers, tenants, maintenance crews, etc.)
Predictable safety is the capability of a system to maintain itself in a safe state during and after exposure to stress. The stress may be defined as a part of the performance requirements for the system.

3.4.2 *Recognize costs and scope of accidents*— Hazards in infrastructure can cause personal injuries. Dramatic examples include falling or being struck (as in the Kansas City walkway collapse) and radioactive contamination (as in the Chernobyl incident). Dangers other than personal injuries include loss of life (the sinking of the Titanic); loss of, or damage to, equipment (the Challenge explosion), and loss of resources (the Grand Teton dam burst, destroying arable land and killing livestock).

3.4.3 *Discover pitfalls of existing (ad hoc) approach to safety*—The current approach to safety in infrastructure design and construction is inadequate to assure safety. Weaknesses in the current approach include:

- The underlying assumption that existing codes and standards adequately cover safety
- The *ad hoc* approach to safety design that omits a safety theme
- Tacking on safety subsystems late in the process
- Lack of systematic thought about safety
- Lack of program controls or audit trails
- Oversimplification of accident causation
- The tendency to discount risk

Today's safety engineer is faced with increasing technological complexity, the increased pace of technological change (which reduces the opportunity to learn from experience), public perception and fear of risks, and increased litigation and professional liability. The protection afforded by a systematic approach to safety is an advantage to the safety engineer.

3.4.4 *Obtain benefits of a systematic approach to safety*—Ensuring safety can avoid direct high-consequence losses (such as injury), indirect high-consequence losses (such as lawsuits), and can protect the designer's reputation and livelihood. Safety is also an ethical requirement. Exposure to hazards can be prevented in three ways:

- Avoiding the hazard (using fireproof materials, for example)
- Containing the hazard (as high-voltage equipment is contained)
- Protecting personnel directly (by providing self-contained breathing apparatus, for example)

The constraints within which safety goals are implemented include:

- Meeting or exceeding codes and standards
- Meeting budget and schedule limits
- Being user-friendly
- Preserving aesthetics
- Posing acceptable risks

- Integrating with other surety and non-surety elements

3.4.5 *Learn strategies for implementing a systematic approach*—The strategies for safe design are hazard avoidance, defense in depth, and the use of redundant systems. The safety process that employs these strategies includes six critical steps:

- Determine hazards and do a risk assessment
- Craft a safety theme
- Collect design alternatives to implement the theme
- Determine metrics by performing a trade-off study to select among the alternatives
- Set up audit trail and program control
- Continue controls throughout the project life cycle

Problems to avoid in the safety process are unrealistic risk assessments and overreliance on redundancy. Risk estimation serves several important functions in safety design and implementation: failure modes can be ranked by risk and the number of accidents over the life of the system can be estimated. In addition, risk estimation can aid in deciding whether to address a particular risk or in choosing among safety alternatives.

3.4.6 *Beware of common problems in safety engineering*—Unrealistic risk assessments, over-reliance on redundancy, and excessive costs are problems to avoid. The lesson to be learned from failures of systems with unrealistic risk assessments is that failure modes should not be dismissed on a low-risk basis. Over-reliance on redundancy can be defeated by common-cause failures and a dangerous reliance on safety factors. It should be evident that the costs of not implementing safety exceed the costs of implementing safety, but trade-offs will be made. The scope of safety implementation is so large that choices will necessarily be made.

Infrastructure safety is often a small portion of the design process, and many design professionals feel that building codes should cover safety issues. *Ad hoc* designs are often implemented without consideration of safety issues. The application of a system-based process that includes safety in the design package will help to assure safety throughout the life cycle of the structure.

Further detail of safety concepts and technology is provided in Appendix D.

3.5 Reliability Concepts and Technology

This class session was based on material developed by the Center for System Reliability at Sandia National Laboratories. The Center for System Reliability is helping industry develop reliability guidelines and standards. The reliability techniques, processes, and technologies developed in Sandia's nuclear weapons laboratory have been successfully applied to private industries, such as manufacturing. These tools can be equally valuable when applied to architectural and infrastructure surety to improve the reliability of the as-built environment.

3.5.1 *Learn a reliability vocabulary*—**Reliability** is the probability that a system will

perform its intended function adequately for a specified period of time under stated conditions. Like safety, reliability is a nested definition, dependent upon an understanding of its defining terms. **Probability** describes reliability as a number between 0 and 1. **Intended function** requires a clear definition of failure. **Time** is the defined mission time over which system performance is evaluated. **Stated conditions** are the operating conditions under which reliability is valid. These terms must be specified to estimate the reliability of a system.

3.5.2 *Recognize the importance of reliability*—A 1989 MIT study showed a serious downturn in the balance of trade in some areas (cars, consumer electronics, machine tools, semiconductors, computers, copiers) over the preceding few decades because of perceived reliability issues. Reliability issues that could affect our exports exceeding our imports include:

- Reliability is an afterthought; designs are approved and accepted before reliability is considered
- American business is preoccupied with short term profits
- Maintenance and failure data tracking systems are poor.
- Customers and suppliers assume adversarial roles rather than partnering
- System analyses often fail to account for uncertainties
- Reliability focus is at the component level rather than the system level.

These reliability issues apply to building design and engineering just as well as they apply to automobile manufacturing.

3.5.3 *Obtain the benefits of a systems approach to reliability*—The primary causes of failures of complex systems are not components. Most failures result from system break-downs. A system-level focus is a critical part of a successful reliability program, and a top-down approach of a system-level focus should start very early in design. Prediction and analysis are used at every stage of design to identify problems in meeting system requirements and to fix them as early as possible.

Optimization techniques drive emphasis at the subsystem and component levels; whereas the systems approach recognizes that most reliability problems involve decision-making under uncertainty. The attributes of a system-level reliability focus that contribute to surety include:

- Emphasis on simultaneous, integrated improvements in safety, reliability, and security
- Emphasis on system-level process to include reliability in design and throughout the life of the structure
- Establishment of an organized data collection program
- Use of modeling and simulation

The earlier in the design process that reliability issues are considered, the more impact these issues can have on cost. There are particular reliability issues that should be considered very early in

the design process. Typical system reliability questions include:

- What is the best allocation to meet a system reliability objective?
- What are the relative costs and benefits of different design options?
- What is the best use for a limited test budget?
- How will warranty cost affect profitability?
- How will system reliability be affected by planned upgrades?
- What is the best spares inventory to improve availability?
- What is the best way to reduce maintenance costs?

3.5.4 *Use measures of reliability*—Most important measures of reliability are tied to measures of system performance. The most significant of these measures include Mean Time Between Failures, Mean Time to Failure, Mean Time to Repair, Availability, Failure Rate, Cost, Factor of Safety, Safety Margin, and Reliability Index. Each of these reliability measures, in combination or alone, is appropriate in particular situations.

3.5.5 *Learn elements of reliability modeling and prediction*—There are five main steps involved in analyzing system reliability:

- Establish system requirements
- Develop reliability model of system
- Populate the model with data
- Execute the model
- Analyze model results

Each of these steps involves gathering and applying information about the system under design and analysis.

3.5.6 *Recognize benefits of designing for reliability*—System reliability is improved by designing for reliability. Model analysis includes uncertainty analyses and optimization studies for design tradeoffs, which drive resource allocation decisions. Appropriate resource allocation is an integral part of reliability improvement. Tools that may be used include equal apportionment techniques, optimization techniques, the ARINC apportionment technique, the AGREE allocation method-effort minimization algorithm, and dynamic programming.

3.5.7 *Incorporate uncertainty*—Uncertainty must be considered in any reliability analysis. Dealing with uncertainty and variability is one of the most important challenges of the reliability analysis process. Failing to analyze the uncertainty of a project leads to understating or overstating reliability. Both of these inaccuracies lead to negative consequences for the project and the designer. The sources of uncertainty include:

- Variability from system to system
- Uncertainty in failure rates
- Natural (stochastic) variability in system
- Uncertainty in modeling results

Further detail of reliability concepts and technology is provided in Appendix E.

3.6 Risk Management

This class session was based on material developed by the Risk Assessment and Systems Modeling Department at Sandia National Laboratories. This department is responsible for risk assessments for commercial, defense, and space nuclear reactors. This lecture served as an introduction to the theory, tools, techniques, and actual and potential uses of risk assessment. This technology has broad application to infrastructure design.

3.6.1 *Understand basic risk concepts*—**Risk** is the frequency with which a given set of consequences would be expected to occur. In discussions of probabilistic risk assessment, risk usually refers to **consequence-weighted risk,** which is the product of an event's frequency and its consequence. Risks may be either voluntary, such as driving a car, or involuntary, such as food additives. To quantify risks, consequence measures, such as injuries or cleanup costs, must be identified. **Probabilistic risk assessment** (PRA) is the systematic process of:

- Identifying undesirable events (What is possible?)
- Estimating the frequency of such events (How likely are they?)
- Estimating the consequences of such events (What are the consequences?)

There are two important theoretical components of PRA: risk assessment and probability theory. **Risk assessment** considers the combined response of hardware, software, and humans to potential system challenges. **Probability theory** involves determining the likelihood of a particular occurrence.

3.6.2 *Learn a limited amount of probability theory*—The basic terminology of probability theory includes the following terms:

- **Sample space**: this contains all possible outcomes
- **Random variable:** a quantity with a value determined by the outcome of a probability experiment
- **Event:** any subset of the sample space
- **Complement:** all of the outcomes not contained in the event
- **Independent:** the probability of one event is not affected by the occurrence of another event
- **Dependent:** the probability of an event varies depending on the occurrence of another event
- **Mutually exclusive**: the occurrence of one event precludes the occurrence of another

3.6.3 *Discuss different risk assessment tools*—Venn diagrams are one method of describing these probability relationships. In addition to Venn diagrams, a variety of tools are available, depending on the complexity of the problem. There are simple methods, such as:

- Checklists
- Hazards analysis
- Failure modes and effects analysis

There are also more complex methods available, such as:

- Event trees
- Fault trees
- Other logic-based diagrams
  - Neural networks
  - Decision trees
  - Influence diagrams

There is no single technique that is suitable for every analysis, so the designer who is serious about risk management must be able to apply the correct tool to each problem.

3.6.4 *Understand fault tree analysis*—A **fault tree** is a diagram that graphically and logically depicts the interrelationships of elementary events that lead to an undesired event (called the "top event" of the fault tree).

The two major activities in fault tree analysis are constructing the fault tree and then evaluating it. Constructing a fault tree involves developing a graphical representation of the failure to be modeled. Special symbols are used in these fault tree models help to keep the new fault tree constructor on track. There is a well-defined thought process for constructing a fault tree, and a number of software packages are available to aid in building them.

Evaluating the fault tree involves mathematically evaluating the system to determine the primary causes of system failure. This evaluation may be quantitative or qualitative. Fault tree evaluation will include determining which events and values drive the results, which will involve evaluating the fault tree uncertainty and importance measures.

There are many types of failures that are well modeled by fault trees, including structural failure, human errors, and common-cause failure.

A handful of symbols is sufficient to build some very sophisticated fault trees.

3.6.5 *Understand quantification processes and results presentation*—The inputs to fault trees are quantified in four distinct ways: experiments, data, analysis, and expert judgment. Each of the four methods has its own shortcomings. There are many problems in interpreting experimental data; for example, problems of scale, completeness, integral and/or synergistic effects, aging effects, instrumentation errors, or atypical quality can render experimental results suspect.

In addition to the quantification of fault tree inputs, uncertainty must be considered. **Uncertainty** denotes imprecisions in the PRA analyst's knowledge or available information. Uncertainty can affect decision-making, for example when comparing two estimates. A clear explanation of the uncertainties presented is essential. Please note that properly developed uncertainty distributions are usually wider than preconceived notions would indicate.

Another factor to be considered in fault tree analysis is that of

importance calculations. Risk reduction, risk increase, uncertainty importance, and partial derivative calculations are the four groups of importance calculations.

This lecture presented an introduction to risk management that included the vocabulary and techniques of PRA. The student should come away with the critical understandings that:

- Risk is very system- and location-specific
- "Worst case" is seldom an important contributor to risk
- Contributors to risk can be isolated and importance ranked
- System insights, not just numbers, are important results
- Risk can and usually should be modeled from the top down
- Multiple failures, dependencies, and human response can dominate the risk of highly redundant systems
- Understanding uncertainty is important to risk management and decision-making

Further detail of risk management concepts and tools is provided in Appendix F.

3.7 Modeling and Simulation-Based Life-Cycle Engineering

This class session was based on material developed by the Engineering Sciences Research Foundation Programs for all Sandia National Laboratories sites. Foundation responsibilities include conducting enabling research and development in the core engineering disciplines required to revolutionize the way life-cycle engineering will be conducted. This revolution in engineering has broad application to infrastructure and architectural surety℠.

3.7.1 *Understand the engineering process*—**Engineering** is the science by which the properties of matter and the sources of energy in nature are made useful to man in structures, machines and products. 'Useful' is a value-based concept that can vary over time, across cultures, and between individuals. How engineers make things more useful is more straightforward: we apply tools and use materials. The history of engineering can be traced by identifying the tools and materials used to make things useful in particular eras. Add the defining event of that era and it will be possible to derive the values that governed the concept of 'useful' at that time. From the New Stone Age (8000 B.C.–1000 B.C.), when people evolved from nomadic hunters and gatherers to planters and the primary tools were stone-based cutters and plows for food production, to our own Space Age (1957-present), with the presence of man beyond Earth influencing the values that make spacecraft such a useful tool, engineering has served its society. The use of tools has significantly influenced the ability to meet needs in every time, in every culture, and for every individual.

Regardless of the driving event or the value-laden tool, the engineering process has remained the same: a "design, prototype, test, refine" process. Until now.

The next significant era is The Engineering Revolution (1997 - future), which is starting now. The defining tool is high-performance

computing and science. New products are generated with science-based algorithms and information. Impact: change in the way engineering decisions are made.

3.7.2 *Become familiar with modeling and simulation-based life-cycle engineering*—It will be possible to simulate the entire product life cycle. What is a life cycle? It begins with requirements, concepts, design, certification and verification, manufacturing, operations and maintenance, and finally dismantlement and disposal (cradle to grave). Products are typically exposed to different types of environments: normal (where the major issue is aging), abnormal environments due to nature (safety), and malevolent environments (requiring security from human intent). Sandia, Lockheed Martin, and the Department of Energy have the responsibility to predict how weapon systems will respond in all of these environments and across all elements of the life cycle.

Computers have been used to support this process. The Engineering Revolution flips these roles. Now we will use the computer to do simulations to refine and optimize concepts. Experiments are used to validate and create these simulations. Tests of complete products will be minimized. The ability to computationally simulate the life cycle for other high-consequence products and systems can provide an enormous competitive advantage for the nation.

3.7.3 *Become familiar with the revolution in engineering and its new tools and approaches*—Until now, engineers had to use a "design, prototype, test, refine" process. This is not evolution here, but REVOLUTION.

The maturation or coming of age of computing power and science includes full three-dimensional models, full representation of the key physical phenomena that span enormous length and time scales, and knowledge of how certain or uncertain we are of predictions. Over the last few years, computing power has increased by factors of 3000 to 5000 to reach tera (that's 10^{12} or one trillion) operations per second, the equivalent of billions of people doing hundreds of calculations each second.

This is enabling us to move toward computer simulation-based engineering decisions. Just as carpenters use a saw as a tool and wood as a material, engineers are using the teraflops computer as a tool and computational models created and validated by fundamental experiments as materials. A transformation between the real, physical world and the virtual, simulation world is necessary in order to take advantage of the power of this new computational engine. This computing engine can process fundamental and basic information such as bond breakage in steel that initiates a crack ... that results in failure of a bolt ... that affects the performance of an engine mount ... that puts abnormal thrust on an engine wing ... that ...

The simulation-based approach will provide a competitive advantage for high-value, high-consequence

products because it is better, faster, and cheaper. Benefits include:

- Decreased time-to-market
- Life-cycle design trade-offs
- Optimal designs
- Explore new, innovative concepts
- Predictive aging
- Characterize catastrophic failure conditions
- Environmentally friendly

3.7.4 *Application to infrastructure and architectural surety*℠—The current state of the U.S. infrastructure is worrisome, to say the least. Just a few examples of the problems we face include:

- 4000 commercial aircraft, 30% of which reach their 20-year design life by 2000
- 16,000 utility-scale wind turbines, with a 3-month stress equivalent to a 30-year aircraft stress
- 10,000 railroad bridges between 85 and 100 years old
- 500,000 highway bridges (200,000 deficient; 150-200 collapses each year)
- 200,000 offshore platforms in the Gulf of Mexico; scores were damaged during Hurricane Andrew
- Thousands of buildings that require inspection after every California earthquake

For success in the future, Infrastructure Surety needs as-built structures that are:

- Affordable to design, build, own, operate, and maintain
- In conformance with all regulations as well as the performance requirements of the owners and users of the structure
- Reliable, reliable, reliable
- Safe, secure, and controllable for owners and users
  - During normal environments (intended use)
  - Under abnormal environments (e.g., storms, fires, earthquakes)
  - Under hostile scenarios (e.g., terrorist threats)
- Environmentally compliant throughout the life of the structure
- Profitable when used as a business asset
- Appealing to occupants and the public

Life-cycle system engineering is the current approach to engineering design. Add modeling and simulations to this approach and a revolution in infrastructure design is underway.

Powerful computers are the most important tool available for the complex modeling and simulation required for decision-based engineering. The supercomputer developed by Intel under the direction of the Department of Energy for the Accelerated Strategic Computing Initiative (ASCI) is a valuable tool in the new engineering approach. It would take someone operating a hand-held calculator about 57,000 years to calculate a problem the teraflops computer could compute in one second. The

teraflops (so called for the nearly two trillion floating point operations per second it is capable of performing), designed to develop the higher-resolution, three-dimensional physics modeling needed to evaluate the aging nuclear stockpile without actual testing, has many other applications. The $55 million teraflops computer and its more powerful successors under the ASCI program have the potential to revolutionize computational science in many disciplines, including structural design. This computing capability is currently being used to support the safety, security, and reliability of our nation's nuclear weapon stockpile. Using it to support the safety, security, and reliability of our infrastructure is in our future.

Another use of the teraflops with even more direct application to architectural surety℠ is a blast-effects problem that examines ways to systematically implement model simulation techniques for enhancing the surety of Federal buildings and other critical infrastructure systems, with special attention to antiterrorist considerations. The goal of this program is to simulate explosive effects on a large structure, using coupled computer codes. This is an enormous computational problem that would be difficult (too time-consuming and expensive) to solve without a supercomputer.

Further detail of modeling and simulation-based engineering is provided in Appendix G.

3.8 Project Planning and Case Histories

This class session was based on material developed by the Security Systems Technology Center and the Architectural Surety℠ Program at Sandia National Laboratories. This lecture demonstrated the importance of incorporating surety concerns at the beginning of the construction life cycle. Failed structures and structural components are analyzed for information that can be used in surety planning and design.

3.8.1 *Demonstrate the need for and issues of surety planning and surety evaluation in the design, planning, and approval phases of a construction project*—Identifying risks and evaluating threats are most efficiently and cost-effectively done at the beginning of a project, as discussed in the earlier lectures. The lessons learned from the failures of the past can inform and guide engineering design judgment on the predictable threats and risks to be considered in surety planning for future projects.

3.8.2 *Examine the effects of unanticipated abnormal and malevolent threats to buildings and structures and present lessons learned that can be used in surety planning to mitigate the consequences of such threats*—Natural disasters, such as windstorms, earthquakes, and floods, present grave risks to infrastructure buildings, systems, and facilities. A few of the many examples cited during this session include:

- **Hurricane Iniki** struck Kauai in the Hawaiian Islands on September 11, 1992, destroying

90% of the island's wood-frame buildings. **Surety lesson:** Building damage was confined to those of poor design and construction. Knowledge of wind effects was incorporated in the well-engineered buildings that withstood the winds.

- When **Hurricane Andrew** pounded South Florida on August 24, 1992, 85,000 dwelling units were destroyed, leaving hundreds of thousands of people homeless. **Surety lesson:** The wind speed of Hurricane Andrew was within the design criteria of the stringent South Florida Building Code, and such massive building damage was unanticipated. There has been some controversy regarding improvements to the code and code enforcement. In either case, many buildings that were expected to withstand hurricanes did not survive Hurricane Andrew. Hurricane risks, like those from fire and earthquake, are quantifiable and controllable. Appropriate decisions with regard to siting, design, construction, and improving facilities can provide good protection from such losses.
- The **Northridge (California) Earthquake** on January 17, 1994, caused extensive and unexpected damage to steel buildings. **Surety lesson:** This earthquake yielded significant new information on the vulnerability of specific structural designs, and resulted in increasingly expensive and sometimes unavailable earthquake insurance. Higher levels of safety were expected than were actually experienced; in response, code revisions are under consideration.
- Washington's **Tacoma Narrows Bridge** ("Galloping Gertie") collapsed on November 7, 1940, a few months after completion. **Surety lesson:** This beautiful and slender suspension bridge failed after resonating in torsion for some time under wind loading. The tie-down cables and inclined stay cables did not prevent the 45° twist that occurred in the 42 mph wind. The Puget Sound valley acted as a wind tunnel that focused lateral forces on the bridge structure. The collapse of the Tacoma Narrows Bridge resulted in a five-point bridge design plan to prevent twisting:
  - "Open" stiffening trusses
  - Increased ratio of width/span
  - Increased bending stiffness of truss/girder
  - Increased dampening of structure
  - Employment of a dynamic damper to reduce resonance
- The **Kemper Arena Roof Failure** in Kansas City, Missouri on June 4, 1979 resulted in no casualties, due to serendipitous timing. The building was empty when the roof fell in, but just 24 hours earlier the $23.2 million arena was filled with thousands of people who were attending the American Institute of Architects convention. **Surety lesson:** The progressive failure was due to lack of redundancy. Rainwater accumulated on the roof during a downpour and, aggravated by two wind effects, caused a deflection in the stiff

horizontal structure, thus allowing more water to pond, and eventually causing bolts on the structure to fail from high stress.

- Another recent failure with surety implications is the **New Orleans (Louisiana) Riverwalk Barge Accident on** December 14, 1996. A barge crashed into a shopping pier thronged with tourists, Christmas shoppers, and schoolchildren on winter holiday. This accident caused minor injuries and more significant property damage. **Surety lesson:** The surety issues are primarily safety-based. The barge pilot had been involved in several accidents before. Neither the barge nor the shopping center had adequate alarm systems, so warning was haphazard. Evacuation was chaotic.
- The **Oklahoma City Federal Building bombing** on April 19, 1995, horrified America. Malevolent threats entered the public awareness in the form of domestic terrorism when 4800 pounds of explosive material concealed in a rented truck exploded 15 feet from the Alfred P. Murrah Federal Building in downtown Oklahoma City. The explosion and partial collapse of the 9-story building killed 168 people, injured hundreds more, and resulted in millions of dollars in losses. **Surety lesson:** The American Society of Civil Engineers (ASCE) and the Federal Emergency Management Agency (FEMA) offer specific recommendations for new structures and facilities based on the lessons learned from this bombing:
  - FEMA supports earthquake-resistant designs even in nonearthquake zones, as this will help protect structures against progressive collapse (from blast effects and other potential threats).
  - HUD supports reducing progressive collapse, which would isolate damage to directly affected areas.
  - Public buildings should be partially protected, and access should be controlled.
  - Compartmentalized construction is encouraged to reduce progressive collapse and isolate effects to local areas.
  - Special moment frames and dual or redundant systems would also reduce vulnerability to progressive collapse.

The cost for incorporating these recommendations into the design and construction of new buildings was estimated to increase total costs by 1 to 2 percent.

- Just over a year after the Oklahoma City Bombing, a truck bomb blasted through an eight-story apartment building at the **Khobar Towers,** an apartment complex serving American soldiers in Dhahran, Saudi Arabia. Its structural integrity after the attack is an indication of the safety features of modular components. A DSWA/WES study of the Khobar Towers made the following recommendations:
  - Terrorist threat protection is a necessary consideration, especially for buildings like the Khobar Towers that house politically vulnerable

American soldiers on foreign soil.

- Standoff distance should be increased to reduce fatalities in the event of an attack.
- Retrofit hardening should be considered, as well as hardening for new designs.
- Construction materials should be hardened.
- Camouflage, concealment, and deception can also protect soldiers and structures from malevolent attack.

Summary case histories of several noteworthy failures and an extended examination of two truck bomb attacks yield information to be considered for the surety aspects of the planning and approval phases of the construction project life cycle. The American Society of Civil Engineers (ASCE) and the Federal Emergency Management Agency (FEMA) offer specific recommendations for new structures and facilities based on the lessons learned from the Oklahoma City federal building bombing. The bombing of the USAF Khobar Tower dormitory in Saudi Arabia is used as a comparison for surety purposes. Its structural integrity after the attack is an indication of the safety features of the modular components.

Further detail of case histories is provided in Appendix H.

3.9 Engineering and Construction Issues

This class session was based on material developed by the Security Systems and Technology Center and Architectural Surety℠ Program at Sandia National Laboratories. This lecture demonstrated the importance of incorporating surety concerns at the beginning of the construction life cycle. Failed structures and structural components are analyzed for information that can be used in surety planning and design.

3.9.1 *Examination of potential engineering or construction failures*—Some areas of failure due to design errors include:

- Errors in design concept
- Lack of structural redundancy
- Failure to consider all loads
- Deficiency in connections
- Calculational errors
- Misuse of computer software
- Selection of incompatible materials or assemblies
- Failure to consider maintenance requirements or durability
- Inadequate specifications and lack of quality controls
- Unclear design intent

Failures may also occur as a result of construction errors. Some areas of failure due to construction errors include:

- Excavation accidents
- Failure of construction equipment
- Incorrect construction sequence
- Inadequate temporary support
- Premature removal of formwork and shoring
- Noncompliance with design intent

The incidence of these failures can be reduced markedly by

incorporating surety considerations into the design and construction process.

3.9.2 *Review surety requirements*—The student of infrastructure surety is required to develop a new approach to engineering and construction, which leads to new areas of consideration in the construction project life cycle. This new approach to engineering design and the incorporation of surety considerations in the construction project life cycle increases the safety, security, and reliability of the project.

3.9.3 *Review the place of surety in the construction life cycle*—In 1985 ASCE made several recommendations for reducing the severity and frequency of failures. These recommendations include:

- Improved structural integrity (ductility, continuity, redundancy)
- Certification of completed building as safe (certification of occupancy)
- Project peer review
- Definition and assignment of responsibility
- Unified risk insurance (combined risk policy)
- Better code enforcement (regulatory function)
- Discourage competitive bidding for A&E
- Improved education (disseminate failure data)
- Creation of repository for failure information
- Development of journal (case studies and failures)
- Improvement of quality assurance and control

Incorporating surety considerations into the engineering and construction project life cycle will reduce the likelihood of failures and meet many of the objectives of the ASCE recommendations.

Further detail of engineering and construction surety issues is provided in Appendix I.

3.10 Performance Codes, Standards, and Guidelines

This class session was based on information developed through the Security Systems and Technology Center and Architectural Surety℠ Program at Sandia National Laboratories. This lecture introduced performance codes and compared the traditional prescription-based codes with performance-based codes, which are developing a following in the design community. The session compared the strengths, limitations, and weaknesses of the performance-based codes with those of the prescriptive-based codes that are in use today.

3.10.1 *Become familiar with the theory of performance-based codes*—The building codes currently in use are prescriptive-based codes. **Prescriptive-based codes** are defined by the International Building Code (IBC) Performance Committee of the AIA as "Requirements which have been empirically derived utilizing the accumulated judgment of a group of experts or by actual field experience ...". This is contrasted with **performance-based codes,** defined

as "Codes which state the intended functional results and also may include the analytical tools or methodologies (standards of practice) used to demonstrate an end result as dictated by the functional statement ...".

The IBC Performance Committee recommendations for the development of performance-based codes and methods include identification of:

- Societal goals
- Functional objectives
- Performance requirements
- Verification methods
  - Deemed-to-satisfy requirements
  - Performance-based methods

Deemed-to-satisfy requirements are similar to the prescriptive codes currently in use. While they are one way to assure achievement of the specified performance objective, the prescribed, deemed-to-satisfy methods are not the only way. Alternative solutions to achieving the performance objective can be verified by a number of methods:

- Laboratory tests
- Tests in situ
- Computer modeling
- Engineering design methods
- Monitoring

Because performance-based codes will include these deemed-to-satisfy requirements and the possibility of using alternative methods of achieving the performance objectives, architects and engineers of future structures will have more design options than are currently available. Smaller projects will probably continue to use the deemed-to-satisfy prescriptive approach. However, larger and atypical projects will likely use alternative methods to satisfy performance criteria.

Performance-based codes will change the way structures are designed in several ways. The need for specialization will increase, as alternative methods for meeting the performance objectives are certain to be more creative, sophisticated, and ingenious than the standard method. In addition, verification and performance certification methods must be developed and accepted. These are likely to include peer review and third-party checking. Assignment and acceptance of liability must be decided, along with the other roles of the professionals vis-à-vis the regulators.

Fire safety is a specific area in which the application of performance-based codes has been explored in more detail.

3.10.2 *Compare prescription-based codes and performance-based codes*—The weaknesses inherent in any prescriptive code include:

- The level of safety is not identified
- The effects of the requirements are not measured
- Safety factors are not quantified
- Increased building costs result

There are also some strengths associated with prescriptive codes, which is one of the best reasons to

continue to use them. These strengths include:

- They work
- They have an established comfort level
- They require less initial effort to implement
- They are comparatively easy to enforce

Performance-based guidelines are under study and development by the building code officials and the AIA because performance-based approaches:

- Achieve specific safety goals for a specific application
- Identify safety factors employed
- Measure performance of the entire project
- Rely heavily on scientific and engineering principles
- Provide greater design flexibility
- Encourage more cost-effective solutions
- Better address complex arrangements

The strengths of performance-based approaches are formidable. These advantages include the following benefits:

- Establishes safety goals, including objectives and criteria
- Evaluates the characteristics of the people or property exposed (identify assumptions)
- Identifies potential hazards and define appropriate scenarios
- Selects suitable design tools (calculation methods, computer models, tests)
- Develops and accesses a proposed solution
- Obtains verification of proposed solution

Performance-based approaches are a developing trend. While there are significant advantages to the performance-based code over the prescriptive codes now in use, no one wants to "throw out the baby with the bath water" and lose the proven strengths of the existing approach. An amalgamated code that provides more options and alternatives, both performance-based and prescriptive, offers the best opportunity for improving the design process.

Further detail on building codes is provided in Appendix J.

3.11 Ethics, Responsibility, and Litigation

This class session was based on information assembled by the Miller, Stratvert & Torgerson law firm of Albuquerque, New Mexico. The lecture presented the changing face of professional liability and familiarized the student with the potential for legal actions resulting from surety failures. The traditional litigation issues of the design professional are introduced and the emerging professional legal issues are considered. Further discussion included the six components of professional ethics and responsibilities specified by Sandia National Laboratories for its engineers, scientists, and administrative staff.

3.11.1 *Professional liability*—Design professionals have not typically been the target of lawsuits in the past. Contractors get sued far more often than architects, engineers, or other structural designers. A

lawsuit is brought to seek legal redress when a legal duty is breached. There are two kinds of *legal duties*, contracts and a torts. A *contract* is a binding agreement. A *tort* is any legally wrongful act other than a breach of contract. Examples include defamation, personal injury, and malpractice.

Professional negligence legally exposes one to third parties, rather than just to the contractual obligor. Design professionals are subject to the **professional negligence standard,** which is a very general standard (i.e., what everyone does) that does not demand perfection.

3.11.2 *Emerging legal issues*—A new concept, the **Informed standard,** is beginning to come into play. This standard considers whether the professional has kept up with changes in the field.

Strict liability, which means liability whether or not negligent, is another legal concern for design professionals. Under strict liability, a product deemed to be unreasonably dangerous, despite reasonable care or standard behavior, may subject its manufacturer or designer to a lawsuit. The improvements in predictive and protective capabilities means that acts of God are less likely to be a legally determined precipitating event, and professional negligence is thus a more likely decision in suits involving natural disasters.

Similarly, courtroom attitudes toward **terrorists** and acts of terrorism are changing. It has become painfully clear that federal/public buildings are fair game in the guerrilla war that some radical individuals and groups are waging against the government. The changing standards make everyone responsible for protecting against both foreign and domestic terrorism.

3.11.3 *Professional ethics*—Sandia National Laboratories in its *Code of Ethics Manual* specifies six components of professional ethics and responsibilities for the engineers, scientists, and administrative staff. These components, which apply equally well to the surety engineer, are:

- Quality
- Integrity
- Leadership
- Respect for the individual
- Teamwork
- Self-assessment

Quality includes exceeding customer expectations for performance. costs, and schedule and explicitly planning for and achieving continuous improvement. **Integrity** comprises honesty, fairness, objectivity, openness, and candor. There are several significant aspects of **leadership**, including:

- Anticipating the needs of the nation
- Conveying vision
- Executing innovative and integrated solutions
- Understanding and managing risk
- Setting the standard
- Being courageous

- Being driven by the desire to be the best

Respect for the individual involves trusting and empowering the individual; benefiting from individuality; being sensitive to individual needs and aspirations; and expecting, encouraging, and rewarding accomplishments. The ethical and responsible professional manifests **teamwork** by ensuring shared values and focus, conducting internal and external teaming, and creating mutual benefits and mutual respect. ***Self-assessment*** involves two major areas: recognizing excuses and self-questioning.

The changing approach to liability evidenced in our courtrooms suggests that ethical and responsible behavior by designers committed to building surety into their structures would certainly make them less vulnerable to lawsuits based on professional negligence. It makes good professional, ethical, and legal sense for today's design professional to ensure the safety, security, and reliability of the as-built environment.

Further detail of professional ethics and liability is provided in Appendix K.

3.12 Student Projects

The term projects submitted by individual students and student teams apply the surety principles and concepts developed over the course of the semester to historical failures. These projects provided students with the opportunity to apply aggregated surety information to real-world situations. This experience equipped the student with new tools that can be brought to bear in engineering design.

This section presents summaries of the overview and recommendation sections of the project reports. The complete text of each project may be found in Appendix O.

3.12.1 *The Murrah Building Surety Assessment*

Overview—The Alfred P. Murrah Federal Building was built in Oklahoma City, Oklahoma in the mid 1970s. This building was built for the GSA Public Buildings Service. The building was designed for a nine story office building with ancillary buildings. It was located, as most federal buildings, in the downtown area. On April 19, 1995, the building was devastated by an act of terrorism. A total of 759 persons sustained injuries, 168 persons died (163 in the Murrah Building and 5 in other locations), 83 survivors were hospitalized, and 509 persons were treated as out-patients. Of those fatalities, 19 were children. This is the largest number of fatalities of any terrorist act in the United States.

Recommendations—The recommendations presented in this section are broadly based. Specific recommendations focused on just the Murrah Building are of very limited utility since there is no plan to rebuild it. The real pervasive value of performing a Surety evaluation of the Murrah Building and of the bombing is to look beyond the particular event. The recommendations derive directly from the lessons learned. Thus, there is a recommendation corresponding to each lesson learned.

- Set up a panel that will define the surety threats and that will

review and update those threats on a periodic basis.

- Institute a process in which agencies responsible for standards and specifications will review and revise them on a periodic basis.
- Institute a process for assessing existing structures in the light of new and revised threats.
- Develop a suite of facility upgrade options designed to enhance the robustness of government office facilities to surety threats.

Implementation of these recommendations will assure that surety threats are kept up to date with the evolving capabilities of terrorist organizations and other adversaries. Implementation will also provide a process to update specification, standards, etc. to reflect the changing threats and to incorporate new techniques for enhancing performance.

The last two recommendations specifically address existing facilities. Periodic assessment will assure that buildings initially deemed acceptable do not unknowingly move into the vulnerable category due to changes in the threats. The last recommendation provides a set of upgrade options that can be used as the basis for enhancing the robustness of existing buildings.

3.12.2 *The World Trade Center Bombing: A Surety Perspective*

Overview—Built in lower Manhattan in the early 1960s, the World Trade Center was designed as a focal point for foreign and domestic trade. New concepts were employed in the building. For example, the slurry wall bordering the river was the first use of this design in the United States. Building support was external to resist winds.

Although it was built when a terrorist bombing was not perceived as a threat, in the early 1970s the CIA identified the World Trade Center as a possible target due to its high public profile, its high occupancy rate, and the large number of government tenants. The World Trade Center was near the top of the CIA's list of potentially vulnerable sites for a high-value terrorist target.

The World Trade Center was the first significant U.S. terrorist bombing since the anarchist bombing on Wall Street in the 1920s. The Al-Fuqra, considered the most dangerous fundamentalist Muslim sect operating in the U.S., developed the plot to bomb New York City's World Trade Center, the United Nations headquarters, the FBI headquarters, and the Lincoln and Holland tunnels. Fortunately, the World Trade Center was the only structure that was bombed.

The terrorists created a large powerful bomb made of conventional materials. These materials were mixed into a paste, placed into plastic bags, and then packed in cardboard boxes. Blasting caps and detonators were then attached to the boxes. The boxes were loaded into a rented van, which was then parked on the 2nd parking level below the Vista Hotel within the World Trade Center. The bomb was positioned to cause maximum damage to the infrastructure of the building and

the commuter network below. The explosives were triggered from a remote site. Due to the lack of security within and around the World Trade Center, this plan was executed very easily.

Recommendations—After the bombing, the Port Authority made the World Trade Center a secured building and implemented several operational procedures that protected the structure without expensive structural work. The vital systems of the building, daily operations control and security, have been separated into different physical locations, thus allowing for greater redundancy in emergencies and decentralizing utilities and vital operations. Baffles were installed in the elevator shaft to redirect the flow of smoke or fumes. A beefed-up evacuation plan that includes battery-pack emergency lighting and photoluminescent striping for all stairwells has been implemented. All on-street parking was eliminated, and large concrete planters to both block vehicle access to the plaza and serve as potential deflecters of blasts from the street were installed.

Access to the underground parking garage was severely limited by the Port Authority. No public parking is permitted. Monthly tenant passes are issued, but background checks are required and extensive electronic and visual surveillance checks are made to match the parking permit, the vehicle, and the tenant accessing the garage.

The only weakness in the structural design, which held up very well, is the use of floor slabs to provide lateral bracing for the columns. When the floor slab is not reinforced for tension in the top of the slab and the slab receives pressure from below, it will fail. This is why the bombing caused the floor slab above ground zero to fail. Retrofitting a slab for this configuration is extremely costly, so reducing the risk of an attack is more important. The Port Authority now has a plan in place that helps reduce the possibility of a terrorist successfully planting a bomb of significant size inside the World Trade Center.

By securing the parking structure from public access and providing a buffer zone from the public streets, the Port Authority reduced both the likelihood of an attack and the consequences should one occur. In addition to the surety actions taken by the Port Authority, additional protection of the parking structure would increase the surety of the World Trade Center. While such protection might be expensive, it is the best solution to the problem of potential insider terrorist attacks.

The World Trade Center bombing was a failure as a terrorist act, because it caused surprisingly little damage and loss of life. Unfortunately, government buildings are now prominent targets. Designing surety into new buildings is an important step, but there are many existing buildings that need to be evaluated. Retrofitting existing buildings is expensive, and frequently such added protection causes aesthetic problems. It is unlikely that building owners will choose to spend additional money to make their structures look like a bunker, unless life safety and structural integrity standards are mandated by law. The enhancements made at

the World Trade Center can serve as examples that other responsible government facility owners may use to develop their surety plans.

3.12.3 *The Citicorp Center Crisis*

Overview—The architect for the Citicorp Center, built and planned in the 70s, was Hugh Stubbins and the structural engineer was Bill LeMessurier. They tried unsuccessfully to buy the old decaying church on the selected site. In order to secure the whole block, Citicorp agreed to demolish the old church building and build a new church as a freestanding part of the new center at the same corner of the block.

To provide space for the new church, the 59-story tower was set on four nine-story-high columns located at the midpoint of each side (rather than at the corners). This unusual placement of columns allowed the corners of the tower to be cantilevered out over the church and the plaza below. The structural steel frame is a tube design with lateral stability provided by six tiers of giant chevron braces on each side. A 410-ton tuned mass damper was emplaced near the top of the tower to reduce sway. The braces were designed to resist perpendicular winds, as specified in the New York City Building Code, but a question later came up about quartering winds.

Initially, the structural engineer was not worried about the effect of winds hitting from a 45°-angle because the six tiers of braces were fully fastened. The new calculations were performed to consider such quartering winds and indicated that four of the diagonals in each tier would be unstressed and the other four diagonals would be doubly loaded. The structural engineer discovered that the connections of the braces had been changed during construction from the welded connections of the design to bolted connections, which were not as secure. Adding to his concern was the discovery that the braces were designed as truss members rather than as columns, which require additional safety factors. It became clear to the structural engineer that the connections of the diagonal braces, upon which the stability of the entire structure was dependent, were very seriously underdesigned. Quartering winds would change the designed loading from 40 percent stress to 160 percent.

Recommendations—Analysis of the severe wind problems and the implications of the bombings at Oklahoma City and the Khobar Towers leads to the conclusion that there are lessons learned that could be utilized in future buildings. It is valuable to make analytical comparisons of building response when wind or blast loads are applied.

Buildings on limited sites, where standoff space is unavailable, could be designed to take advantage of standoff height. The Oklahoma City and Khobar Towers explosions have demonstrated that structural damage to the upper levels was not significant. The base structure at the Citicorp Center is approximately as high as the Murrah Federal Building at Oklahoma City, which suggests that if the base structure were hardened, the building could survive a blast without collapsing. The four support columns are the

major structural elements requiring protection.

Transferring the shear forces to the core is an interesting design concept. The trussed tube rising above the base structure could have the strength to redistribute the vertical forces in the event that one of the four supporting columns was destroyed. The four supporting columns would necessarily be very large reinforced elements with great resistance to explosions. The core, which contains the stairways, elevators, and utility chases, would be a reinforced concrete structure that, because of its locations and limited and protected openings, has great blast resistance.

The platform on which the trussed tube structure is located should be a heavy cellular reinforced concrete structure with great redundancy and resistance to the blast effects from below. The structure could be made more redundant by providing the platform with corner columns in addition to the four at each midpoint. With eight columns, the structure could be designed to survive despite the loss of two or possibly more columns.

3.12.4 *Infrastructure Surety Report on the John Hancock Mutual Life Insurance Building*

Overview—In 1967, Henry Cobb of Ieoh Ming Pei & Partners was commissioned by the John Hancock Life Insurance Company to design their new headquarters building in Boston. In August 1968, construction began on the Hancock Towers, a prominent office tower totally clad in reflective glass. Despite its problem-plagued construction period, the building has received awards from the American Institute of Architects and the Boston Society of Architects.

The 62-story steel-framed tower is totally clad with story-high panels of reflective glass. The 790-foot-tall building has an asymmetrical plan of 300 feet x 104 feet. The foundation is a reinforced concrete mat supported by steel piles driven to bedrock. The original design used 32,000 tons of structural steel, the most ever used in New England. Occupancy was three years behind schedule, and the cost ran $65 million over the original budget.

The Hancock Towers experienced failures in four major areas: (1) failure of the excavation system, (2) excessive movement due to wind, (3) discovery of a potential overturning problem in the primary structural system, and (4) dramatic failure of the glass facade. The legal settlement between John Hancock and all parties involved forbid discussions of the investigations into the failures of the Hancock Towers project. However, the construction industry grapevine has been the most fruitful source of information. Neither a prominent Boston area structural engineer nor the other regional engineers were willing to provide information on the subject.

Recommendations—Engineers should be willing to convince the public and local building departments of the value of independent peer project review of structural designs, because structural failures are some of the most disastrous consequences of human error. The loss of life, the

injuries suffered, and the cost of property damage is severe enough to warrant the design professional to change the process. However, as in the case of the Hancock Tower, the mood following the discovery of a structural problem is not conducive to a dispassionate study of the actual causes.

A few municipal building departments require the owner to pay for a review of the structural design by an independent structural engineer as part of the permit process. The building owner is usually not happy to pay for what is seen as an additional cost. There are several circumstances that can be cited where these reviews are nothing more than the reviewer filling out a standard checklist, rather than a review of the assumptions, methods, and procedures made by the designer.

A four-point program to restore concern for structural safety in current design practices was recently submitted to the ASCE *Practice Periodical on Structural Design and Construction.* The third point of the proposed program was for Uniform Building Code provisions requiring independent peer review of the structural design, drawings, and specifications submitted with the application for a building permit. These code provisions would require the owner to select a review engineer from a list approved by the building department to review the structural design to determine its compliance with the relevant provisions of the building code. The scope of the review would be custom-tailored to each project. At a minimum, the review would check the design criteria, verify the foundation design against the geotechnical report, verify the design's consistency with accepted practice, and perform calculations on representative members. Some engineers are reluctant to embrace these reviews because they feel insulted or threatened when a building department reviewer requests a copy of the structural calculations.

Designers of projects that intend to push the envelope should do research and study any pertinent technical publications to determine if the proposed system or design has a tested track record. Lastly, engineers are human and humans make mistakes, but if problems do arise, engineers should always act ethically even if it means losing a client.

3.12.5 *St. Francis Dam – A Reliability, Safety, and Security Failure: Surety Issues in Action*

Overview—Spanning the midnight hour between March 12 and March 13, 1928, St. Francis Dam, a grand achievement of the Los Angeles Bureau of Water Works and Supply, broke. It spilled 12 billion gallons of water, combined it with more than 500,000 cubic yards of landslide soil, and headed down the San Francisquito Canyon. Five and a half hours later, it reached the ocean, leaving more than 300 dead and over 100 missing (presumed dead). Strewn in its path were shocked and stumbling homeless, weeping survivors and a broken engineering career.

Recommendations—St. Francis Dam will never rest in peace. Those interested in infrastructure will

always find that we can learn more from its collapse.

Reliability—A smooth management transition and a system of peer review would have done much to improve St. Francis Dam's performance probability. Not all structures are significant enough to merit extensive review processes. The review, cost and commitment, must match the project. A large dam merits the maximum process.

The process starts with an internal house review. In a house review, a peer who was not a part of the design group would ask questions about the design approach and the information on the dam. These questions would be the least threatening in the review process and should serve to provide in-house quality control.

Outside consultants appropriate to the project become very important. St. Francis may have survived. To survive, the outside review group would have had to identify what the designers missed, the paleo-mega landslide geology. The project engineer, Mulholland, recognized its significance. If the in-house review missed it, the outside review might not have. Even if all the reviews had also failed, the water bureau would have had some relief from guilt.

Then the construction process also failed. There should have been a system that recognized significant design changes, sent them to design teams, and prompted a timely review, including a return to the outside consultants.

Safety—A communication plan would have saved lives. Complete emergency-response plans that include inundation maps, evacuation plans, and coordination with emergency services would have reduced stress on all concerned. We cannot hold 1920s Los Angeles to 1990s standards, but we can use St. Francis as a tale that motivates responsible parties today.

Security—St. Francis is an interesting exercise in the liability changes around security issues. From 1924 until it collapsed, the threat was clear. Yet no one would have then considered Los Angeles responsible for the attack if it had been caused by dynamiting. Contrast that with today. Victims of assault in hotels sue the hotel owner based on some theory of inadequate security. The recent bombing of the federal building in Oklahoma City has prompted suits based on the federal government's theoretical inability to have foreseen the assault.

Owners of public infrastructures must now consider security issues. These considerations extend beyond protection of just the asset, but also to a responsibility to protect the public and employees from being caught in the cross fire.

3.12.6 *Surety Lessons Learned From Student Projects*

The student projects uncovered the surety issues involved in these failures. The most significant surety considerations include:

- Murrah Building – This building was designed to code. The code did not address progressive collapse and was inadequate to accommodate unanticipated loads.

- World Trade Center – Its robustness due to over-design provided an extra margin of safety. Had this building been "value engineered" before construction, this extra safety margin would likely have been removed.
- Citicorp Tower – The failure to address all possible loads in the original design was exacerbated by changes during construction that were not coordinated with the designer. The mature attitude during retrofit was the reason for the smooth, cost-effective, and timely repair.
- Hancock Tower – A fragmented planning, design, and construction process, replete with uncoordinated changes, led to a seriously flawed structure.
- St. Francis Dam – A planning, design, construction process that was fragmented and lacked a method of coordinating engineering and other changes diminished the engineering integrity of the structure so seriously that it failed catastrophically.

The complete text of these projects is provided in Appendix L.

Section 4.0

International Conference

Today's engineering design and building management community face new and emerging threats to infrastructure. There is a growing awareness of public vulnerability in the wake of bomb attacks at the World Trade Center, Oklahoma City federal building, and the Khobar Towers housing complex in Saudi Arabia. El Nino, hurricanes, earthquakes, and other natural disasters are widely discussed in the media, and predictive capabilities of climatologists have improved dramatically. Our deteriorating facilities are subject to higher performance expectations now than when they were new. Approaches that are both innovative and more risk management-based are required to address these structural issues. Enhanced building and infrastructure safety, security, and reliability are required to protect the public from vulnerability to injuries, death, and property losses.

The March 1996 workshop on architectural surety℠ convened by Sandia National Laboratories to consider ways to address these problems suggested an international conference as part of the educational and professional outreach effort. To the purpose of bringing scientists, engineers, architects, insurers, lawyers, academics, city planners, and other design professionals together to exchange technical information and identify industry and technology trends, Sandia joined with two distinguished professional societies to hold the first international conference on architectural surety℠ in May 1997. Many of the issues raised and topics discussed in the pioneering Civil Engineering graduate course offered at UNM the preceding semester were further explored and refined at the conference.

4.1 Introduction

The first international conference on architectural surety℠, cosponsored by the Security Systems and Technology Center of Sandia National Laboratories, the American Institute of Architects, and the Architectural Engineering Division of the American Society of Civil Engineers, was held in Albuquerque, NM, on May 14 and 15, 1997. *Assuring the Performance of Buildings and Infrastructures: A Conference on Architectural Surety℠* provided a forum for exchanging ideas and information on capabilities that relate to the architectural surety℠ needs of global issues and national security objectives. Many federal, international, and private agencies and organizations are frequently faced with high-consequence situations with unwanted effects resulting from accidents, natural catastrophes, or malevolent human activities. The conference was intended to improve interaction among these organizations and to build on the existing broad technical experience base that has the potential to mitigate the risk of damage, injury, and loss.

Numerous technical experts from government, industry and academia were invited to present information on current national and international concerns, disaster mitigation issues,

state-of-the-art tools and capabilities, design and construction standards, and implementation plans and practices. The conference included a plenary session and two parallel breakout sessions that permitted presentations and discussions on topics concerning national requirements. Threats, analysis techniques and risk management assessment, and engineering and construction issues were the major technical areas.

4.2 Presentations

The full text of the papers presented at the conference may be found in the conference proceedings (Proceedings of *Assuring the Performance of Buildings and Infrastructures: A Conference on Architectural Surety℠*, 1997), available through Sandia National Laboratories. A summary of the presentations follows. (The invited papers presented at the conference were not reviewed or edited by the conference sponsors; the approaches and views contained therein represent those of the presenters and participants, and not necessarily those of Sandia National Laboratories or other sponsors.)

Keynote Address—"Protection of Federal Buildings in an Urban Environment" was based on information compiled by the General Services Administration's (GSA's) Office of Property Development. The GSA manages 280 million square feet of workspace in over 8000 buildings. This represents 40 percent of the federal government's office space and serves one million government employees.

While building security has always been a concern to the GSA, the April 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City caused a reevaluation of the efficacy of design standards. A report by the Department of Justice and two Executive Orders by the President in the summer of 1995 resulted in immediate action to safeguard individuals and property as well as continue operations of the federal government in the event of terrorist activity.

The keynote address discussed three aspects of building security: (1) the development of security forces and the use of surveillance systems, (2) new design criteria for new construction and major modifications, and (3) special treatment of windows to prevent or minimize the effects of flying glass.

Plenary Session—The introductory plenary session included six presentations by experts in their particular fields. An urban planner addressed infrastructure issues, an architect discussed life-cycle project planning, performance codes, and other developments, and an engineer discussed the broad problems of communication in structural design. The role of the national laboratories in architectural surety℠ was also presented.

- "Los Angeles Decaying Infrastructure" was based on information from the Bureau of Engineering of the City of Los Angeles. The City of Los Angeles encompasses 480 square miles measuring 45 miles north to south. Its infrastructure includes municipal buildings, sewers, storm drains, streets, and street lights that are all designed by the Bureau of Engineering and maintained by the Department of Public Works and the Department of General Services. The City owns 7000 parcels of land, 700 municipal

buildings, over 1000 bridges, and miles of storm drains, sewers, and streets.

Many of the City's buildings were constructed prior to 1936 and therefore are required to be seismically rehabilitated. Its major bridges, which were built through the Works Progress Administration in the 1930s, are in need of major seismic and rehabilitation work. In the past 17 years, the City has programmed over $2 billion to upgrade its sewer treatment facilities and collector system. The major sewer trunk lines were built in the early 1900s and are in need of repair. The City's streets and alleys are deteriorating at a rate that makes resurfacing the only alternative.

- "Industry Perspectives From an Architect's View" was based on information compiled by the AIA's Building Performance Center during its effort to create a performance-based International Building Code. To serve its members effectively, AIA management must constantly analyze global trends and events affecting the building industry and anticipate future developments. In addition to its work with international and performance-based codes, the AIA has addressed the facilities and infrastructure issues from a life-cycle point of view. Because capital cost is only a fraction of life-cycle cost, appropriate design can increase facility production and significantly reduce the costs of life-cycle performance. The technological advances required to employ performance-based codes and life-cycle design will require significant research and development resources. The developing partnership between academia, industry, government, and the national laboratories evidenced by this conference is an encouraging step.

- "Identifying Performance and Priorities" was based on information developed by the Architectural Engineering Division of ASCE. The presentation proposed that although our scientists know more about our environment and the extreme requirements it can place upon our structures than ever before and our designers, architects, and engineers have more and better tools for satisfying these requirements, these new tools are not well integrated into a design process. It suggested that in our effort to design and build structures that are more sophisticated and productive, we fail to ask the right questions and thus fail to apply the right answers. Better communication and information exchange between scientists, engineers, architects, and building owners can improve building performance.

- "The Role of the National Laboratories" presentation explained the strong interest in infrastructure protection held by both the Department of Energy and Sandia National Laboratories and listed the contributions to infrastructure surety that can be made by the national laboratories. These contributions include providing technology, performing vulnerability assessments, identifying connectivity among infrastructure elements and critical nodes, serving as independent, third-party, objective advisors to the government, providing liaison between industry and government,

and helping develop a national strategy for infrastructure surety.

- "Surety Principles"described the approach to nuclear weapon surety developed by Sandia National Laboratories. The presentation identified common solutions to the national security needs that are the primary mission of the national laboratories and the industry needs for architectural surety℠, as summarized in **Table 4-1**.

- "Introduction to the Architectural Surety℠ Program" summarized the emerging program area under development at Sandia National Laboratories. The Architectural Surety℠ Program addresses four major elements of technology requirements at the national level: education, research, development, and application. Architectural surety℠ involves a risk-management approach to solving problems of the as-built environment through the application of safety, security, and reliability principles developed in the nuclear weapon programs of the Department of Energy. The changing responsibilities of engineering design professionals was addressed in the light of the increased public awareness of structural ands facility systems vulnerabilities to malevolent, normal, and abnormal environment threats. A brief discussion was presented of the education and technology outreach programs initiated through a graduate-level infrastructure surety course taught in the Civil Engineering Department of the University of New Mexico and through the architectural surety℠ workshops and conferences already held and planned for the future. Also presented was a summary description of selected technologies with strong potential for application to specific national architectural and infrastructure surety concerns. These technologies include super-computational modeling and structural simulations, window glass fragmentation, risk management procedures, instrumentation and health monitoring systems, and three-dimensional computer-aided design virtual reality visualization techniques.

The presentations of the introductory plenary session illustrated the shared national requirements and concerns of the national laboratories and the design community of architects and engineers.

Breakout Sessions—The two parallel breakout sessions permitted

National Security Needs	Common Solutions	Industry Needs
Predicting and controlling failure modes	Materials research engineering simulations, physical testing	Predicting and controlling structural failures
Predicting and soft-landing for rare/high-consequence events	Engineering simulations, physical testing, systems engineering	Bounding dollar losses of rare/high-consequence events (e.g., hurricanes)
Predicting performance of new components and technologies	Materials research, advanced engineering simulations	Predicting the outcomes of performance-based building codes
Reducing costs with performance rather than prescriptives rules	Computer simulations, physical testing, systems engineering	Reducing costs with performance-based building codes

Table 4-1. Common Needs—Common Solutions

presentations and discussions on topics concerning threat analysis, analysis and risk management techniques, and engineering and construction issues.

Threat Analysis

- "The Perception of Risk," based on material developed by the Federal Emergency Management Agency, specified the responsibility of architects and engineers to use the tools of risk identification to protect American society from risk.

- "Blast Threats to Buildings and Blast Mitigation Technology" was based on material developed by the Defense Special Weapons Agency. The presentation identified the increasing blast threat to buildings and the resulting necessity for blast mitigation methods to be developed and widely applied.

- "Flood Damage, Risk, and Levees in a Changing Environment," based on material developed by the U.S. Geological Survey, discussed an analysis of the changes in flood risk due to a variety of factors. Suggestions for research to help reduce risk on floodplains were also presented.

- "Key Lessons Learned From the 1994 Northridge and 1995 Kobe Earthquakes: The Successes and Failures" was based on material developed by EQE International, Inc. The presentation summarized the effects of these earthquakes, the first truly urban events affecting large numbers of modern buildings, as yielding only one real surprise: the poor performance of certain types of steel-frame buildings. It noted that many modern designs have become more vulnerable because of "cost optimization."

- "Anticipating Fire: A Sociotechnical Approach to Mitigation" was based on a study conducted at the University of Pittsburgh. Through a review of the 1995 Kobe fire that followed an earthquake and the 1991 firestorm that engulfed the Oakland/Berkeley Hills, the presentation showed that fire is a complex, dynamic phenomenon in which small differences in initial conditions lead to large differences in outcome. Designing structures to reduce risk of fire and to facilitate rapid intervention in the event of a fire are critical elements in a risk-mitigation strategy.

- "Issues in Civil Infrastructure Systems Engineering" was based on information developed by the University of Cincinnati's Infrastructure Research Institute. This presentation showed the necessity for integrative, interdisciplinary, and multi-institutional research and technology development, conducted by university-government-industry partnerships, to develop the innovations required to sustain civil infrastructure systems.

Analysis Techniques and Risk Management Assessment

- "Architectural Design for Reliability" was based on information developed by Sandia National Laboratories. Design-for-reliability concepts can be applied to the construction industry, which includes buildings, bridges, transportation systems, dams, and other structures. The application of a systems approach to designing in reliability emphasizes the

importance of incorporating uncertainty in the analyses, the benefits of optimization analyses, and the importance of integrating safety, security, and reliability.

- "Probabilistic Analysis of Structural Safety" was a demonstration based on risk assessment methods used at Sandia National Laboratories

- "An Industrial Insurer's Approach to Risk Management," based on information developed by Factory Mutual Research Corporation, included a discussion of a highly protected risk approach, worldwide field operations, and supporting operations.

- "New Technologies Ensure Structural Safety," based on material developed by the Hart Consultant Group, provided an introduction to recent advances in the development of reliability-based design. Base isolation and viscous dampers were discussed.

- "Design Professionals, Litigation, and Architectural Surety℠" was based on material developed by the Miller, Stratvert, Torgerson & Schlenker law firm. The presentation summarized various approaches to defining the legal duties of design professionals (architects and engineers) and discussed how courts might view issues of design failure resulting from natural disasters or terrorist attacks. The legal implications, including liability issues, of performance-based codes were also considered.

- "Risk Factors and the Performance of Constructed Facilities" discussed technical risk factors including design issues such as form, function, location, and access, natural and anthropogenic loadings, analytical techniques for modeling and computation and determining prudent margins of safety, and construction and durability issues that encompass materials, fabrication processes, and overall quality. The presentation suggested an integrated facility delivery process to ensure that all technical risk factors are included in an overall risk management strategy.

- "Risk Management for Buildings—Has the Time Come?" was based on material developed at Sandia National Laboratories. This presentation discusses both incentives and challenges for applying risk management procedures to buildings and other structures. It concluded that a formal risk-management approach, including probabilistic risk assessment methods, to help identify dominant risks to public health, safety, and security and to help manage these risks in a cost-effective manner, is inappropriate for certain types of buildings.

- "The Status of the Property Insurance Industry," based on information compiled by USAA Property & Casualty Insurance, concluded that a better built environment means less damage from catastrophes, less disruption to our economy, less loss payments for the insurance industry and thus subsequent lower insurance premiums, and less depletion of materials for rebuilding. These result in an improved life cycle of the system.

- "A Corporate Program for Earthquake Risk Management,"

based on information from EQE International, Inc., provided a description of an engineering-based risk assessment and reduction program. The key steps in a successful natural hazards risk management program are to quantify the expected losses, maintain the program, and conduct cost-benefit analyses to determine the value of loss control measures versus insurance.

- "Hazard Reduction in Structures Subjected to Explosive Threats" was based on information compiled by Weidlinger Associates. This presentation compared several of the design and analysis provisions for resisting seismic excitation with blast protection counterparts. The use of composite materials for the retrofit of structures was discussed, and the special requirements of urban structures were addressed.

- "Issues in Performance-Based Design" was based on material developed at Stanford University. The presentation included a description of the general framework for a new generation of seismic codes that are based on different performance requirements of buildings. It also identified the major components of performance-based design approaches, presented key issues that arise in the development of such codes, and drew from examples of preliminary performance-based design procedures.

- "Full-Scale Testing for Structural Safety and Assessment," based on technology developed by GA Consulting (United Kingdom), presented a case for full-scale testing of complete structures as an essential element in the search for improved economy and safety of structures. The main requirement for the future is to improve the correlation between the design models and the behavior of actual structures.

- "Vibration-Based Health Monitoring and Model Refinement of Civil Engineering Structures," based on technology developed by Los Alamos National Laboratory, discussed the study results of experimental modal analyses performed on an undamaged Interstate-40 highway bridge and immediately after each of four progressively severe damage cases inflicted in the main girder of the structure. The use of modal properties to validate computer models , the use of computer models in the damage detection process, and the lack of experimental investigation of large civil engineering structures were also addressed.

- "A Competitive Advantage for Assuring the Performance of Buildings and Critical Infrastructure," based on an engineering approach developed at Sandia National Laboratories, introduced Modeling and Simulation-Based Life-Cycle Engineering (MSBLCE), a departure from traditional prototype/test-based engineering. Full-spectrum supercomputing and a robust science and engineering technology base permit high-level modeling and simulations that enable better, faster, cheaper life-cycle engineering.

- "Guidelines for the Use of the ICC Performance Code," based on material developed by the Clark County Building Department in Las

Vegas, NV, described the background, rationale, major differences, and benefits of using a uniform international performance-based building code.

- "The Nature of Materials and Their Effective Use in Civil Engineering Structures" was based on information compiled at the University of British Columbia. The presentation explored alternatives for breaking the cycle of deterioration of existing structures. Effective ways to combine new and old materials to improve the load-carrying capacity of existing structures was also presented.

- "The Characterization of 'Non-Ideal' Explosives" was based on information compiled at New Mexico Tech. This presentation reported the preliminary findings of a program designed to document the differences between non-ideal (terrorist) explosives and ideal (military) explosives. The energy released in non-ideal explosives occurs over a longer period of time and results in a significantly different blast profile, which can result in significantly different damage effects.

- "Security System Design and Integration," outlined the security system design evaluation process used at Sandia National Laboratories. The primary steps in the process include determining the objectives of the system, designing the system, and analyzing the design. Other considerations were discussed.

Banquet Address— "The Real and Hidden Cost Benefits to the Developer, the User, and the Nation by Designing a Truly Intelligent Building" was based on information developed by Advanced Ergonomic Technologies, Ltd. (United Kingdom). Finite world resources, the real needs of the user for staff productivity, and changing legislation in the workplace are affecting the design of services in buildings. Flexibility, adaptability, and reusability are fundamental in addressing intelligent building design; the techniques already exist in most areas of construction to meet these goals. Considering life cost in design does not necessarily increase initial cost.

Further detail of these conference presentations are available in the conference proceedings (*Proceedings of Assuring the Performance of Buildings and Infrastructures: A Conference on Architectural Surety℠, May 14-15,* 1997), available through Sandia National Laboratories.

4.3 Further Reading

A Conference on Architectural Surety℠: Assuring the Performance of Buildings and Infrastructures Proceedings, Sandia National Laboratories, Albuquerque, NM, May 1997.

Section 5.0

Recommendations

Surety principles and technologies developed at Sandia National Laboratories through DOE sponsorship in the nuclear weapons program have direct application to assuring the performance of buildings and infrastructure. Adaptation of these principles and technologies to the design, engineering, and construction of buildings, facilities and infrastructure projects will benefit the nation by improving the safety, security, and reliability of the as-built environment. The vulnerability of our citizens to the normal, abnormal, and malevolent threats to our public facilities—shopping centers, office buildings, transportation systems, military facilities, sports arenas, and all the structures that comprise the infrastructure—can be reduced using such surety principles, risk management techniques, and vulnerability assessments.

The programs that develop and refine these technologies have been sequestered in the national laboratory complex. Academia has not had access to the specialized results of the nuclear weapons research and development projects, and thus the training of architects, engineers, city planners, environmental scientists, and other designers and resource managers has lacked the surety component. The particular needs for safety, security, and reliability that drive the weapons programs led to the development of a very sophisticated body of knowledge that has not been generally available in the commercial arena or the academic community.

The architectural surety℠ program at Sandia is intended to bring the results of 50 years of nuclear surety research, development, and application into wider circulation. The nation will be well served when this knowledge is made available to industry through the universities. Breakthrough technologies developed in the national laboratory complex with broad applications to the constructed environment can also be disseminated through the architectural engineering curricula. This knowledge belongs to the nation and, through a partnership of the national laboratories, industry, and academia, architectural surety℠ can benefit our society.

The infrastructure surety curriculum developed for the UNM graduate course was the first attempt to transfer surety technology to the engineering and construction arena.

To further these goals, the following tasks are required:

- Refine the current infrastructure surety curriculum to meet the requirements of the architect/engineer community. At a minimum, further development and application of risk management principles, cost-benefit analyses, decision-making procedures, contracting, planning, performance-based building code implementation, systems

approaches, and liability are necessary.

- Evaluate the applicability of surety principles to other engineering disciplines, such as architecture, mechanical, electrical, chemical, nuclear, and structural engineering. Consider both undergraduate and graduate curricula.

- Evaluate the additional benefits that might be derived from incorporating surety principles in general science and engineering program courses, including mathematics, statistics, and computational modeling.

- Develop procedures for accreditation of current infrastructure surety curriculum for civil engineering and architect/engineer programs.

- Develop a formal text for Infrastructure and Architectural Surety℠.

- Develop a syllabus for professional continuing education short courses, including a short course for the construction trades.

- Develop course presentation materials, including viewgraphs, videotapes, and computer and physical models.

- Evaluate alternative educational transfer methods, such as Internet sites and video conferencing, for appropriateness to infrastructure surety.

- Assure both that the knowledge developed at Sandia is transferred to the nation and that the requirements of the design community are met by developing a continuous conduit for information transfer.

- Evaluate the effectiveness of traditional information transfer methods, such as university programs and formal texts.

- Develop a procedure to elicit curriculum evaluation critiques from students, faculty, and university administration.

- Provide a temporary assignment system that permits Sandia staff members to participate full-time directly in a university curriculum.

These tasks are intended to put the tools and technologies of surety in the hands of the people who design and build the infrastructure of our nation. Architectural surety℠ principles can improve the safety, security, and reliability of buildings and facilities. By protecting the infrastructure from threats, the risk of loss and injury to our citizens is reduced. Transmitting the information to industry through education and surety knowledge preservation is a primary element of the architectural surety℠ program.

SAND98-2086
Unlimited Release
Printed September 1998

Appendices

Intentionally Left Blank

Appendix A

Introduction to Surety Principles

Objectives

The objectives of the initial class session presented on January 27, 1997, by the class instructors, Rudolph Matalucci and Dennis Miyoshi of Sandia National Laboratories, were to:

- Obtain student buy-in on the exploratory nature of this first-ever infrastructure surety class
- Identify the preliminary objectives of the class
- Introduce students to the concepts of architectural and infrastructure surety, including terminology

1. Introduction

Students were provided with a summary description of the class. They were informed the class would develop surety principles involving safety, surety, and reliability processes. Applications to engineering designs and construction of structural systems and other infrastructure projects and systems would be discussed. The course would present surety tools that designers can use to achieve high-quality, integrated designs. Instructors would discuss normal, abnormal, and malevolent threat conditions, including treatment of standard loads, severe wind and weather effects, earthquake motions, and explosive impacts. The course's multidisciplinary approach would explore threat assessment and risk management techniques, surety models and design approaches, performance-based building codes, professional ethics, litigation potential, protective mitigation measures, and life-cycle concepts from the perspectives of technical experts. These subject matter specialists would offer guest lectures that would explore the application of infrastructure surety techniques and technologies in their particular areas of expertise. During the course of the semester, actual failure analysis studies would be reviewed, case histories would be discussed, and group projects that explore surety issues would be presented.

A preliminary outline of class lectures (**Figure A-1**) was provided. This schedule was subject to change, depending on the availability of guest lecturers, the time constraints of the semester, and the as-yet undefined interest areas of the students.

The instructors, Rudolph Matalucci and Dennis Miyoshi of Sandia National Laboratories, informed the students of the class format and the experimental nature of the class. The class format would include:

Class Sessions	Date
Introduction to Surety Principles	January 27
Threats and Threat Environments	February 3
Security Concepts	February 10
Security Systems Technology	February 17
Safety Technology	February 24
Reliability Issues and Technology	March 3
Risk Assessment, Probability, and Liability	March 10
Spring Break	March 17 (no class)
Modeling, Simulations/Calculations, Life-Cycle Engineering, and Health Monitoring	March 24
Project Planning, Design Criteria, & Cost Trade-Offs	March 31
Engineering, Contracting, and Construction Issues	April 7
Case Histories and Failure Analyses	April 14
Performance Codes, Standards, and Guidelines (class projects)	April 21
Ethics/Responsibilities/Litigation (class projects)	April 28
Class Review of Surety Concepts and Final Projects by Students	May 5
Student Presentations and Wrap-Up	Final week

Guest lecturers from security, safety, failure analysis, construction, and similar fields will participate in this course.

Figure A-1. Preliminary Course Syllabus

- Seminar-style class meetings, with lectures, discussions, and high student participation.
- Handouts for each class that would include outlined notes and readings. (No textbooks are available in this new field, of course. This class developed its own course materials.)
- Guest speakers on special topics. All speakers would address actual, factual structural applications of the theory presented. Examples of applications would be included.
- Case histories.
- Short quizzes; no final.
- Short weekly project summaries that would apply the concepts presented in class to an ongoing or completed project with which the student is very familiar.
- Term project report.

All class meetings were videotaped, which benefited the students by allowing missed classes to be easily made up and the instructors by providing complete documentation of the course. It was emphasized to the students that because this was an experimental course, student feedback and evaluation would be critical. The flexible syllabus was designed to allow student input to be incorporated into the development of course material.

Because student feedback would be such an integral part of this class, the students were apprised of the expectations the instructors held. Students would be expected to:

- Participate actively (get involved).
- Identify surety applications.
- Read and discuss assigned material.
- Develop surety projects.
- Embrace surety principles.
- Bring ideas and articles to class.

This high level of student involvement was expected to result in enhanced surety awareness and application. The student of surety is required to think outside the box (**Figure A-2**).

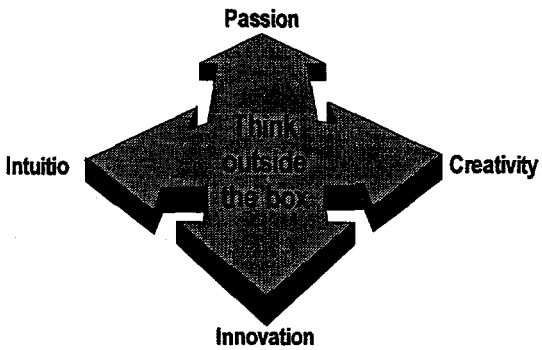


Figure A-2. Requirements for the Successful Study of Surety

In addition to this class's unusual requirement for an extremely high level of interaction, the more usual class requirements, such as attendance, assignments, tests, term papers, and other grading components, were also presented.

2. Theory and Principles

To provide the background on the evolution of this class, surety perspectives were presented. The four significant introductory areas of surety included:

- National needs—Our aging infrastructure is crumbling and vulnerable. Retrofits and new construction are inevitable. The infrastructure is subject to normal, abnormal, and malevolent threats. The critical infrastructure surety needs must be addressed.
- Role of national laboratories—Technologies currently available through the national laboratories can be used to improve the surety of our nation's infrastructure. Other technologies can be cost-effectively adapted to meet national infrastructure requirements.
- Input from industry and academia—The needs of the design community can best be identified by designers. This information will guide the way toward adapting engineering and architectural curricula to incorporate surety concerns.
- Motivation for teaching this course—This course is intended to help identify the needs of the design community, to develop an awareness of architectural surety℠ requirements, and to define the surety body of knowledge that applies to public safety and security.

Students were introduced to the following basic terminology of architectural surety℠, as it will be used in this class.

Infrastructure

- An underlying foundation or basic framework (*Webster*).
- The basic facilities, equipment, services, and installation needed for the growth and functioning of a country, community, or organization (*American Heritage*).
- From *Measuring and Improving Infrastructure Performance* by the National Research Council: generally used in this report to refer to facilities and their operations and the operation and management institutions that provide water, remove waste, facilitate movement of people and goods, and otherwise serve and support other economic and social activity or protect and enhance environmental quality.
- A diverse collection of constructed facilities, public and private, and associated services, ranging from airports to energy supply to landfills to wastewater treatment.
- From *Toward Infrastructure Improvement* by the National Research Council: an earlier NRC committee (1987) wrote that infrastructure includes both specific functional modes—highways, streets, roads, and bridges; mass transit; airports and airways; water supply and water resources; wastewater management; solid-waste treatment and disposal; electric power generation and transmission; telecommunications; and

hazardous waste management practices—and the combined system these modal elements comprise. A comprehension of infrastructure spans not only these public works facilities, but also the operating procedures, management practices, and development policies that interact together with societal demand and the physical world to facilitate the transport of people and goods, provision of water for drinking and a variety of other uses, safe disposal of society's waste products, provisions of energy where it is needed, and transmission of information within and between communities.

To these previously cited modes may be added public buildings—schools, health care facilities, government offices, and the like—that are linked by the functional systems they house to provide important public services, in much the same fashion as highways and water supply facilities.

Surety

- Something beyond doubt; a certainty (*American Heritage*).
- A pledge or formal promise made to secure against loss, damage, or default; a guarantee or security (*Webster*).
- Nuclear weapons safety, security, reliability, and control (Sandia)
- The level of confidence that exists in the appropriate performance of nuclear weapons, and their safety, security, and reliability in all environments (Sandia)
- Class definition: 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**. Infrastructure surety is a **risk management** approach to providing confidence that structures and facilities will perform in acceptable ways when subjected to threat environments:
  - normal
  - abnormal
  - malevolent

Threats

- Indications of impending danger or harm (*American Heritage*).
- People, things, or ideas regarded as possible dangers; menaces (*Webster*).

Security

- Freedom from risk or danger; safety (*American Heritage*).

Safety

- Freedom from danger, risk, or injury (*American Heritage*).
- Dependability (*American Heritage*).
- From *Measuring and Improving Infrastructure Performance* by the National Research Council: a component of performance; the likelihood that infrastructure effectiveness will be maintained over an extended period of time; the probability that service will be available at least at specified levels throughout the design lifetime of the infrastructure system.

Risk

- A factor, element, or course involving uncertain danger; hazard (*American Heritage*).

- The possibility of suffering harm or loss; danger (*Webster*).

Probabilistic Risk Assessment

- The combination of probability theory and risk assessment.

Performance-based codes

- Performance—the way in which someone or something functions (*American Heritage*).

3. Applications

Now that infrastructure surety has been defined, the challenge becomes identifying and addressing infrastructure surety issues or problems. Some of the most pressing concerns in the fields of design and construction are surety issues, including:

- Crime and violence
- Terrorism and malevolence
- Natural disasters
- System failures
- Aging and deterioration
- Accidents

There are several ways infrastructure surety principles address these problems. The results of applying infrastructure security principles are to:

- Enhance safety, security, and reliability
- Increase public awareness
- Gain technical consensus
- Create constituency
- Impact education and industry

How are architectural surety℠ principles applied? How are the concepts presented to the design community? There are a number of ways to introduce the concepts of infrastructure surety to the design community and to apply surety principles in structural designs, including:

- Forming partnerships of academics and professionals
- Exchanging information at conferences
- Integrating building codes
  - verification testing
  - innovation implementation
- Making cost comparisons
- Networking with construction and insurance industries
- Teaching, evaluating, iterating

Surety principles are applicable in almost all phases of the construction life cycle. (See **Figures A-3** and **A-4**.) This course describes surety principles and applications during project life cycles. Surety evaluations are important in all stages of a project and must be addressed to ensure appropriate implementation. **Figure A-4** indicates a select number of components associated with the stages of a project life cycle.

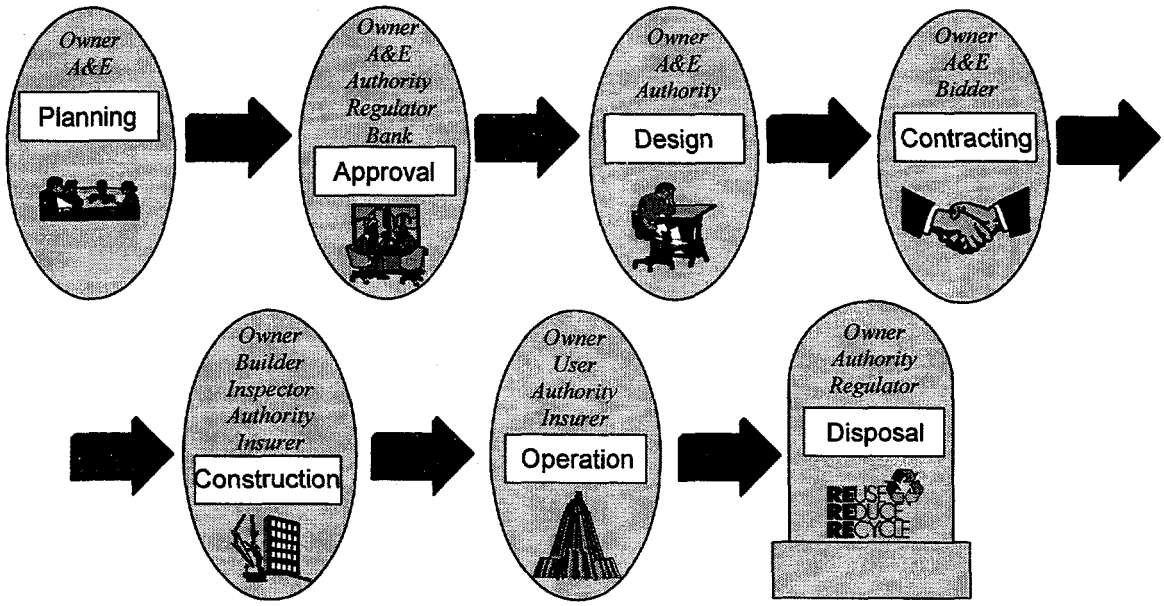


Figure A-3. Construction Project Life Cycle

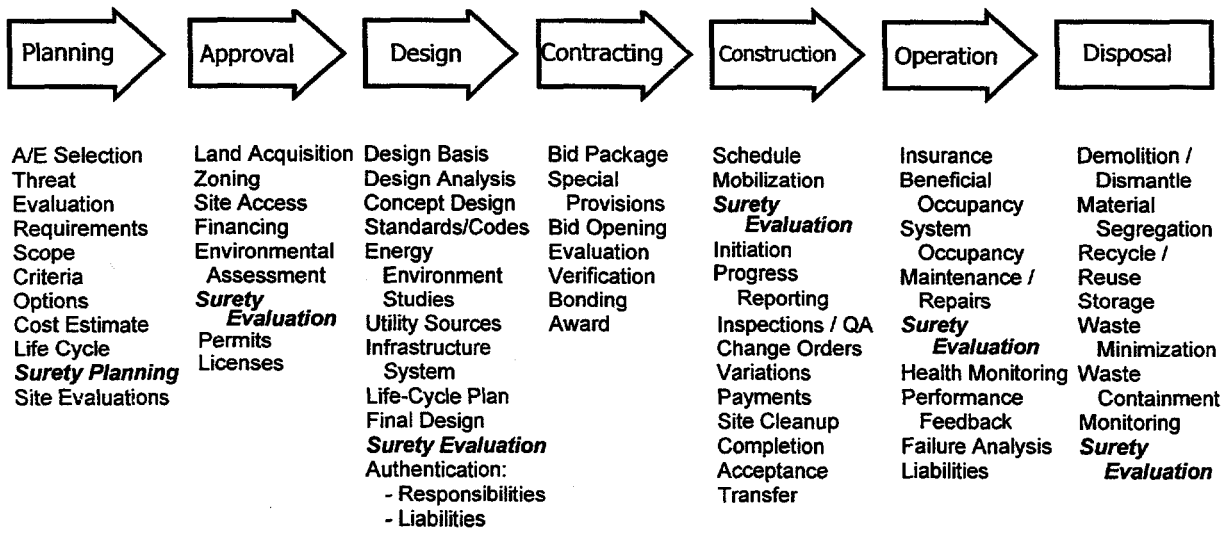


Figure A-4. Components of Construction Project Life Cycle Phases

4. Summary

The application of surety principles throughout the entire life-cycle process of an infrastructure project is the challenge for architects and engineers today. It is important that surety elements are addressed during each phase of a project so that ultimately the owner, user, and the public can experience the benefits derived from the incorporation of safety, security, and reliability measures. Engineers and architects alike must first recognize the natural and man-imposed threats to which infrastructures projects are exposed. They must then join in partnership with the owners and builders to provide the required physical protection and performance against malevolent attacks, against the destructive forces imposed by natural disasters, and against the aging and deterioration process caused by normal use and continuous exposure to stress and weathering. Although there are currently no accepted building standards and guidelines that address surety issues, as the public becomes more concerned about failures that result from inadequate codes and standards, the design and construction profession can expect to provide the user of these systems more confidence of performance under all conditions. It is important for the educational institutions to become aware of this need and make their contribution to society and to the building industry through research and appropriate curricula.

5. Further Reading

Bombproofing Embassies Is a Delicate Protocol, *The Wall Street Journal,* August 1, 1996, Sec. B, p. B1.

Martin J. Fertal, Designs for Blast Protection, in *Civil Engineering,* pp. 3A-5A, September 1996.

Al Grant, Civil Infrastructure Systems: The Big Picture, in *Journal of Infrastructure Systems,* vol. 1, no. 2, June 1995.

Eve E. Hinman, Defensive Architecture, in *Skylines,* pp. 14-16, May 1995.

Andrew C. Lemer, Ken P. Chong, and Mehmet T. Tumay, Research As a Means for Improving Infrastructure, in *Journal of Infrastructure Systems,* vol. 1, no. 1, March 1995.

National Research Council, Commission on Engineering and Technical Systems, Building Research Board, Committee on Infrastructure, Executive Summary, in *In Our Own Backyard: Principles for Effective Improvement of the Nation's Infrastructure,* Albert A. Grant and Andrew C. Lemer, (eds.). National Academy Press, Washington, D.C., 1993.

D. A. Stolovitch, Drawing Security Into Building Design, in *Security Management,* pp. 69-75, December 1995.

Richard N. Wright, National Goals for Construction Technology, in *Journal of Infrastructure Systems,* vol. 1, no. 4, December 1995.

Appendix B

Threats and Threat Environments

Objectives

The objectives of this class lecture, presented by Joel Carlson of Sandia National Laboratories, former Federal Bureau of Investigation Special Agent, on February 3, 1997, are to:

- Define the criminal threat as an important factor in the planning and design of new structures or the remodel of existing structures.
- Challenge the engineer and the architect to ask the appropriate questions and to require participation of the client in the planning process thus assuring that threats to the property and the employees of the client are considered and incorporated.

The architectural client knows best his enterprise, his facility, his employees, and the dynamics of his business. In planning and designing a new or remodeled facility, the client must identify, define, and communicate those factors to include security concerns, so that appropriate facility planning will be undertaken to meet the threat and frustrate potential adversaries from harming employees or damaging property. The architect or engineer must insist on the client's involvement and may have to assist the client in that task.

1. Introduction

The science of physical protection has expanded in scope over the years as protected property has increased in value and as the criminal element has gained in sophistication. Business enterprises in our current world are complex, their interrelationships are competitive, their communications have exponentially expanded, the supportive politics has moved from local to international, and technology is the essence of their existence. All of that dynamism has brought forth criminals who have grown to meet the new challenges of the new world, i.e., the terrorist, the white collar criminal, the hacker, the industrial espionage agent.

What does all that have to do with meeting the architectural and engineering needs of a client? From a security perspective, it poses a challenge of defining the changing needs and meeting them in the design and construction of facilities to house, accommodate, and protect the enterprises, to include the complex facilities that serve them and a highly skilled labor force that activates and sustains this new world.

2. Theory and Principles

So you are the architect/engineer who has been hired to design an office building that will house an insurance company with all of its executive and operational elements. Beyond the foundation and the walls and the roof, what threats should you and the client consider in the planning effort? The textbook tells us that to understand what we are to protect and from whom, we must define the threat and identify the targets. Threats to an insurance company? What would they be? There are competitors who would like to know insider information, such as rate schedules, client lists, and new product specifications. There are external threats such as gangs who might like to vandalize the outside of the building. There are thieves who might like to break into employee vehicles in the parking lot. There are computer hackers who would delight in modifying company records remotely or onsite. There may be criminals in the community who would look to breaking into the building to steal equipment, attacking women employees in the parking lot, or protesting the fact the company has invested in third-world countries or corporations with adverse political interpretation.

As the architect/engineer, you don't know what the total threat is to your client unless you do some research and convince that client to help you in that endeavor. Where do you start? Have a meeting with the client early in your relationship and outline the concern you have for helping to design a building or a remodel that is not only functional, but will provide a tailored response to the environment wherein the facility is placed. If the building is to be in a gang infested area, who are they and what is their history? If there has been a history of disgruntled employees in the company, is access control to the new work areas important to the client? If there are a lot of company trade secrets or privileged information in the company's operation, how do we want to protect it, shielded cabling, limited access areas, vaults? If the company has employees on shifts, should we consider guard houses, closed circuit television in the parking areas, enhanced lot lighting, or other physical security installations? The meetings with the client to talk about security in the new facility will save him grief and heartache and will permit you to meet those challenges in your initial design rather than in a "change order" later in the process.

A process to ensure that the security threat is completely explored and that the targets are identified should include the client and his employees as well as you and your staff. How do you convince the client to take an active role in threat prediction? Perhaps the most important approach is to convey the fact that his customers and his employees will judge his enterprise by the way it treats or accommodates people. Safety and security are important to the people with whom his enterprise interacts in business dealings. Employee safety and security in the workplace, document security of customers' private information, and security of work products are vital to the credibility of the enterprise. You must convey this thought and incorporate it into your service to the client.

The Loyola College Center for Social Research recently conducted research on how safety and security impact the attitudes of people. The study focused on mall customers and showed that 9% of shoppers avoid malls for security reasons, 19% avoid strip malls for

security reasons, 1/3 of respondents avoid strip malls for safety reasons, 91% considered the presence of security guards a significant safety factor, and only 30% believed parking lot security adequate. Obviously, if you are designing a shopping mall, this study should provide you and your client some guidance on design.

If you are designing a federal office building, the Murrah Building experience should provide guidance; if you are designing a facility for the Internal Revenue Service, militant anti-IRS groups should factor into your planning; if you are designing a plant for production of micro chips, the theft problem or the commercial espionage experience of your client or even of his competitors would bear examination; if you are designing a post office building, the experiences of distraught and violent attacks by employees or former employees should be examined, etc. You may have to take the lead in researching and locating studies that pertain to your project. Your work product will be better for the effort you and your client spend on incorporating the security and safety experiences of others.

An approach that you might suggest to your client is for the client enterprise to form an evaluation A/E team with representatives from security, plant operations, process operations, engineering, financial operations, personnel management, etc., for the purpose of formulating recommendations regarding safety and security based on past experience and future projection. The forming of such an A/E team accomplishes several important functions, including a buy-in of the ultimate security systems of the new facility by the employees, and a client-driven requirements mechanism that lessens your research effort and places the responsibility for requirement identification with the client. This A/E team would have the responsibility for identifying major security issues, defining protection strategies, reviewing and defining threats vs. security systems, determining potential impact of loss in each area of the client enterprise, informing the client management of the issues identified and recommendations, and reviewing a vulnerability assessment of the facility.

Some of the factors that the A/E team might explore would include:

- The classes of possible adversaries, i.e., outsiders, insiders, or outsiders in collusion with insiders
- The breadth of possible adversarial tactics, i.e., stealth, force, deceit
- The capabilities of the adversary, i.e., knowledge, skills, motivation, weapons and tools

Further, the A/E team should characterize the projected facility against the profile of the potential security threats. This would include an assessment of site boundaries, buildings, access points, room locations, communication conveyances internal and external to the facility, process within the facility, employee accommodations, existing physical protection features, process locations in facility, and other experiences of this client, his past facilities, and his competitors.

A vulnerability assessment (VA) can also be conducted by the A/E team with the help of contractors who are experienced with such studies. The VA would incorporate the A/E team's study of threat and would additionally define the company's security interests, identify consequences of

adversarial action, characterize protection schemes, describe the adversaries based on community profile and the threat assessment, analyze current and projected security systems effectiveness based on legal and technical experience, and conduct a cost benefit analysis of what should be incorporated in the facility you are designing. Obviously, the A/E team-generated threat assessment and the vulnerability assessment would provide you and your client important data to incorporate into the design of the facility. It also will identify possible security incorporations that the client will declare too expensive or beyond his willingness to install in the facility. This client decision will alleviate future responsibility and "finger pointing" at you as the architect or engineer for security or safety failures that could have been avoided "if they had been incorporated in the building design."

An interesting and sometimes debated process of marriage between the security and design interests can be found in the Crime Prevention Through Environmental Design (CPTED) Program actively instituted in Canada and being utilized widely in the United States. This program provides the facility owner with law enforcement/crime prevention personnel and security professionals to study crime problems in private or public facilities, with recommendations for remedial actions related to those problems and for facility remodel or revamp to alleviate the security problems identified. Remedies under this program might include building wall dividers in hallways to channel foot traffic and thus prevent overcrowding and resultant rowdiness, pocketpicking, and vandalism; replacement of shrubbery outside buildings with patios, rockeries, or other attractive landscaping to alleviate assault, thievery, vandalism, or burglary; and the reemplacement of driveways with landscaped mound separators to avoid drive-through lanes, obscured parking areas, and overgrown parking lot perimeters that promote theft, assault, or rape.

These cooperative security studies are conducted after the fact of crime commission, but are useful in alleviating reoccurrence of crime in existing facilities. Some police agencies, as part of their crime prevention programs, offer services to prospective enterprises in their community in the planning of facilities that are resistant to the crime known to the police. Such surveys are conducted by the crime prevention officer and could be useful to you as an adjunct to the input you receive from the client and his employees.

Where do you or the client obtain the information you need to make a meaningful assessment of the security problems you face in building or remodeling a facility? There are a number of sources that will provide information on specialized security measures and equipment, on community crime statistics, on studies of groups and gangs, on commercial or international espionage, on terrorist and domestic dissident groups, and on various other specialized security related concerns. There is no one place where you will get everything you need to make your assessment of security requirements for a particular facility.

Some of the obvious sources of information will include the local, county, and state law enforcement agencies. Some national sources might include the Uniform Crime Reports of the Federal Bureau of investigation (FBI), specialized crime studies available through the National Crime

Justice Reference Service (NCJRS), and specialized studies of non-governmental groups that can be identified through the library, Internet, or private associations such as the American Society for Industrial Security. These resources are replete and are important factors in bringing to your client the information he or she needs in developing a facility that will not only meet the business needs of the enterprise but will predict and address security challenges that are increasingly a factor in our day-to-day lives.

3. Applications

This section will present examples of your work/ideas/expertise in the "real world." Practical uses of your subject matter will probably include a discussion of the benefits, cost-effectiveness, and tradeoffs involved in applying the principles and theories to actual projects. This is also an appropriate place to discuss "lessons learned" from case histories of failures and to build scenarios. (What if the Murrah Building had a setback like the Khobar Towers? What if A/E contracts contained a clause holding the A/E responsible for operations phase facility problems?)

4. Summary

You, as the architect or engineer of a new facility or of the remodel of an existing facility, have an important responsibility to help the client identify and address the needs that must be incorporated into the project. You surely have the training and experience to address the adequacy of the air conditioning system to provide sufficient cooling to accommodate employee comfort, or the parking lot capacity and traffic flow design for anticipated customer and employee vehicles, or the wiring and cabling for telecommunications. You realize that our evolving society has an inherent problem of crime ranging from espionage to petty theft, from rape to computer hacking, and from youth gang violence to terrorism. The fact is that these activities are a real part of your professional life and of the service you owe to you client. Security must become as important in what you do as cooling systems, rest room appliances, and paint colors.

5. Further Reading

Bernalillo County Sheriff's Department Gang Unit, Gangs in Albuquerque, undated unpublished map.

Joel Carlson, Some Sources of Information in Security, Threat Assessment, and the Engineering Response to Such Phenomenon. Resource list compiled for Sandia National Laboratories Architectural Surety℠ program, Albuquerque, NM, 1997.

Goals 2000: Educate America, Safe, Disciplined, and Drug-Free Schools, a background paper for the satellite town meeting, July 20, 1993.

Sandra R. Sabo, Security by Design, in *American School Board Journal,* pp. 37-38, January 1993.

U. S. Department of State, list of major terrorist groups from *Global Terrorism.* U. S. Department of State, Washington, D.C., 1995.

Intentionally Left Blank

Appendix C

Security Concepts and Technology

Objectives

The objectives of this lecture, presented by Dennis Miyoshi of Sandia National Laboratories on February 10 and 17, 1997, are to:

- Understand the basic concepts of security
- Be able to describe the steps in designing a security system
- Be familiar with the various security technologies on the market today

This lecture introduces the basic theories of security systems engineering and develops the process that is employed in the design and evaluation of any security system, whether you are protecting a government building, a home, or a convenience store cash register. There are many, many security technologies available to support the **detection**, **delay**, and **response**, but the appropriateness and cost-effectiveness for any particular application can vary widely. Understanding the total system and the needs vs. constraints of each application is the first step in accomplishing an effective security system.

1. Introduction

In the new but growing field of architectural surety℠, security plays a major role in addressing the *malevolent* threat. This is one of the more difficult parts of surety, as security is not determined by laws of nature, as in the expected effects of a 100-year storm. The human element is quite difficult to predict, indeed, the actions of a malevolent person toward a site or structure is almost infinite in the number of approaches possible. Through careful analysis of the more likely possibilities, this threat to surety can be greatly mitigated.

2. Theory and Principles

The design of an effective physical protection system (PPS) is a cyclic process as illustrated in **Figure C-1.** The process begins with the definition of the PPS objectives followed by the design of a PPS. The effectiveness of the PPS design is then analyzed. The results of the analysis answer the question: "Does the PPS satisfactorily meet the protection objectives?" If the system is not satisfactory, it must be redesigned. The next design cycle then attempts to eliminate weaknesses identified in the system. The cycle is repeated until an effective "final design" is achieved.

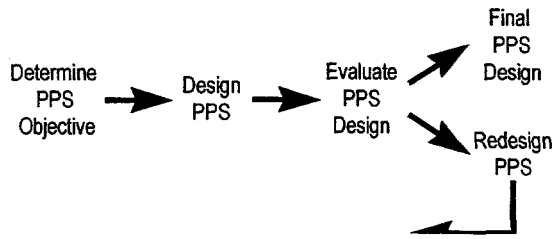


Figure C-1. Physical Protection System

Determining the PPS Objectives

In addressing this first step of determining the objectives of the protection system, the designer must (1) characterize/understand the facility's (or structure's) operations and conditions, (2) define the threat, and (3) identify the targets.

(1) Characterize the facility. Facility operations and conditions characterization require developing a thorough description of the facility (or structure) itself, for example, the location of the site boundary, structure locations, floor plans or layouts, and access points. A description of the processes within the facility or location is also required, as well as identification of any existing physical protection features. This information can be obtained from several sources, including facility blueprints, process descriptions, safety analysis reports, and environmental impact statements. In addition to acquisition and review of such documentation, a tour of the site being examined and interviews with facility personnel or other relevant stakeholders are necessary. This provides an understanding of the physical protection requirements for the site as well as an appreciation for the operational and safety constraints that must be considered. Compromises must usually be made on all sides so that operation can continue in a safe environment while an acceptable level of security is maintained.

(2) Define the threat. A threat definition for the facility must be made, with information collected to answer three questions about any potential adversaries:

- What type (or class) of adversary is to be considered?
- What is the range of the adversary's tactics?
- What are the adversary's capabilities?

Adversaries can be separated into three classes: outsiders, insiders, and outsiders in collusion with insiders. For each class of adversary, the full range of tactics (deceit, force, stealth, or any combination of these) should be considered. Deceit is the attempted defeat of a security system by using false authorization and identification; force is the overt, forcible attempt to overcome a security system; and stealth is the attempt to defeat the detection system and enter the site covertly.

Important capabilities for the adversary include his knowledge of the PPS in place, his level of motivation, any skills that would be useful in the attack, the speed with which the attack is carried out, and his ability to carry necessary tools and weapons. Since it is not generally possible to test and evaluate all possible capabilities of an unknown adversary, the designer and analyst of the security system must make assumptions. These assumptions can be based on published information about human performance and the tested vulnerabilities of physical protection elements.

Figure C-2 shows example adversary capability and motivation charts that may be used in helping to adequately define this threat.

Outsider Adversary

		Type of Adversary		
		Terrorist	Criminal	Extremist
Potential Action Likelihood *(H, M, L)	Theft			
	Sabotage			
	Other _____			
Motivations *(H, M, L)	Ideological			
	Economic			
	Personal			
Capabilities	Number			
	Weapons			
	Equipment and tools			
	Transportation			
	Technical experience			
	Insider assistance			

* H = High
M = Medium
L = Low

Insider Adversary

Insider	Access to SNM (Often, Occasionally, Never)	Access to PPS (Often, Occasionally, Never)	Access to Vital Equipment (Often, Occasionally, Never)	Theft Opportunity *(H, M, L)	Sabotage Opportunity *(H, M, L)	Collusion Opportunity *(H, M, L)

* H = High
M = Medium
L = Low

Figure C-2. Examples of Adversary Capability and Motivation Charts

(3) Identify the targets. Target identification is a critical step in the PPS process, as a site cannot protect everything—the cost would be prohibitive. The attractiveness of individual targets for theft or sabotage is important to understand, so that a PPS can be designed that protects those targets at greatest risk while staying within budget. Not surprisingly, the approach for protecting an item for theft versus protecting an item or structure for sabotage can be very different. Defining the theft or sabotage target(s) is the information that will help define how extensive the technology components will be in order to provide protection with any given response force.

Designing the PPS

The next major step in the PPS creation is to determine how best to combine such elements as fences, vaults, sensors, procedures, communication devices, and protective force personnel into a PPS that can achieve the protection objectives. The resulting PPS design should meet these objectives within the operational, safety, and economic constraints of the site. The primary functions of PPS—detection, delay, and response—will be discussed in detail later in this chapter.

Certain general guidelines should be observed during the PPS design. A PPS system is generally better if detection is as far from the target as possible, and delays are near the target. In addition, there is close association between detection and assessment, for either interior or exterior situations. (The designer of the PPS should be aware that detection without assessment is not detection). Another close association is the relationship between response and response force

communications. A response force cannot respond unless it receives a secure communication call (or alarm) for a response.

These and other features of PPS components contribute to the PPS design when the designer takes advantage of the strengths of each piece of equipment and uses equipment in combinations that complement each other and protect any weaknesses.

Analyzing the PPS Design

Analysis and evaluation of the PPS design begins with a review and thorough understanding of the protection objectives the designed system must meet. This can be done simply by checking for required features of a PPS, such as intrusion detection, entry control, access delay, response communications, and a protective force. However, a PPS design based on required features cannot be expected to lead to a high-performance system unless those features, taken together, are sufficient to assure adequate levels of protection. More sophisticated analysis and evaluation techniques can be used to estimate the minimum performance levels that will actually be achieved by an existing or a proposed PPS.

An existing PPS at an operational facility cannot normally be fully tested as a system. The nature of some facilities and materials prevents tests involving simulated adversary teams that penetrate barriers or actually steal or sabotage targets; the cost of doing such a test may well exceed the cost the target being protected. This is especially true of sites vulnerable to explosives, etc. When direct system tests are not practical, evaluation techniques are based on performance tests of component subsystems. Component performance estimates are then combined into system performance estimates by the application of system modeling techniques.

The end result of this phase of the PPS design and analysis process is a system vulnerability assessment. Analysis of the PPS design either finds that the design effectively achieved the protection objectives or identifies weaknesses. Some types of analyses actually help to select particular system improvements, and can allow cost vs. system effectiveness comparisons to be made. If the protection objectives are achieved, then the design and analysis process is completed. However, the PPS should be analyzed periodically to ensure that the original protection objectives are still valid and that the protection system continues to meet them.

Redesigning the PPS

As mentioned earlier, the result of the analysis phase is a system vulnerability assessment. If the PPS is found ineffective, vulnerabilities in the system can be identified. The next step in the design and analysis cycle is to redesign or upgrade the initial protection system design to correct the noted vulnerabilities. An analysis of the redesigned system is performed and this cycle continues until the results indicate that the PPS meets the protection objectives.

The Detailed PPS

Figure C-3 shows the PPS further broken down into tasks or components. The technology components will be further explained in the remainder of this chapter.

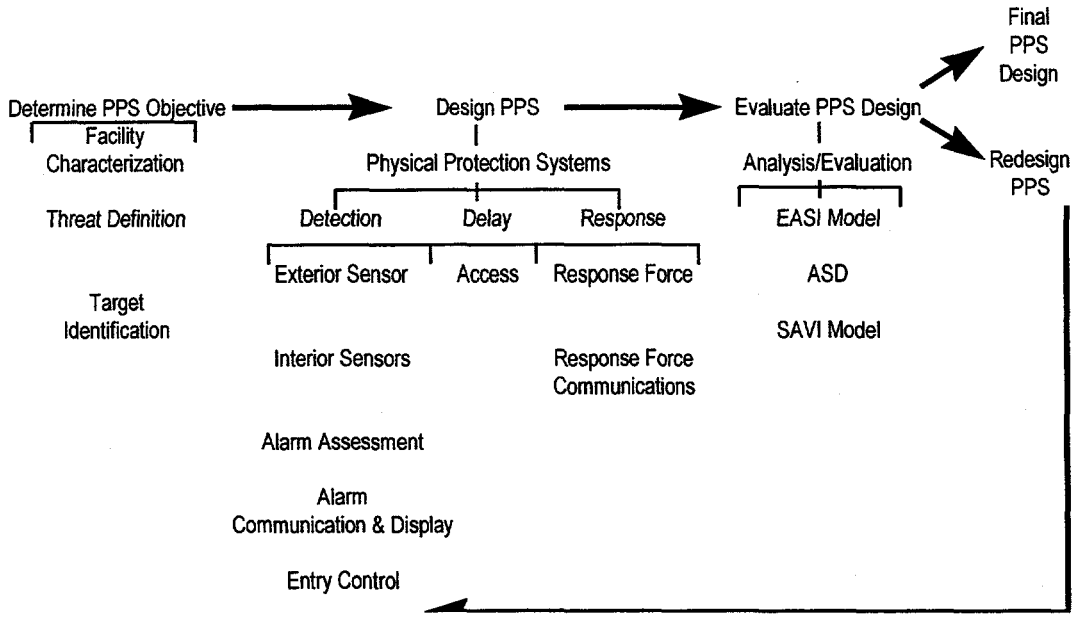


Figure C-3. Physical Protection System Broken Down into Tasks

There are two basic methods for preventing theft and sabotage:

(1) Deter the adversary. Convince the adversary that the task of attacking your target is either too difficult or will most likely result in the adversary being caught. The best possible scenario is that by implementing a PPS that is perceived as too difficult to defeat, you are avoiding attacks. However, the problem with deterrence is that, while you may be doing a great job of deterrence and everyone in the community is keenly aware of the terrific protection system you have, you could still have an attempted attack, especially by someone who is under the influence of alcohol or drugs. On the other hand, you could have no deterrence at all, and just *happen* to not have any attacks on your site simply by chance. It would be impossible to measure the effectiveness and, therefore, justify the expense of a deterrence effort.

(2) Defeat an adversary attack with your PPS. There are three major functions of an actual PPS system—detection, delay, and response. See **Figure C-4**. Detection is the ability of your system to notice an intrusion or other unwanted action, which is then communicated to your response force. Delay is the element that slows your adversary down and keeps him from being able to immediately walk away with an item of value or blow up a bridge, until your response force is able to prevent him from accomplishing his goal. The response can take the form of either a simple interruption or an actual "neutralization" of the adversary, depending on the target value/risk and the threat.

Defeating the Adversary

Ideally, to maximize the probability of intercepting and/or neutralizing an attack, a site must make any attacker's task extremely difficult to complete. Providing a number of protective

elements in sequence to optimally "burden" the attacker is called **protection-in-depth**. Basic approaches of protection-in-depth will increase the adversary's uncertainty about the system, require the adversary to make more extensive preparations before the attack, and create additional steps where the adversary may fail or abort his mission. **Balanced protection** is a guiding principle that suggests that all elements of a particular layer of protection be equivalent in the delay time necessary to defeat them. For example, a building can be a layer of protection; the various elements of that layer include the walls, the doors, the windows, and the roof. It would be a waste of money, and NOT balanced protection, to spend $20,000 on a vault door to the building, which would provide an hour of delay for the adversary to penetrate, when the walls

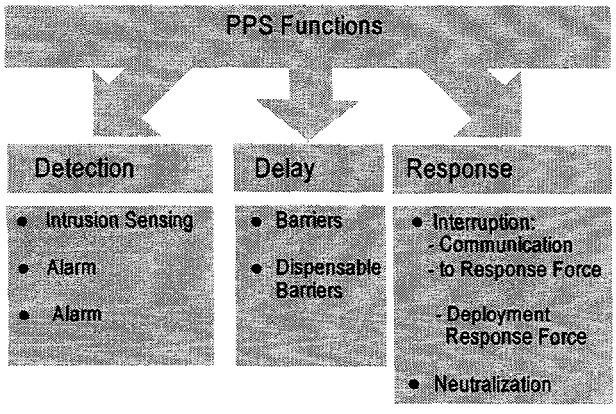


Figure C-4. Three Major Functions of PPS System–Detection, Delay, and Response

around the vault door are simple sheet rock over wood framing, which allows a less than 30-second delay to penetrate.

Single point failures are to be avoided at all costs within a well-designed PPS. If the single sensor you were counting on for detection is out of order as a result of a lighting storm, then your entire PPS has failed and the attacker will be successful. **Graceful system degradation** is a concept that provides that your PPS not go from totally adequate to totally inadequate just because your perceived threat is slightly different. For example, if your perceived threat of one teenager who brings along a friend is that now your adversary consists of two teenagers, the system should not automatically fail so that the two are easily able to successfully accomplish their task.

All of these constraints and provisions must, of course, fit within the daily operations or environment of your site or structure. It would be ludicrous if, because of the possible damage a motorist with a bomb could do to a particular bridge, you forbade any vehicles from crossing that bridge. Security is merely a part of the entire picture.

Analyzing Possible Adversary Paths or Sequence of Tasks

Simply put, in order to thwart an attacker of a particular site or structure, the possible **paths** that the attacker might take to accomplish his goals must be well understood. Once all the paths into a facility or steps toward a goal can be established, the easier/cheaper-to-thwart/more likely paths can be examined independently and evaluated as to their vulnerabilities, weaknesses, and possible upgrades to make them more difficult/expensive-to-attack/less likely avenues for an attacker. For example, if you were trying to assure the safety of a town's water supply by protecting the pump on its well, a possible path might be:

(1) Penetrate fence

(2) Penetrate outer door of well house

(3) Penetrate inner wall of pump room

(4) Penetrate the inner door of well enclosure

(5) Destroy the pump

It is key here to devise a type of detection mechanism and/or delay mechanism on each of these path elements. A reasonable approach for the example of a town well is shown in **Figure C-5**.

Adversary Action	Delay Element	Detection Element
Penetrate Fence	Fence Fabric	Fence Sensor
Penetrate Outer Door	Door Hardness	Sensors on Door
Penetrate Wall	Wall Hardness	Personnel Hear Noise
Penetrate Inner Door	Door Hardness	Sensors on Door
Destroy Pump	Time Required to Sabotage Target	Loss of Pump

Figure C-5. Protection Elements Along Path

It is obvious that to "beat" the adversary, our response force must be deployed and respond at the site in less time than it takes the adversary to successfully completely his path or sequence of tasks **after** detection has been made and the response force notified. See **Figure C-6**. To accurately predict that the response force's response time to neutralization is less than the attacker's path time after detection and notification, a site must

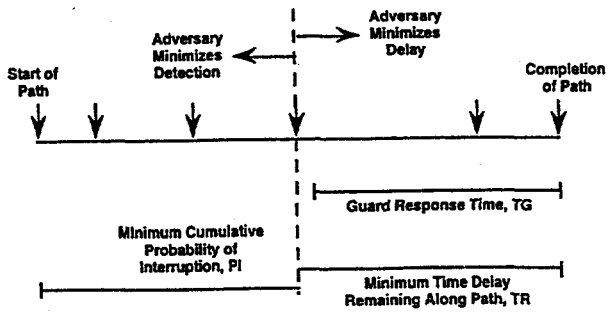


Figure C-6. Sequence of Tasks After Detection

develop a series of timings that are probably "best case" (for the most well-trained attacker) for defeating the various elements of the PPS. The sum of these minimum times yields the Time to Goal (TG). The site must then develop or calculate the highest possible probability of NOT detecting the adversary at each of these elements. The product of these probabilities of each of the elements, subtracted from one, provides the Probability of Detection. Clearly, the response force's Time to Respond (TR) must be less than the adversary's TG. See **Figure C-7**.

Figure C-8 gives a visual diagram of a typical facility that has several layers of protection elements. These layers are similar to those of an onion, in that each of them ideally encompasses the entire set of layers that lies beneath it. The various possible paths of an adversary become clear, but may be

Action	Minimum Time	Maximum Nondetection Probability	
Penetrate Fence	6 sec	0.5	PI = 1 - .03 = .97
Penetrate Outer Door	84 sec	0.2	
Penetrate Wall	120 sec	0.3	
Penetrate Inner Door	84 sec	0.1	TR = 114 sec TG = 100 sec
Destroy Pump	30 sec	0.0	

Figure C-7. Response Force's Time to Respond, TR, and Adversary's Time to Goal, TG

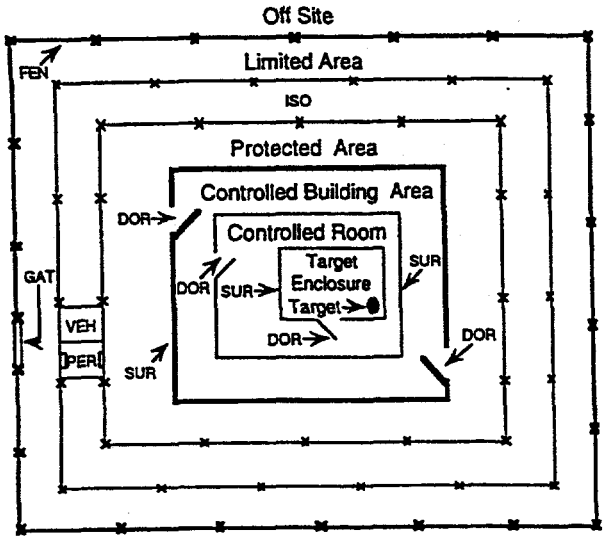


Figure C-8. Typical Facility with Layers of Protection

further illustrated by an Adversary Sequence Diagram, ASD, as shown in **Figure C-9**. An ASD explicitly illustrates those paths that are a possibility by the perceived threat to a site.

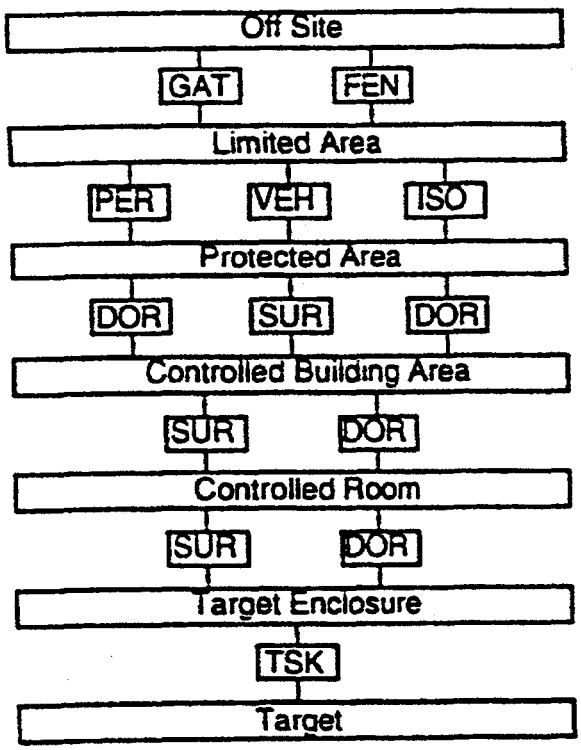


Figure C-9. Adversary Sequence Diagram

3. Applications

The Detection Technology Components of the PPS

Technology can provide many different approaches to accomplishing the detection function of your PPS. The technology components that make up detection include:

- Exterior intrusion sensors
- Interior intrusion sensors
- Assessment
- Alarm communication and display
- Entry control

As anyone with an alarm system in their own home knows, one of the most important objectives of any detection system is to minimize the alarms that are not related to an actual adversarial intrusion. These nonadversary-related alarms can be categorized in the following manner:

- Nuisance alarms are the response to a known stimulus unrelated to an intrusion attempt. Alarms generated by any known nonintruder stimulus would be classed as nuisance, even if the stimulus produced a sensor output identical to that for an intruder. For example, whenever authorized people, vehicles, or activities in the vicinity of a sensor result in alarms, those alarms are nuisance alarms. Animals, wind, rain, and electromagnetic interference (EMI) can also cause nuisance alarms.
- Unknown alarms are caused by an unidentified source. Reasonable efforts should be made to identify the cause of all alarms so that the number of unknown alarms is low.

- False alarms are caused by internal equipment malfunction. Since false alarms often have no readily assessable cause, they can also be referred to as unknown alarms.

How vulnerable to defeat a particular sensor is can be another important measure of quality. There are two basic defeat modes: spoof and bypass. Spoof refers to defeat modes that employ equipment and actions to mask the intruder's signal or inhibit the electronics from producing an alarm during an intrusion through the detection zone of the intrusion detection sensor. Bypass is a defeat mode in which the intruder is able to defeat the intrusion detection sensor by avoiding its detection zone.

Sensors can be made less vulnerable to defeat if they are equipped with tamper alarms, anti-capture circuitry, line supervision capability, and full end-to-end self-test capability. Installation practices such as overlapping the sensor fields to provide mutual protection for each sensor or adding special sensors to protect weak points in the sensor system are also essential considerations in the design of a sensor system that is not highly vulnerable.

Sensors, both for exterior and interior applications, may generally classified into five different methods:

- Passive/active
- Covert/visible
- Line-of-sight/terrain following
- Mode of application
- Volumetric/line detection

Passive sensors detect energy emitted by the target (here we are referring to the adversary as the target) of interest or detect the perturbation of some natural field of energy by the target. An example of the former is the mechanical energy from a walking human transferred to the soil or from a human climbing on a fence. An example of the latter is detection of a change in the local magnetic field caused by the introduction of ferromagnetic material.

Active sensors transmit energy and detect a change in the received energy because of the presence or motion of the target. An example of an active sensor is one that transmits electromagnetic energy of a certain wavelength and measures the energy returning to a receiver. The fixed amount of energy normally detected by the receiver is perturbed by the presence or motion of a target.

The distinction between passive and active sensors has practical importance for some applications. The presence and/or location of a passive sensor is more difficult to determine than that of an active sensor, putting the intruder at a disadvantage. In environments with explosive vapors or materials, passive sensors are safer than active ones because no potentially explosion-initiating energy is emitted. However, signal processing techniques for active sensors are generally more effective at discriminating against nuisance alarm sources than such techniques for passive sensors.

Covert sensors are hidden from view, such as sensors buried in the ground. Visible sensors are in clear view of an intruder; examples are sensors attached to a fence or mounted on their own support. Covert sensors are more difficult for an intruder to detect and locate, and thus they can be more effective. Covert sensors are also more aesthetically pleasing. But visible sensors may have a psychological

deterrent effect. Visible sensors are typically simpler to install and easier to repair than covert ones.

Line-of-sight (LOS) sensors require a clear LOS in the detection space. This usually means a clear LOS between the transmitter and the receiver for active sensors. These sensors normally require a flat ground surface, or at least a clear LOS from each point on the ground surface to both the transmitter and the receiver. If these conditions are not met for LOS sensors, then detection is incomplete.

Terrain following sensors detect equally well on flat and on irregular terrain. The transducer elements and/or the radiated field follows the terrain and results in uniform detection throughout the detection zone.

The main practical consequence of this distinction is the cost of installation. For sites without flat terrain, the use of LOS sensors requires expensive site preparation to achieve acceptable grading.

Mode of application is the classification that groups sensors into three common classes:

- Buried-line, in which the sensor is in the form of a line (or lines) buried in the ground
- Fence-associated, in which the sensor either is mounted on a fence or forms a sensor fence
- Freestanding, in which sensors are neither buried nor associated with a fence but mounted above ground on their own supports.

Volumetric/line detection refers to a sensor's detection envelope. A volumetric sensor exhibits detection in a volume of space. A line sensor exhibits detection along a line. Volumetric sensors generally have a detection volume that is not visible and is difficult to identify precisely. For this reason, intrusion attempted around this volume would not possess a high possibility of bypassing the sensor undetected. On the other hand, a line sensor generally has a detection zone that is more easily defined. For example, a fence disturbance sensor has a clearly defined detection zone, i.e., the fence. Therefore, an intrusion that does not touch the fence has a high confidence of no detection. Of course, there are applications for which the line sensor may be better because nearby activity or narrow confines may increase the nuisance alarm rate of volumetric sensors.

Exterior Sensor Systems

Preferred features for an exterior sensor system include:

- Continuous line of detection
- Protection-in-depth
- Complementary sensors
- Alarm combination and priority schemes
- Clear zone
- Site-specific design
- Tamper protection
- Self-test capability
- Suitable for the physical and environmental conditions intended
- Integrated with video and barrier systems

Table C-1 summarizes the different exterior intrusion sensor technologies according to the different sensor classification schemes.

Exterior Sensor Descriptions

- **Pressure or seismic sensors** respond to disturbances of the soil caused by an intruder walking, running, jumping, or crawling on the ground. Pressure sensors are generally sensitive to lower frequency pressure waves in the soil, and seismic sensors are sensitive to higher frequency vibration of the soil. A typical pressure sensor consists of a reinforced hose that is filled with a pressurized liquid and connected to a pressure transducer. A typical seismic sensor consists of a string of geophones. A geophone consists of a conducting coil and a permanent magnet. Either the coil or the magnet is fixed in position, and the other is free to vibrate during a seismic disturbance; in both cases, an electrical current is generated in the coil.
- **Magnetic field sensors** respond to a change in the local magnetic field caused by the movement of nearby metallic material. Magnetic field sensors, therefore, are effective for detecting vehicles or intruders with weapons. This type of sensor consists of a series of wire loops or coils buried in the ground. Movement of metallic material near the loop or coil changes the local magnetic field and induces a current.
- **Ported coaxial cables** respond to motion of a material with a high dielectric constant or high conductivity near the cables. This material includes both the human body and metal vehicles. The sensor consists of a transducer cable with an outer conductor that does not provide complete shielding for the center conductor, and, therefore, some of the radiated signal leaks through the ports of the outer conductor.
- **Fence disturbance sensors** respond to mechanical disturbances of the fence. They are primarily intended, therefore, to detect an intruder who climbs on or cuts through the fence fabric. Several kinds of transducers are used to detect the movement or vibration of the fence. These include switches, electromechanical transducers, and strain sensitive cables.
- **Sensor fences** are also designed primarily to detect climbing or cutting on the fence. Taut wire sensor fences consist of many parallel, horizontal wires with high tensile strength that are connected under tension to transducers near the midpoint of the wire span. These transducers detect deflection of the wires caused by an intruder cutting the wires, climbing on the wires, or separating the wires. The wire is typically barbed wire, and the transducers are either mechanical switches or

Table C-1. Different Exterior Intrusion Sensor Technologies According to Classification Schemes

	Passive or Active	Covert or Visible	LOS or Terrain Following	Volumetric or Line Detection
Barrier Line				
Seismic pressure	P	C	TF	L
Magnetic field	P	C	TF	Vol
Ported coaxial	A	C	TF	Vol
Fence Associated				
Fence disturbance	P	V	TF	L
Sensor fence	P	V	TF	L
Electric field	A	V	TF	Vol
Freestanding				
Active infrared	A	V	LOS	Vol
Bistatic microwave	A	V	LOS	Vol
Video motion detection	P	C	LOS	Vol

piezoelectric elements. Another type of sensor fence uses mesh fabric as the transducer.

- **Electric field or capacitance sensors** are designed to detect a change in capacitive coupling among a set of wires attached to, but electrically isolated from, a fence.
- **Active infrared sensors** work by transmitting an infrared (IR) beam from an IR light-emitting diode through a collimating lens. This beam is received at the other end of the detection zone by a collecting lens that focuses the energy onto a photodiode. The IR sensor detects the loss of the received infrared energy when an opaque object blocks the beam. A typical multiple-beam IR sensor system typically consists of two vertical arrays of IR transmitter and receiver modules. The IR sensor creates an IR fence of multiple beams but detects a single beam break.
- **Bistatic microwave sensors** consist of two identical microwave antennas installed at opposite ends of the detection zone. One is connected to a microwave transmitter and the other is connected to a microwave receiver that detects the received microwave energy. This energy is the vector sum of the direct beam between the antennas and the microwave signals reflected from the ground surface and other objects in the transmitted beam. Microwave sensors respond to changes in the vector sum caused by objects moving in that portion of the transmitted beam that is within the viewing field of the receiver. These sensors are often installed to detect a human crawling or rolling on the ground across the microwave beam.
- **Video motion detectors (VMDs)** process the video signal from closed-circuit television (CCTV) cameras. These cameras view the scene of interest and may be jointly used for detection, surveillance, and alarm assessment. Lighting is required for continuous 24-hour operation. VMDs sense a change in the video signal level for some defined portion of the viewed scene. Detection of human body movement is reliable except during conditions of reduced visibility.

Interior Sensor Systems

Table C-2 summarizes the different interior intrusion sensor technologies according to the different sensor classification schemes.

Table C-2. Different Interior Intrusion Sensor Technologies According to Classification Schemes

	Passive or Active	Covert or Visible	Volumetric or Line Detection
Boundary Penetration Sensors			
Electro-mechanical	P	C	L
Infrared	both	V	L
Vibration	P	C	L
Capacitance	P	C	L
Sonic	both	C	V
Interior Motion Sensors			
Microwave	A	V	V
Ultrasonic	A	V	V
Sonic	A	V	V
Infrared	P	V	V
Proximity Sensors			
Capacitance	P	C	L

Interior Sensor Descriptions

- **Electromechanical sensors** include the common and relatively simple door and window switch. Most of these switches are magnetic switches, which consist of two units: a switch unit and a magnetic unit. The switch unit, which

contains a magnetic reed switch, is mounted on the stationary part of the door or window. The magnetic unit, which contains a permanent magnet, is mounted on the movable part of the door or window, adjacent to the switch unit. With the door or window closed, the magnetic field from the permanent magnet is adjusted to place the magnetic reed switch in the closed (or secure) position. A subsequent opening of the door or window (removal of the magnet) results in the decrease of the magnet field and movement of the switch to the open (or alarm) position. Protection by these sensors is only as good as the penetration resistance of the door or window. These sensors are only adequate if the intruder opens the door or window for entry.

- **Active infrared sensors** establish a beam of infrared light using an infrared light source or sources as the transmitters and photodetectors for receivers. Several transmitters and receivers are usually employed to provide a system with multiple beams, and the beams are configured into a vertical infrared "fence." The narrow vertical plane in which this sensor operates does not provide any significant volume coverage, and the PPS designer must carefully consider its installation in order to avoid easy defeat or bypass. These sensors can also be used over short ranges for applications for filling gaps, such as gates, doors, and portals.
- **Vibration sensors** detect movement of the surface to which they are fastened. A human blow or other sudden impact on a surface will cause that surface to vibrate at a specific frequency determined by its construction. The vibration frequencies are determined to a lesser extent by the impacting tool. Vibration sensors may be as simple as jiggle switches, or they may be as complex as inertial switches or piezoelectric sensors. In each case, they are designed to respond to frequencies associated with breaking and entering (>4 kHz) and to ignore normal building vibrations such as air conditioning or heating noise. Glass break sensors are vibration sensors that are specifically designed to generate an alarm when the frequencies more nearly associated with breaking glass are present (>20 kHz).
- **Capacitance proximity sensors** establish a resonant electrical circuit between a protected metal object and a control unit. The capacitance between the protected metal object and ground becomes a part of the total capacitance of a tuned circuit in an oscillator. The tuned circuit may have a fixed frequency of oscillation or the oscillator frequency may vary. Oscillators whose frequency is fixed have an internally adjustable capacitance that is used to compensate for different capacitive loads. A loop of wire, known as the protection loop, is connected between the conductive object or objects to be protected and the control unit that contains the tuned circuit. Once the connection is made, the circuit is adjusted to resonance using a tuning meter for an indicator. Then any change in capacitance between the protection loop (which now includes the metal objected to be protected) and ground will disturb the resonance condition, thereby causing an alarm.
- **Passive sonic sensors** are one of the simplest intrusion detectors, using a microphone to listen to the

sounds generated in the area within range of the microphone. If sounds of the correct amplitude, frequency content, and duration or repetition rate corresponding to a destructive penetration are heard, an alarm is generated. Passive sonic sensors are made up of a microphone, amplifier, and signal conditioner.

- **Active sonic sensors** establish a detection field using energy in the acoustic spectrum at frequencies between 500 and 1000 Hz. Since a much lower frequency is transmitted, good reflections are obtained, and standing waves are established in the protected volume. Active sonic sensors are similar to ultrasonic detectors in that they both use air as their signal transmission medium. The primary difference between the two is that sonic detectors fill the volume requiring protection with energy in the audible frequency range instead of with ultrasonic energy.
- **Microwave sensors** establish an energy field using energy in the electromagnetic spectrum, usually at frequencies on the order of 10 GHz. Interior microwave motion sensors are nearly always in the monostatic configuration with a single antenna used to both transmit and receive. Intrusion detection is based on the frequency shift between the transmitted and received signal caused by the Doppler effect from a moving object in the beam. The shape of the detection zone is governed by the design of the antenna and is roughly similar to an elongated balloon.
- **Ultrasonic sensors** establish a detection field using energy in the acoustic spectrum typically in the frequency range between 19 and 40 kHz. For monostatic ultrasonic sensors, detection is based on the frequency shift between the transmitted and received signal caused by the Doppler effect from a moving object in the beam. Most common solid materials such as walls, cardboard, windows, etc., will stop or deflect ultrasonic waves.
- **Pressure sensors**, often in the form of mats, can be placed around or underneath an object. Pressure mats consist of a series of ribbon switches positioned parallel to each other along the length of the mat. They are constructed so that when an adequate amount of pressure, depending on the application, is exerted anywhere along the ribbon, the metal strips make electrical contact and initiate an alarm. When using pressure mats in security applications, the mat should be well-concealed under carpets or even under tile or linoleum floor coverings. If the intruder is aware of their existence, he can just step over or bridge over the mat.

A large number of environmental conditions can produce noise in the same energy spectra that the intrusion sensors are designed to detect. These outside noise sources can degrade sensor performance and cause the sensor to generate an alarm even when an intruder is not present. Environmental conditions that can affect different types of interior sensors include:

- Electromagnetic (e.g., lightning, power lines, radio frequency, telephone lines)
- Nuclear radiation (e.g., the semiconductors within sensors can be damaged by nuclear radiation)
- Acoustic (e.g., ventilating, air-conditioning, and heat equipment,

television equipment, aircraft, vehicles, trains)

- Thermal (e.g., anything that causes uneven heat distribution)
- Optical (e.g., light energy from sunlight, interior lighting, highly-reflective surfaces)
- Seismic (e.g., seismic phenomena can produce undesirable vibration in interior areas, including earth tremors, trains, thunder)
- Meteorological (e.g., lightning, thunder, rain, hail, temperature, wind)

New/Emerging Sensor Technologies

Some of the new sensor technologies that are being introduced for the protection of sites and structures include:

- Hand-held sensors
- AIR Shield Sensor
- Dual PIR detectors
- Hall effect balanced magnetic switches
- Fiber optics for use in floors, ceilings, and blankets
- Standard test glassbreak sensors

Alarm Assessment

Assessment is essential to identify the cause of an alarm and determine if an alarm is a threat or nuisance. Assessment is usually provided through closed-circuit television coverage of each sector (group) of sensors, supplemented in some facilities by visual checks from towers or roving patrols. A video alarm assessment system allows authorized personnel to rapidly assess sensor alarms at remote locations.

There are two purposes of assessment. The first is to determine the cause of each sensor alarm. This includes determining whether the alarm is a threat or nuisance alarm. The second purpose is to provide information about an intrusion. This includes specific details such as who, what, where, and how many.

A typical video alarm assessment system is shown in **Figure C-10**.

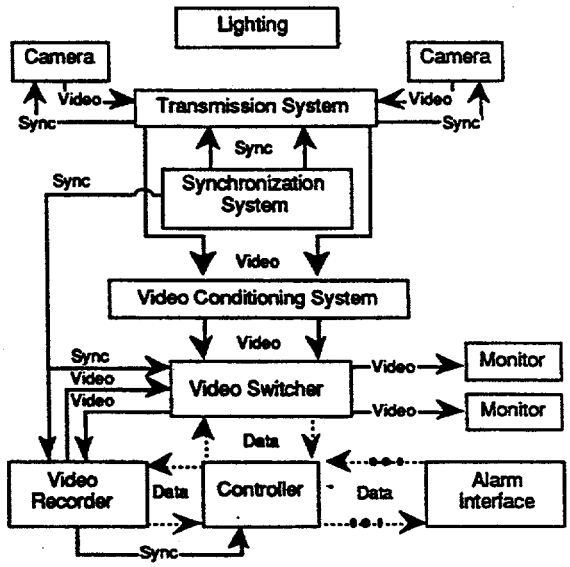


Figure C-10. Typical Video Alarm Assessment System

The major components and their functions include:

- The camera and lens to convert the image of the physical scene into an electrical signal
- The lighting system to illuminate the alarm location evenly with enough intensity for the camera and lens
- The transmission system to connect the remote cameras to the local video monitors so that no undesirable effects are introduced to the video signal

- A synchronization system to ensure that switching and recording are clean and free of vertical roll
- Video switching equipment to connect multiple video signals from cameras with monitors and video recorders,
- A video recording system to produce a record of an event
- Video monitors to convert a signal to a visual scene on the face of the output display
- A video controller to interface between the alarm sensor system and the alarm assessment system

Alarm Communication and Display

An essential part of any alarm reporting system is the communication link that transmits information from the sensors to the display and assessment equipment. Design considerations for alarm communication systems include the ability of the system to continue working after component failures, line supervision to detect broken lines or tampering, worst case delay in reporting an alarm, the ability to initiate sensor self-tests, ease of expansion, and cost. The most common types of communication links employed are land lines and radio or microwave links. Land lines are generally more practical for shorter distances (one or two kilometers) and radio is usually less expensive for longer distances.

Several physical protection techniques have been used to prevent or delay physical access to the line. One protection method employs metal conduit to protect the communication line. This method provides even more security if the joints are securely welded. Another technique for line protection is burial of the communication line. This can be costly for long distances. It does delay even the most determined attacker. When burial is planned, extra lines should be included in the cable to allow future expansion or individual line failure. The cable an be encased in concrete, or the soil directly above the cable can be covered with concrete or asphalt. If the entire area surrounding the cable path can be paved, any digging will most likely be easy to detect.

The alarm display equipment (operator's console) receives information from the sensors. There are several concerns which must be addressed in the design of the operator's console including the following:

- What information is presented to the operator
- How the information is presented
- How the operator communicates with the system
- The arrangement of the equipment at the operator's workstation

Examples of information that can be presented to aid in zone security include the following:

- The access/secure/alarm/tamper status of a zone
- The geographical location of the zone
- The time of the alarm
- Information about any special hazards or material associated with a zone
- Instructions for special actions
- Telephone numbers of persons to call
- Maps of the secure area

Entry Control Systems

An entry control system allows the movement of authorized personnel through normal routes, while detecting and delaying movement of unauthorized personnel or personnel carrying contraband (weapons, explosives, etc.). An alarm should occur when an entering individual is not properly identified or when contraband is detected. Upon receipt of an alarm, the protective force assesses the problem, determines whether the alarm is nuisance or valid, and, if necessary, initiates a preplanned response. Where entry is controlled, it is expected that all personnel and baggage will be examined for contraband. Maintenance tools, food, instruments, building materials, and operating supplies are candidates for examination.

Personnel entry control is the portion of an entry control system used to authorize entry and to verify the authorization of personnel seeking entry to a controlled area. This verification decision is usually based on determining whether the person:

(1) Is carrying valid credentials. Types of credentials used are photo identification badges, exchanges badges, stored-image badges, and coded credentials, which include key-cards and smart-cards.

(2) Knows a valid personal identification number (PIN). To gain entry, the user enters his memorized PIN on a keypad, which is then compared to the number stored in a reference file for that person.

(3) Or possesses the proper unique physical characteristic that matches the person's characteristic recorded at enrollment. (This is explained further in the following text.)

The physical characteristic match verifies the person's identity; the credential and ID number only verify that the person requesting entry has a valid credential or knows a valid code.

Personal identity verification. Personal identity verification systems verify claimed identification on the basis of some unique physical biometric characteristic of the individual. Commercial equipment is available that uses hand geometry, handwriting, eye retinal pattern, fingerprints, speech, and other characteristics, as described in the following.

- Hand geometry is based on the 3-D measurement and verification of the hand. This technique assesses several hand profile features such as the width of the hand and fingers at various places, finger lengths, finger thicknesses, and finger curvature.
- Signature verification has been used for many years by the banking industry, although signatures are easily forged. Automatic handwriting verification systems have been developed that use handwriting dynamics (such as displacement, velocity, and acceleration). Statistical evaluation of these data indicates that an individual's signature is unique and reasonably consistent from one signature to the next. Transducers that measure these characteristics can be located in either the writing instrument or the tablet.
- Fingerprints have been used as a personal identifier for more than 100 years and are still considered one of the most reliable means of distinguishing one individual from another. The art of processing human fingerprints for

identification has been greatly improved in recent years by the development of automated systems. All fingerprint identification systems require care in finger positioning and accurate print analysis and comparison for reliable identification.

- The retinal scan identity verification process relies on the fact that the pattern of blood vessels in the body is unique, and the pattern on the retina of the eye can be assessed optically through the lens of the eye. A circular path about the center of vision is scanned with a very low-intensity, nonlaser light from infrared light-emitting diodes. The intensity of the reflected light versus beam position during the scan indicates the unique location of the retinal blood vessels.

Contraband detection. Contraband consists of items such as unauthorized weapons, shielding material, explosives, and tools. Methods of contraband detection include metal detectors, package searches, explosives detectors, and low-dose x-ray machines for personnel, as described in the following.

- Metal detectors presently used to detect contraband carried by personnel generate a time varying magnetic field and either detect the changes made to the field due to the introduction of metal to the field, or detect the presence of eddy currents that exist in a metallic object caused by a pulsed field. The magnitude of the metal detector's response to metallic objects is determined by several factors: the conductivity of the metal, the magnetic properties of the metal (relative permeability), its shape, its size, and the orientation of the object within the magnetic field.
- Packages may be searched for contraband manually or by active interrogation. Active interrogation methods used to detect various metal objects considered contraband include x-ray, multiple energy x-ray, gamma ray, and neutron activation. In general, these methods are not safe for use on personnel.
- Passive explosives detectors detect the vapor emitted from explosives and can be safely used to search personnel. Some explosives cannot be detected by commercial explosives detectors because of their extremely low vapor pressures. Passive methods of detection are vapor detectors such as electron capture, mass spectrometry, ion mobility spectrometry, and chemiluminescence. The other type of passive vapor detector is the olfactory capability of animals, such as dogs.
- Low-dose x-ray capabilities for use on personnel have only recently been introduced to the market, but are gaining great favor with some markets. These low-dose x-rays use an energy output so low that the best way to describe its energy output is the difference between being inside or outside a building during daylight hours. These instruments have the capability to detect most of the contraband that can be carried by people.

The Delay Technology Component of the PPS

The objective of the physical protection system is to make sure that an adequate response force arrives in time to prevent an adversary from accomplishing his goal. The role of barriers is simply to increase the

adversary task time following detection by introducing impediments along any path the adversary may choose, thereby providing the needed time for the response force to arrive and react. Some barriers might deter or, if the adversary is unable to complete penetration, even defeat some threats. Since the degree to which the barriers are able to fulfill these two roles is uncertain, they can be considered only as obstacles to delay adversaries who are well equipped and determined.

Traditional barriers, such as chain-link fences, locked doors, grilled windows, masonry walls, and even many types of vaults, are not likely to delay a small group of properly equipped and dedicated adversaries for a significant length of time.

Dispensable (or activated) barriers can, on command, stop or delay an adversary from accomplishing his objective. Several types are being used today. A typical dispensable barrier system includes:

- A process for decision-making to determine when the dispensable barrier is to be activated
- Command and control hardware to implement this decision
- Material that is dispensed to physically deny access
- The dispensing mechanism
- A protective force located on site to respond

The dispensable material is normally stored in a compact form, and through a chemical or physical reaction, is expanded to an effective denial state. The properties that permit compact storage and rapid expansion make activated denial systems attractive in physical protection applications where operational consideration are dominant. Specific dispensable materials and associated dispensing hardware that have been developed include:

- Rigid polyurethane foam
- Stabilized aqueous foam
- Chemical smoke
- Sticky thermoplastic foam

4. Summary

This lecture describes the basic goals of a well-designed physical security system—detection, delay, and response—as well as presenting many of the technologies currently available to accomplish these goals. The process of incorporating these technologies into the system design is a cyclical process that emphasizes the complete understanding of the site or structure constraints. Even if funding is minimal, approaching the security problem through this methodology will yield the best security system that protects against the stated threats.

5. Further Reading

Robert Barnard, *Intrusion Detection Systems*. Butterworth-Heinemann, Stoneham, MA, 1988.

National Institute of Justice, *Research in Brief: The Expanding Role of Crime Prevention Through Environmental Design in Premises Liability*, NCJ 157309, U. S. Department of Justice, Washington, D.C., April 1996.

Physical Protection Systems, in *The Ninth International Training Course.* Sandia National Laboratories, Albuquerque, NM, 1993.

Nadine M. Post, More Than Merely Cops and Robbers, in *Engineering*

News Record, Special Report: Defensible Space, 1996.

Process of System Design and Analysis, in *The Ninth International Training Course.* Sandia National Laboratories, Albuquerque, NM, 1993.

Threat Definition, in *The Ninth International Training Course.* Sandia National Laboratories, Albuquerque, NM, 1993.

What is terrorism? In *The Economist,* pp.23-25, March 2, 1996.

Appendix D

Safety Concepts and Technology

Objectives

The objectives of this lecture, presented by John Covan of Sandia National Laboratories on February 24, 1997, include familiarizing the student with:

- Safety vocabulary
- Costs and scope of accidents
- Pitfalls of existing *(ad hoc)* approach to safety
- Benefits of a systematic approach to safety
- Strategies for implementing systematic approach
- Common problems in safety engineering

At the worst, infrastructure safety is a bit player; many design professionals feel that building codes should cover safety issues. Often *ad hoc* designs are committed to before safety is considered. This chapter proposes the application of a systems-based process to design in safety and maintain it throughout the life of the structure.

1. Introduction

Before an overview of safety as a component of infrastructure surety can be meaningfully presented, certain terms must be defined. **Safety, hazard**, and **danger** are defined below. Other terms, such as **safety culture, predictable safety, safety theme, safety principles, probability analysis, risk**, and **risk analysis** are defined later in this chapter, as the concepts are introduced.

For our purposes, the definition of **Safety** is nested within the definitions of hazard and danger, as shown in **Figure D-1**. To understand **safety**, one must have a clear understanding of **hazards** and **dangers**.

Some examples of personal injury can be shown as the result of **hazards** in buildings:

- Falling or being struck, such as the Kansas City walkway collapse
- Drowning, in indoor pools
- Fires, burns, electrocution (these hazards are ubiquitous)
- Suffocation/asphyxiation, in confined spaces
- Infection, such as Legionnaire's Disease

Safety As a Nested Definition

- ***Safety*** freedom from exposure to hazards
- ***Hazard*** a source of danger; a chance event: accident
- ***Danger*** liability to injury, pain, or loss

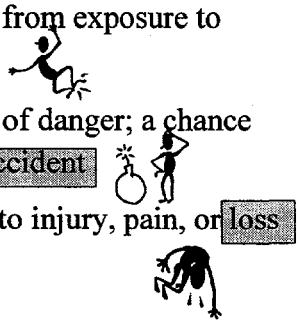


Figure D-1. Safety As a Nested Definition

- Bodily contamination, such as Chernobyl

Some of examples of danger include:

- Loss of life, such as the sinking of the Titanic
- Personal injury, such as the Union Carbide piping systems failure in Bhopal India.
- Loss of, or damage to, equipment, such as the space shuttle *Challenger* explosion
- Loss of resources, such as the Grand Teton dam burst, causing the loss of 16,000 livestock and the destruction of 100,000 acres of farmland

Stressors that may contribute to failures in structures can be identified as external forces and internal forces. External forces include both naturally occuring stressors, such as earthquakes and tornadoes, and manmade stressors, such as plane crashes and explosions. Internal pressures can include excessive static or dynamic loads or excessive pressures of any kind. Forces, whether external or internal, can be foreseen or unforeseen. When considering such stressors, it is important to recognize that such forces are rarely the sole cause of a failure.

The current approach to safety in infrastructure design and construction is inadequate. Some of the flaws include:

- The general assumption that existing codes and standards cover safety
- Safety designs are *ad hoc* and not integrated; there is no safety theme
- Safety subsystems often are tacked on late
- No systematic thought about safety
- No program controls or audit trails

Another problem of current infrastructure safety thinking is that accident causes are often oversimplified. When the vessel *Baltic Star* ran aground at full speed on the shore of an island in the Stockholm waters, the cause was widely reported as thick fog. A closer examination of the accident revealed that one of the boilers had broken down, the steering system reacted only slowly, the compass was maladjusted, the captain had gone down into the ship to telephone, the lookout man on the prow took a coffee break, and the pilot had given an erroneous order in English to the sailor who was tending the rudder. The latter was hard of hearing and understood only Greek. They were under time constraints for economic reasons. The lesson of the *Baltic Star* is that opportunities for safety are often missed.

Yet another flaw in current safety design is our tendency to discount risk. The sinking of the *Titanic* in 1912 is an example that could happen today. Calculations showed that up to four underwater compartments could be ruptured without the ship sinking. In the history of maritime accidents, none had involved the compromise of more than four compartments. The *Titanic*, therefore, was designed to withstand the rupture of four compartments, An iceberg cut a 300-foot gash in one side of the ship, flooding five adjacent compartments. The *Titanic Effect* is an important lesson to be learned: major accidents are often preceded by the belief that they cannot happen.

Just because most safety engineers are using the same approach that was used 85 years ago when the unsinkable *Titanic* went down on her maiden voyage doesn't mean things aren't changing. The incredible increases in technological complexity; the pace of technological change, which results in less chance to learn from experience; the public awareness and fear of risks; and litigation and award sizes are important trends that affect safety engineering. The lesson to be recognized is that life is getting tougher for the safety engineer. The old approach is even less effective than it was when the failures of the past occurred.

2. Theory and Principles

Why should the effort be expended to provide safety? How should the safety component of surety be addressed in the design and construction of infrastructure projects? There are several benefits to ensuring safety:

- It can avoid ***direct*** high-consequence losses
- It can avoid ***indirect*** high-consequence losses (e.g., lawsuits)
- It can safeguard against the designer's loss of reputation and livelihood
- It's the right thing to do

Similarly, there are steps that can be taken to prevent exposure to hazards. These actions include:

- Avoid the hazard itself, by using fireproof materials, for example
- Contain the hazard, as high-voltage equipment is contained
- Protect personnel directly, by providing self-contained breathing apparatus, for example.

There are clear goals of safety implementation. Safety implementation should:

- Meet or exceed codes and standards
- Be compatible with budget and schedule limits
- Be user-friendly (all phases)
- Not sacrifice aesthetics
- Pose acceptable risks (all kinds)
- Integrate well with other surety elements (e.g., make sure safety features do not interfere with security features and vice versa)
- Integrate well with non-surety elements (e.g., make sure building operational features do not interfere with safety features and vice versa)

When implementing safety, trade-offs will necessarily be made. Not everyone will be happy. This is at least, in part, because the scope of safety implementation is so large. The safety implementation scope should cover all of the following phases of the project life cycle:

- Business planning/concept phase
- Design/design verification phase
- Fabrication/construction phase
- Occupation/maintenance phase
- Refurbishment phase
- Demolition/recycle phase

This is the appropriate place to introduce some new terminology:

- **Safety culture**—a paradigm for key players in a system to embed predictable safety in an integrated fashion throughout the life cycle of the system. For a structure, key players include A/Es, fabricators, installers, tenants, maintenance crews, etc.
- **Predictable safety**—the capability of a system to maintain itself in a safe state during and after exposure to stress. The stress may be defined as a part of the performance requirements for the system

The strategies for safe design are hazard avoidance, defense in depth, and the use of redundant systems. These strategies can be employed using a safety process.

3. Applications

There is a safety process that can be applied for designing infrastructure projects. The six critical steps of the safety process include:

(1) Determine hazards and do a risk assessment

(2) Craft a safety theme

(3) Collect design alternatives to implement the theme

(4) Determine metrics—do trade-off study and select among alternatives

(5) Set up audit trail and program controls

(6) Continue controls throughout the life cycle

There are three types of risk associated with safety:

(1) Risk of realized hazards during fabrication, construction, occupation, etc.

(2) Programmatic risk, such as the loss of financier confidence, etc.

(3) Technical risk, such as when fail-safe devices do not operate as planned

Risk estimation serves several important functions in safety design and implementation. These roles include:

- Providing a way to rank various failure modes by risk
- Providing a way to estimate the number of accidents over life of system
- Serving as an aid in choosing whether to address a risk
- Serving as an aid in choosing among safety alternatives

Problems to avoid in the safety process are unrealistic risk assessments and overreliance on redundancy. The following examples illustrate these potential pitfalls.

Unrealistic Risk Assessment. In August 1989, a United Airlines DC-10 crashed near Sioux City, Iowa. A fan disk in one of the engines failed, severing all three (assumed independent) nearby hydraulic system lines. Because of this common-mode failure, flight controls were totally disabled. The aircraft made a crash landing using engine thrust as the sole means of control.

During certification, the DC-10 manufacturer submitted a probability calculation showing the chance of total loss of hydraulic fluid from engine rotor burst was less than one-in-a-billion. The need for compliance to fail-safe standards was judged to be unnecessary based upon the low probability result. Probability calculations used standard techniques of the industry and were accepted as evidence of a safe design.

Lesson: Don't dismiss failure modes on a low-risk basis. The low numbers simply say that the system is not going to fail by the ways considered but instead is going to fail at a much higher probability in a way not considered (*Fault Tree Handbook*, NUREG-0492).

Overreliance on Redundancy. At the Brown's Ferry Nuclear Power Plant in 1975, a fire burned uncontrolled for nearly eight hours. One of two nuclear power reactors was dangerously out of control for several hours. The emergency safety devices failed because fire destroyed the redundant electrical power and control systems.

Lesson: Common-cause failures can defeat redundancy.

Overreliance on Redundancy. The space shuttle *Challenger* relied on an apparently solid safety practice: a safety factor of 3 was chosen for the O-rings. The assumption was that if the first O-ring failed, the secondary one would seal. As we all sorrowfully know, this safety factor of 3 did not prevent tragedy. The failure of the primary O-ring led to failure of the secondary O-ring.

Lesson: Reliance on safety factors can be dangerous.

Another concern to be considered when designing for safety is cost. It is undeniable that there are added project life-cycle costs associated with safety, including:

- Direct costs of design, fabrication, and construction
- Maintenance costs
- Upgrade costs
- Demolition and disposal costs
- Insurance and other liability costs

These costs should be tracked and traded off against the benefits of implementing safety (avoiding **direct** high-consequence losses and **indirect** high-consequence losses such as lawsuits, safeguarding the designer's reputation and livelihood, and ethical considerations). It should be evident that the costs of NOT implementing safety far exceed the costs of implementing safety.

To show how the safety process works, let's very broadly apply it to the pump station example discussed in a previous lecture. Remember, the safety process steps are:

(1) Determine hazards and do a risk assessment

(2) Craft a safety theme

(3) Collect design alternatives to implement the theme

(4) Determine metrics—do trade-off study and select among alternatives

(5) Set up audit trail and program controls

(6) Continue controls throughout the life cycle

The pump station **hazards** could include both local and area hazards. Local hazards could include drowning, asphyxiation (confined space), burns, and electrocution. Area hazards might include flooding and chemical and/or bacterial contamination.

A preliminary and general **risk assessment** of these identified hazards could be performed by completing **Table D-1**.

Table D-1. Pump Station Risk Assessment Chart

hazard	frequency (# events/year)	consequence ($/event)
drowning		
asphyxiation		
burns		
electrocution		
flooding		
contamination		

The **safety theme** for the pump station is to provide a design and operational plan that avoids hazards or at least minimizes exposure to them. In the event that operators or the public are exposed to a hazard, the design will limit the consequences to a level commensurate with the benefits expected.

The **design variables** that are considered in identifying the pump station design alternatives include both location variables (such as surrounding topography, size of plot and maintenance access, and nearby population concentrations) and technical/aesthetic variables (such as the portion of the station that is above grade, whether it is electric-, diesel-, or gasoline-powered, and the degree to which the station is automated). The **design alternatives** will include considering the location choices of low spots to contain flooding and acquiring a buffer zone (space + capacity). Technical/aesthetic considerations might include considering that electric power avoids contamination, high automation and low MTBF avoid operator exposure, nested barriers prevent access to hazards, and interlocks on electrical and rotating gear can reduce hazard exposure.

Metrics for these design alternatives could include:

- Cost and lifetime
- Safety effectiveness
- Impact on security
- Impact on operations
- Impact on aesthetics

The **audit trail** and **program controls** for the pump station might include assuring the safety program documentation and its continuing availability and developing such **life-cycle controls** as materials and manufacturing methods during fabrication, construction and refurbishment methods, operational controls, and special considerations during demolition.

This very general example of applying the safety process to a pump station is intended to familiarize the student with the concepts. Obviously, an actual project would require much more intensive attention.

4. Summary

This lecture consisted of five parts:

- Part 1: Vocabulary and Definitions
- Part 2: Safety As It Exists Now
- Part 3: Safety As It Should Be
- Part 4: Safety Process: Steps and Things to Watch Out For
- Part 5: A Partially Worked-Out Example: Pump Station

Suggested discussion topics include:

- How to reconnect "A" to "E" in A/E (a safety-control issue)
- How to convince financiers that a sound system-safety program will save money
- How safety strategies differ if the scope changes from one to many identical structures

5. Further Reading

Air safety takes back seat to security, *USA Today,* Sec. Letters, February 18, 1997.

R. E. Follensbee, The Fail Safe Concept, presented at the Seattle Aircraft Certification Office Systems Designated Engineering Representative Workshop, September 14, 1993.

A. Ian Glendon and Eugene F. McKenna, *Human Safety and Risk Management.* Chapman and Hall, New York, 1995.

National Research Council, Commission on the Safety of Existing Dams, Water Science and Technology Board, Commission on Engineering and Technical Systems, Risk-Based Decision Analysis, in *Safety of Existing Dams: Evaluation and Improvement,* National Academy Press, Washington, D.C., 1983.

Charles Perrow, *Normal Accidents.* Basic Books, New York, 1984.

Gary Salmon, Dave Cattanach, and Desmond Hartford, Risk Management at Wahleach Dam, in *Civil Engineering,* pp. 39-41, February 1997.

Mario Salvadori, *Why Buildings Stand Up.* W. W. Norton, New York, 1980.

Mario Salvadori and Matthys Levy, *Why Buildings Fall Down.* W. W. Norton, New York, 1992.

John Shipp, Steel's Performance in the Northridge Earthquake, in *EQE Review,* Fall 1994.

Intentionally Left Blank

Appendix E

Reliability Concepts and Technology

Objectives

This lecture, presented by Robert Cranwell of Sandia National Laboratories on March 3, 1997, enabled students to gain a high level of understanding of:

- The importance of reliability
- The benefits of a systems approach to reliability
- Reliability vocabulary
- Measures of reliability
- Reliability modeling and prediction
- Benefits of designing for reliability
- Importance of incorporating uncertainty

1. Introduction

According to a 1989 Massachusetts Institute of Technology (MIT) study, the U.S. balance of trade has taken a serious downturn over the past few decades in the areas of automobiles, consumer electronics, machine tools, semiconductors, computers, and copiers (**Figure E-1**). Some of the possible reasons that our imports are exceeding our exports are reliability issues, including:

- Reliability is an afterthought; designs are approved and accepted before reliability is considered.
- American business is preoccupied with short-term profits.
- Maintenance and failure data tracking systems are poor.
- Customers and suppliers assume adversarial roles rather than partnering.
- System analyses often fail to account for uncertainties.
- Reliability focus is at the component level rather than the system level.

A system-level focus is a critical part of a successful reliability program. Historical data on complex systems indicate that the primary causes of system failures are not components. The top-down approach of a system-level reliability focus starts very early in design. Prediction and analysis are used at every stage of design to identify problems in meeting system requirements and to fix them as early as possible.

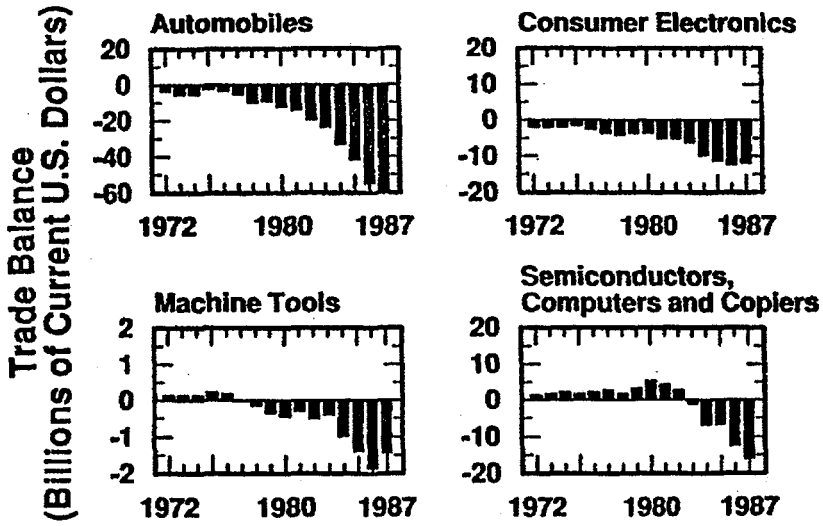


Figure E-1. U.S. Balance of Trade 1972-1987

Optimization techniques are used to drive emphasis at the subsystem and component levels. The systems approach recognizes that most reliability problems involve decision-making under uncertainty. Decisions are evaluated in terms of their effects on system performance. The *Challenger* accident illustrates some of these principles.

The National Research Council's (NRC's) evaluation of NASA's safety analysis of the *Challenger* emphasized three critical flaws. First, NASA relied heavily on subjective judgment rather than risk analysis. Second, NASA lacked a well-defined objective method by which to sort significant from trivial issues. Finally, no systematic or objective criteria were developed to judge the adequacy of waiver rationales. The NRC made three recommendations for improvements to NASA's safety analysis. First, NASA should adopt the methods of **probabilistic risk assessment (PRA)**. Second, NASA should strengthen their focus on risk assessments by incorporating **uncertainties.** Finally, NASA should put more emphasis on **systems** analyses. Thus the NRC review of the space shuttle *Challenger* disaster identified the lack of a system-level reliability focus as a major contributing factor.

A system-level reliability focus is an integral part of system surety. The traditional academic approaches have included two primary schools of thought. The first is the normal accidents theory, exemplified by Perrow in his statement that ". . . serious accidents are nonetheless a 'normal' result or an integral characteristic of the system. Serious accidents in organizations managing hazardous technologies may be rare, but they are inevitable over time." The opposing school of thought specifies that " . . . serious accidents with hazardous technologies can [be] prevented through intelligent organizational design and management." The question to be addressed is whether this is the entire surety spectrum. Are these statements the theoretical boundaries of surety?

Certainly, there are successful reliability practices that can contribute to surety. Such practices include

- Emphasis on **simultaneous** (integrated) improvements in safety, reliability, and security
- Emphasis on system-level process to design in reliability and maintain it throughout the life of a structure
- Establishment of an organized data collection program

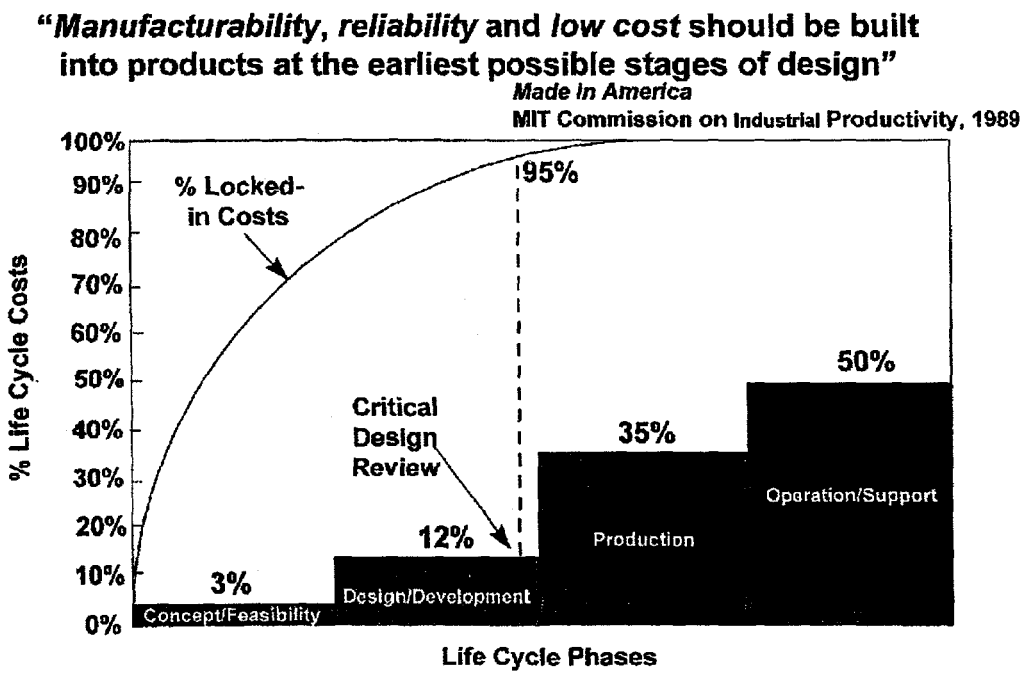


Figure E-2. Relationship Between the Costs of Project Life-Cycle Phases and Point in the Life-Cycle

- Use of modeling and simulation

One "best practice" identified by the MIT Commission on Industrial Productivity study is that "Manufacturability, reliability, and low cost should be built into products at the earliest possible stages of design." **Figure E-2** shows the relationship between the costs of specific project life-cycle phases and point in the life-cycle when project costs are locked in. At the critical design review, 95% of the entire project life-cycle costs have been determined. **Figure E-3** shows the influence of various project cost areas on total project costs. The earlier that reliability issues are considered, the more impact these issues can have on costs.

There are particular reliability issues that should be considered very early in the design process. Typical system reliability questions include

- What is the best allocation to meet a system reliability objective?
- What are the relative costs and

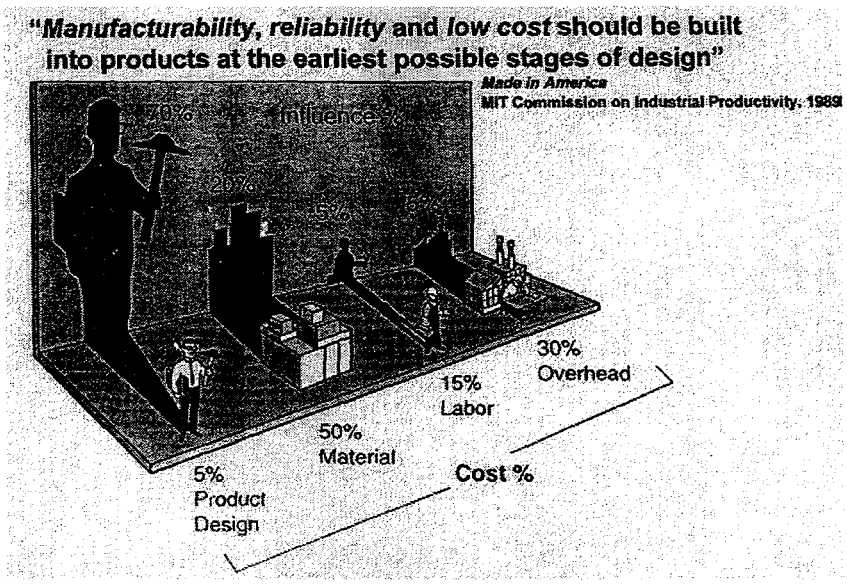


Figure E-3. Influence of Project Cost Areas on Total Project Costs

benefits of different design options?

- What is the best use for a limited test budget?
- How will warranty cost affect profitability?
- How will system reliability be affected by planned upgrades?
- What is the best spares inventory to improve availability?
- What is the best way to reduce maintenance costs?

This lecture addresses these reliability issues and their surety applications in six parts. Part 1 introduces reliability vocabulary and definitions, Part 2 lists some measures of reliability, and Part 3 discusses the reliability analysis process. Part 4 discusses designing for reliability, which includes reliability modeling and prediction. Part 5 provides some example problems and Part 6 discusses reliability-based predictive maintenance.

2. Theory and Principles

Just what is reliability? There are many definitions of reliability, each with at least one recognizable grain of relevance. A few examples include

- Dependability (*American Heritage*)
- "Conformance to requirements" (Phillip Crosby)
- "Minimum loss passed on to society" (Dr. Deming)
- "I may not be able to define it, but I know it when I see it!" (Justice Frankfurter)
- What the customer says it is! (In the final analysis, the most important definition of all.)

For the purposes of this discussion, however, reliability is defined as the **probability** that a system will perform its **intended function** adequately for a specified period of **time** under **stated conditions.** This definition contains four essential elements:

- **Probability**—reliability is a number between 0 and 1.
- **Intended function**—requires a clear definition of failure.
- **Time**—mission time over which system performance is evaluated.
- **Stated conditions**—operating conditions under which stated reliability is valid.

As an example of an application of this definition, the Ore bridge has a 98% probability of maintaining an allowable stress of 40,000 lb/in^2 for the next 50 years given a maximum anticipated stress of 25,000 lb/in^2. The essential elements include:

- **Probability**—98% probability
- **Intended function**—allowable stress of 40,000lb/in^2
- **Time**—50 years
- **Stated conditions**—anticipated stress of 25,000 lb/in^2

Is this example credible? Do we believe it? In fact, the " . . . expected reliability of most civil engineering systems will be in the range of 0.95 to 0.99," according to the *Reliability-Based Design in Civil Engineering*, 1987.

There are several important measures of reliability, most of which are tied to measures of system performance. The most significant of these measures include

- **Mean Time Between Failures (MTBF)**—defined as the average (operational) time a system

performs its intended function between failures. Commonly used in the analysis of repairable systems.

MTBF = operational time/# of failures

- **Mean Time To Failure (MTTF)**—for non-maintained systems, MTTF is a measure of the expected time a system is operable before it fails. This measure is often used for systems where repairs are not possible (e.g., light bulbs).

MTTF = operational time/# of failures

- **Mean Time to Repair (MTTR)**—the average time to correct a failure and return the system to its intended function. Used in the analysis of repairable systems. Sometimes referred to as *maintainability.*

MTTR = total repair time/# of failures

- **Availability**—the probability that a system can perform its intended function when required. Used in the analysis of repairable systems.

Availability = MTBF/(MTBF+MTTR)

- **Failure rate**—the failure rate λ over an interval of time T is defined as the number of failures per unit of time in that interval.

λ= # of failures/T = 1/MTBF

- **Cost**—the cost to maintain or repair a system. Other cost measures include warranty cost and life cost. Used for repairable and non-repairable systems.
- **Factor of Safety (FS)**—the Factor of Safety (FS) of a system is defined as

FS =C/D,

where C = Capacity of system, D = Demand.

- **Safety Margin (S)**—the Safety Margin (S) of a system is defined as

S = C–D.

- **Reliability Index**—reliability index β is defined as the number of standard deviations between the mean value of the safety margin and S = 0. That is,

$\beta = E(S)/\sigma(S)$

Examples of some of these measures are provided below. See also **Figure E-4**.

MTBF Example. Thirty units of a product are observed in the field for a period of one week. The units are operated continuously 24 hours a day, five days a week. During this time, eight failures are observed that are immediately repaired and the unit put back into operation. What is the MTBF of this product?

Solution: Recall, MTBF = operational time/# of failures

Operational time is 30(24x5)=30x120=3600 hr.

Thus,

MTBF = 3600/8 = 450 hr.

MTTF Example. Assume the eight failures in the previous example are not repaired, and the failed units are taken out of operation and not replaced. The times to failure of the units that failed are 8, 16, 24, 40, 56, 72, 88, and 104 hr. What is the MTTF of the system?

Solution: Recall, MTTF = operational time/# of failures

The operation time is $\Sigma t_f + (N-n_f) T$,

where

t_f is the time to failure for the individual units,
N is the total number of units,
n_f is the number of failed units,
and
T is the total time.

Thus, operation time

=(8+16+24+40+56+72+88+104)+(30–8)120
=(408+2640)
=3048

So,

MTTF
$= (\Sigma t_f + (N - n_f)T)/ n_f$
= 3048/8
= 381 hr.

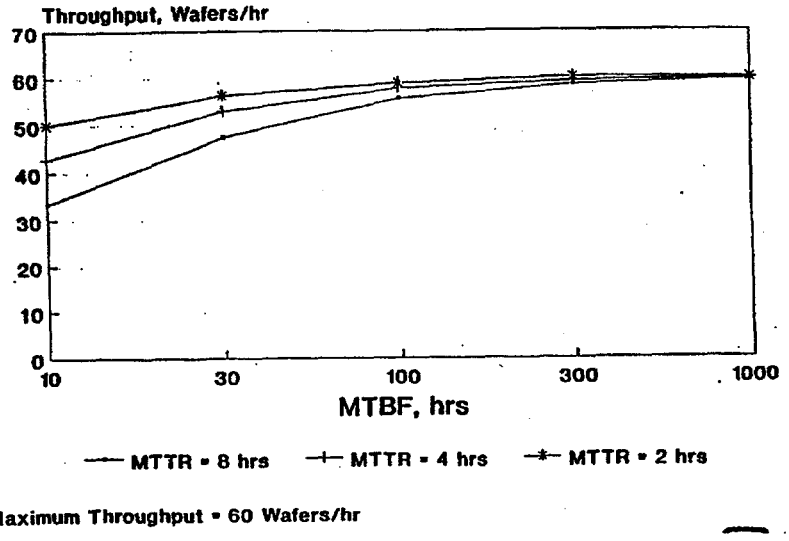


Figure E-4. MTBF Plotted Against Hourly Throughput in a Wafer Facility for Three MTTRs

MTTR Example. a repairable system is operated for 350 hours during which five failures occur. Their repair times are 2, 1, 5, 3, and 4 hours. Estimate the system MTTR.

Recall, MTTR = total repair time/# of failures.

So,

$$\text{MTTR} = \frac{(2+1+5+3+4)\text{hours}}{5\text{ failures}} = 3\text{ hours}$$

Availability Example. A system has an MTBF of 200 hours and an MTTR of 5 hours. What is the system availability?

Recall,

Availability = MTBF/(MTBF+MTTR).

So,

$$\text{Availability} = \frac{200\text{ hours}}{(200+5)\text{hours}} = 0.9756$$

Factor of safety and safety margin example. The Ore bridge has a 98% probability of maintaining an allowable stress of 40,000 lb/in^2 for the next 50 years given a maximum anticipated stress of 25,000 lb/in^2. What is the factor of safety and safety margin for this bridge?

$$FS = C/D = 40{,}000/25{,}000 = 1.6$$

$$S = C–D = 40{,}000–25{,}000 = 15{,}000\text{ lb/in}^2$$

Failure rate example. A repairable system is operated for a period of 100 hours. During that time, five failures are observed that are immediately repaired and the system put back into operation. What is the failure rate and MTBF of the system?

$$\lambda = 5/50 = 0.05$$

$$\text{MTBF} = 1/\lambda = 100/5 = 20\text{ hr.}$$

Constant failure rate. If the failure rate (λ) can be approximated as constant over a time interval T, it can be shown that the reliability is

$$R(T) = e^{-\lambda T}$$

So, the probability of failure over time T is

$$Q(T) = 1 - R(T) = 1 - e^{-\lambda T}$$

See **Figure E-5.**

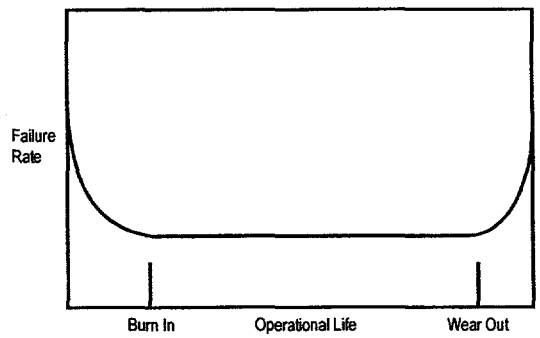


Figure E-5. Failure Rate Plotted Against Burn In, Operational Life, and Wear Out

There are five main steps involved in analyzing system reliability:

(1) Establish system requirements
- understand normal operation of system
- what are system requirements in terms of reliability?
- will system be modeled as a repairable or nonrepairable system?
- are there availability and maintainability issues?
- what measures of system performance will be used?

(2) Develop reliability model of system define system failure divide system into major subsystems
- identify failure mechanisms/modes
- develop high-level model of system

(3) Populate model with data (including uncertainties). Data sources include
- historical data
- generic industry failure rate data
- testing
- expert judgment from qualified and trained experts
- uncertainty is an enormous issue in reliability, which is discussed at some length below

(4) Execute model. **Figure E-6** below shows the importance of executing a reliability model in the reliability engineering cycle.

(5) Analyze model results. There are several important components of model analysis, including reliability prediction, sensitivity analyses, reliability improvement, uncertainty

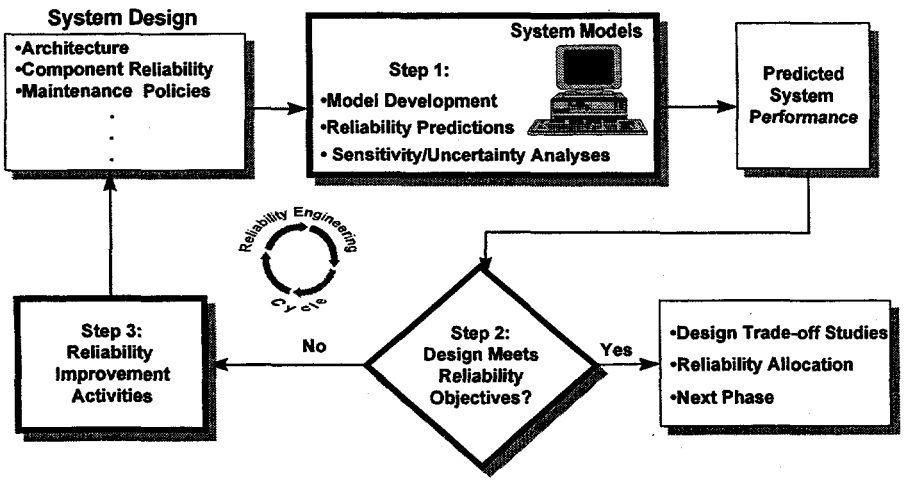


Figure E-6. Execute Reliability Model—Reliability Engineering Cycle

analyses, and optimization studies for design tradeoffs.

Reliability prediction. As an example of a reliability prediction, **Figure E-7** shows a histogram of the predicted MTBFs for a system.

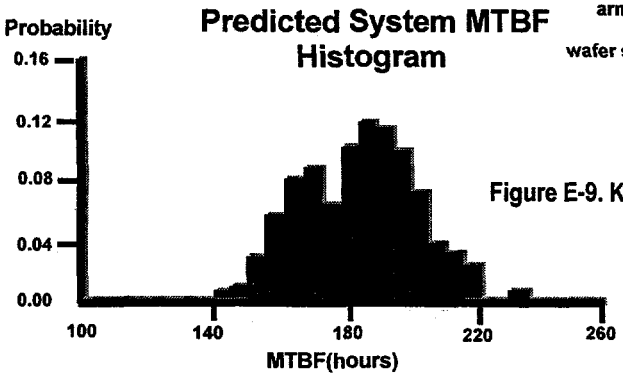


Figure E-7. Histogram of MTBFs

Sensitivity analyses. Figures E-8, E-9, and **E-10** illustrate the results of differently focused sensitivity analyses.

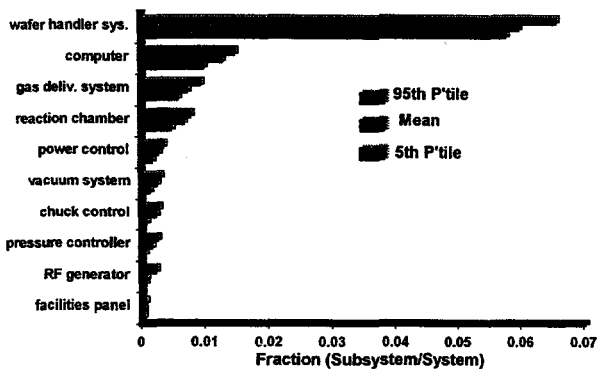


Figure E-8. Key Subsystem Contributors to System Failure

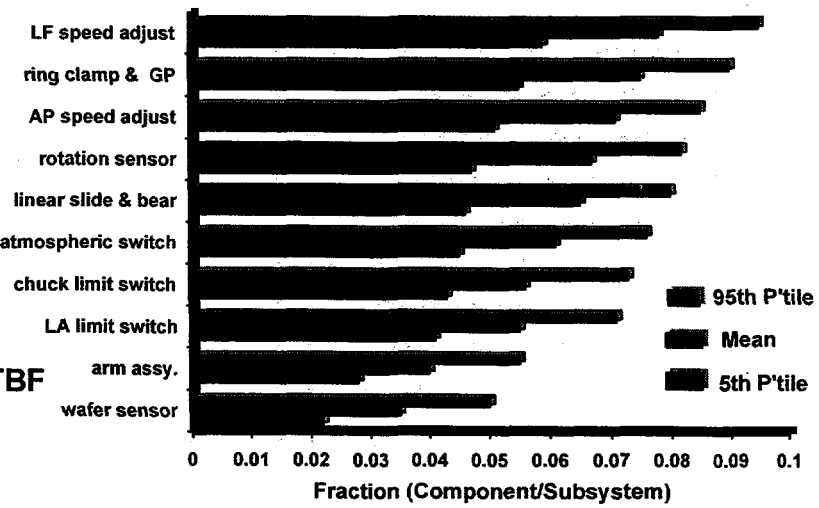


Figure E-9. Key Component Contributors to Subsystem (Wafer Handler) Failure

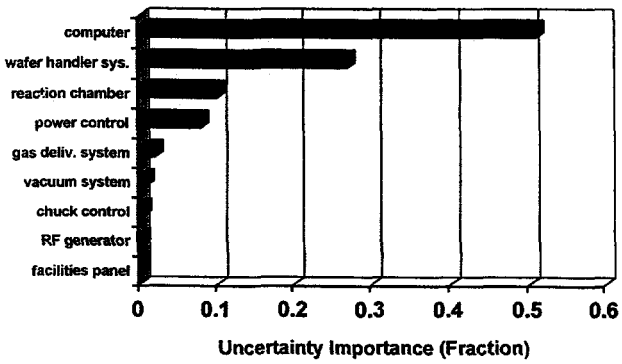


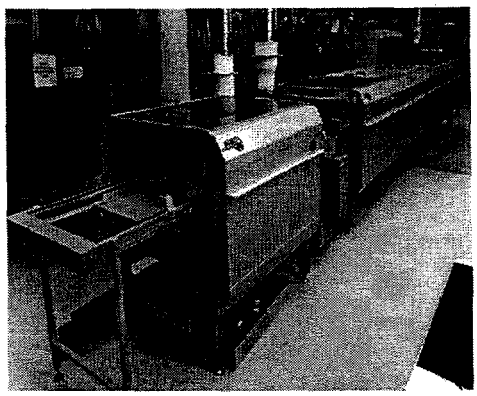
Figure E-10. Key Contributors to Uncertainty

Reliability improvement. Reliability allocation is an integral part of reliability improvement. Tools that may be used to improve reliability include:

- Equal apportionment technique
- Optimization techniques (such as GAs)
- The ARINC apportionment technique
- The AGREE allocation method–effort minimization algorithm
- Dynamic programming

Background

- **Manufacturer of solder equipment**
- **Company wanted to:**
  - **Increase reliability (150 hr MTBF target)**
  - **Increase availability (.90 target)**
  - **Decrease reliability-related costs**
- **Subject to equipment improvement budget ($40,000)**
- **Looking at 30 upgrades**



Wave Solder Machine

Figure E-11. Improved Reliability Problem at Manufacturing Facility

Optimal allocation is illustrated by the following example. A semiconductor equipment manufacturer is considering upgrades to various subsystems. There are 12 subsystems, with ten levels of upgrades for each subsystem. The system reliability (MTBF) target for the upgrade is 200 hours. To find the combination (allocation) that meets the target at minimal effort (cost), many variables must be considered. **Table E-1** shows the results of the complex computations.

Table E-1. Optimal Resource Allocation for Upgrade

Option Name	Level	Cost
Load Station	-	-
Central Vacuum	7	100
Controller	6	30
Power Distribution	3	15
Unload Station	5	70
Robot	-	-
Transfer Chamber	4	200
Chamber	3	200
Chamber Vacuum	7	100
TCU	7	300
Gas Distribution	8	80
RF Plasma	4	80
		1175

Another example of an effort to improve the reliability of a manufacturing facility is described in **Figure E-11**. The results of this effort are shown in **Table E-2**.

Table E-2. Optimal Solution vs. Baseline for Improved Reliability at Manufacturing Facility

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

Uncertainty analyses. Dealing with uncertainty and variability is one of the most important challenges of the reliability analysis process.

> It can be seen that the reliability of ... a system is known with certainty after it has been used until it is worn out and its failure history has been faithfully recorded. But, for purposes of doing anything about the reliability of this equipment, this knowledge has no value. Before this point, reliability cannot be known with certainty (*emphasis added*) (MIL-HDBK-217E).

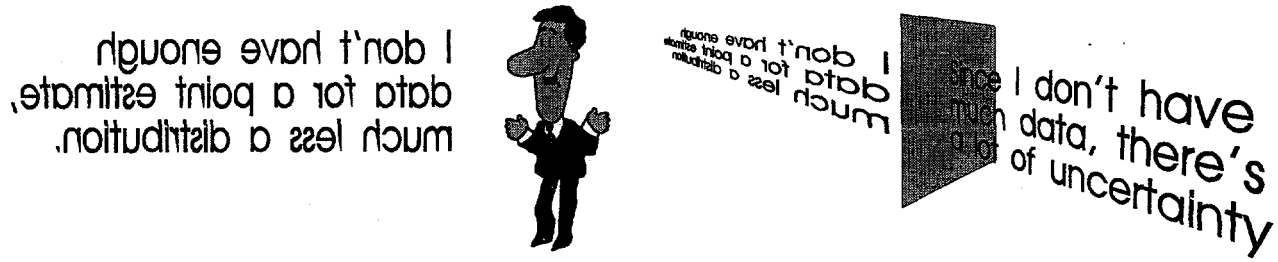


Figure E-12. (Left) The Data Dilemma. (Right) The Flip Side of the Uncertainty Coin

Uncertainty must be considered in any reliability analysis. Rather than succumbing to the data dilemma, the reliability analyst will turn the argument around (**Figure E-12**).

There are unfortunate consequences of failing to analyze the uncertainty of a project. Understating reliability as a consequence of ignoring uncertainty can lead to unimpressive advertising and initial bids lost to the competition. Overstating reliability as a result of failing to analyze uncertainty can lead to a multitude of dire consequences, including:

- False advertising
- Unrealistic customer expectations
- Unpleasant surprises
- Unexpected maintenance costs
- Lost repeat business
- Diminished corporate reputation

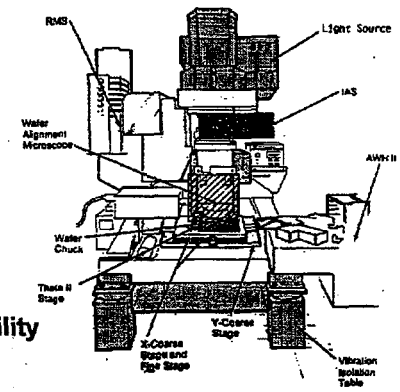
The sources of uncertainty include:

- Variability from system to system
- Uncertainty in failure rates
- Natural (stochastic) variability in system
- Uncertainty in modeling results

Optimization studies for design tradeoffs—Figures E-13, E-14, and **E-15** and **Table E-3** also show the importance of appropriate resource allocation in improving reliability. This example follows a semiconductor manufacturing facility's problems with its spares kit.

Background

- **Semiconductor equipment manufacturer (steppers)**
- **Only a few customers bought recommended spares kits**
- **Some customers considered recommended kit too expensive**
- **Recommended spares kit was not directly based on equipment reliability**



Stepper

Figure E-13. Importance of Resource Allocation to Improving the Reliability of Spares Kit Within a Semiconductor Manufacturing Facility

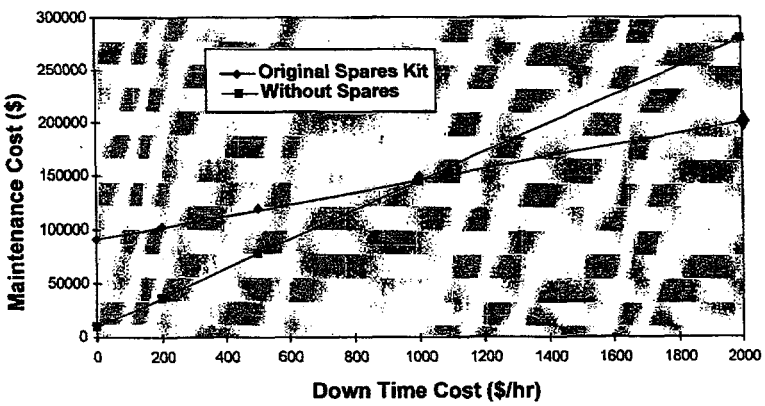


Figure E-14. Importance of Resource Allocation to Improving the Reliability of Spares Kit Within a Semiconductor Manufacturing Facility

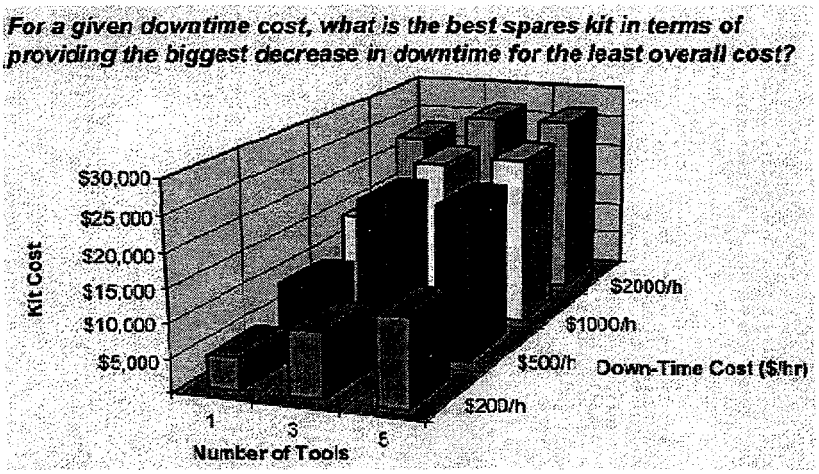


Figure E-15. Importance of Resource Allocation to Improving the Reliability of Spares Kit Within a Semiconductor Manufacturing Facility

Table E-3. Importance of Resource Allocation to Improving the Reliability of Spares Kit Within a Semiconductor Manufacturing Facility

Budget	$X	$4X	$10X	$20X
Robot Assembly			1	2
Robot Arm Assembly				1
Assembly, Optical Encoder Card		1	1	1
Assembly, Control Display Module	1	2	2	2
Assembly, VTS Fan	2	1	1	1
Power, Supply, Converter, DC-DC	2	1	1	1
Assembly, PCB MCC4, MTR-5		2	2	2
Assembly, Harmonic Drive Motor, <100 Arc Sec	1	1	2	2
Coupling Rework	1	1	1	1
Assembly, Brake	1	1	1	1
Kit, Misc., VT5/MT5, New Ballscrew		1	1	1
Assembly, Z-Axis Motor	1	1	2	2
Down Time Reduction (0/0)	26	40	65	80

3. Applications

Several real-world applications of reliability theory and principles have been cited previously to illustrate the concepts presented. In designing for reliability, both the techniques and technologies of reliability modeling and prediction are used to resolve reliability issues before they occur. This premise is well stated in MIL-HDBK 217.

> . . . considering the various stages back through production, development, installation, shipment, . . . etc., less and less can be known with certainty about reliability. However, what is known or predicted becomes more and more valuable as a basis for taking action. After all, there is no value in simply knowing that a certain failure will occur at some specific time in the future. The value comes in having the opportunity to do something to prevent the failure from occurring . . . *Thus, prediction becomes part of the process of 'designing the future.'*

Reliability modeling is making contributions to engineers and designers in a great number of fields. A sampling of the varied applications includes nuclear power plants, the semiconductor industry, the solar industry, the *USS Iowa* investigation, the machine tool industry, the medical industry, weapons systems, transportation systems, the airline industry, nuclear waste repositories, and the automotive industry.

In the semiconductor industry, technologies are changing very quickly.

Background

- **Semiconductor equipment manufacturer**
- **Considering new design based on:**
  - **Performance improvements**
  - **New technology**
  - **Market potential**
- **Predict performance of new design**
  - **Identify potential problem areas**
  - **Suggest improvements**
  - **Predict equipment reliability**

Figure E-16. Reliability Prediction of New Equipment Design

Figure E-16 describes the design problems faced by an equipment manufacturer.

The reliability tools that the engineer can apply to this problem are numerous. Baselines will be determined and system performance will be predicted and observed. **Figure E-17** shows a chart that depicts this approach.

Calculational tools, whether specialized programs like the Sandia-developed software shown in **Figure E-18** or more general mathematical and engineering products, greatly enhance reliability engineering calculations, analysis, and modeling. **Figure E-19** shows other methods of modeling reliability. Fault trees and block diagrams for series and parallel systems are illustrated in **Figure E-20**.

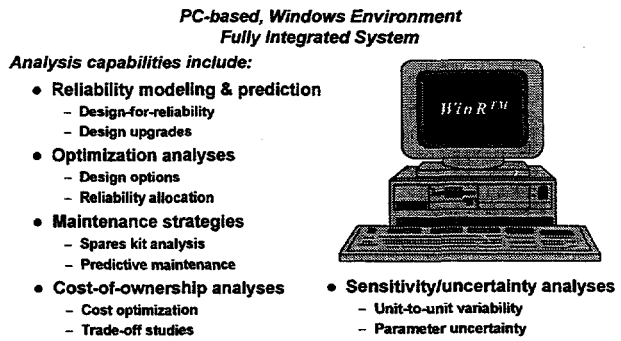
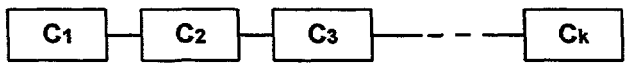


Figure E-18. Capabilities of Optimization Software



In a series system, failure of any subsystem or component results in

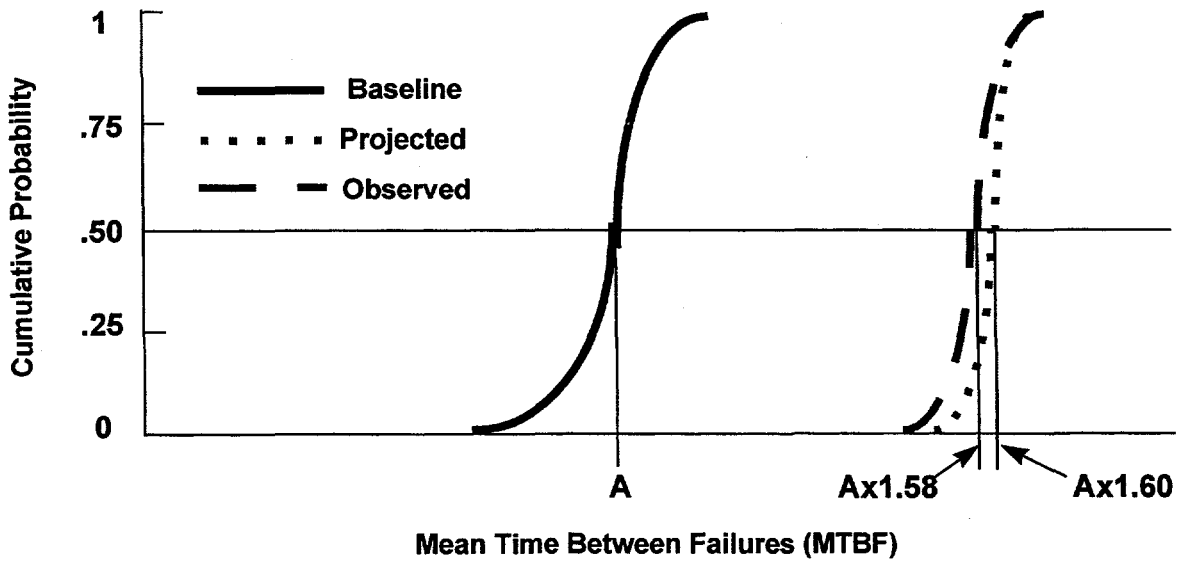


Figure E-17. Projected vs. Observed Performance

- **Fault Trees**
  - "Top-down" approach
  - Identify most likely failure paths
  - Isolate specific failures
- **Block Diagrams**
  - Shows functional relationships
  - Provides clear picture
  - Used to create mathematical model
- **Markov Models**
  - System modeled as states
  - Dynamic modeling
  - Difficult if large # of states

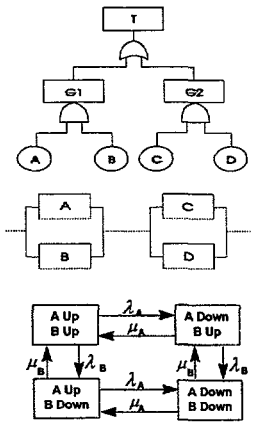


Figure E-19. Methods of Modeling Reliability

failure of the system.

Let E_i=event that I operates successfully over time interval T

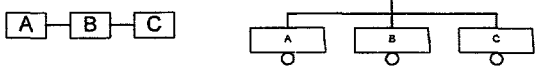
$R_i = P(E_i)$ = Reliability of I
R_s = System Reliability

Then

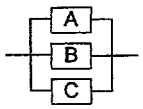
$$R_s=P(E_S)+P(E_1 \cap E_2 \cap E_3 \cap E_k)$$

Block Diagrams & Fault Trees

Series = OR



Parallel = AND



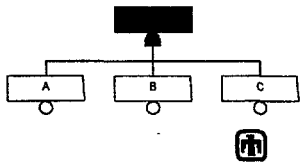
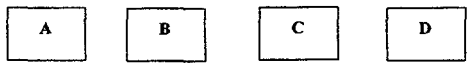


Figure E-20. Block Diagrams and Fault Trees

Assuming independence

$$R_s=P(E_1)P(E_2)P(E_3)\ldots P(E_k)= R_1R_2R_3\ldots R_k$$

The following example shows how to calculate the reliability of a series system, using the component reliabilities shown.



If $R_A = 0.99$, $R_B = 0.95$, $R_C = 0.70$, and $R_D = 0.95$,

then $R_S = R_AR_BR_CR_D = 0.63$.

Suppose a series system has n subsystems with identical failure probability q. Then,

$$R_S = (1-q)^n \approx 1-nq$$

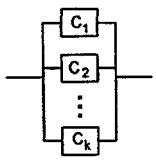
This approximation is accurate to two decimal places when nq = 0.1

Example: If we want R_S = 0.99999 in a system with 20 components, then

0.99999 = 1-20(q)
q = 0.0000005
R = 0.9999995 for each subsystem

Unlike the series system, a parallel system does not fail unless all components fail.

Let W_i = event that component i fails
Q_s = system failure probability
Then
$Q_s = P(W_1 \cap W_2 \cap W_3 \cap \ldots \cap W_k)$
Since Q = 1-R



$$R_s=1-Q_s=1-\prod_{i=1}^{k}(1-R_i)$$

Assuming independence

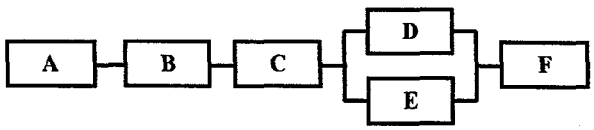
$$Q_s=P(W_1)P(W_2)..=\prod_{i=1,k} Q_i$$

On the surface, it may look as though a parallel system would always be more reliable than a series system.

However, redundancy, which is the core of parallel systems, can create more surety problems than it resolves.

Overreliance on redundancy can result in three specific problems. First, the concept of keeping a design as simple as possible is violated. Next, common-cause failures can defeat redundancy. For example, in 1975 at the Brown's Ferry nuclear power plant, a fire burned uncontrolled for nearly eight hours. One of two power reactors was dangerously out of control for several hours. Emergency safety devices failed because fore destroyed redundant electrical power and control systems. Finally, reliance on safety factors can be dangerous, as exemplified by the space shuttle *Challenger* disaster. A safety factor of 3 was chosen for the infamous O-rings. It was thought that if the first O-ring failed, the secondary one would seal. Unfortunately, failure of the primary O-ring led to the failure of the secondary O-ring.

Combined series and parallel systems can offer high reliability. For example,



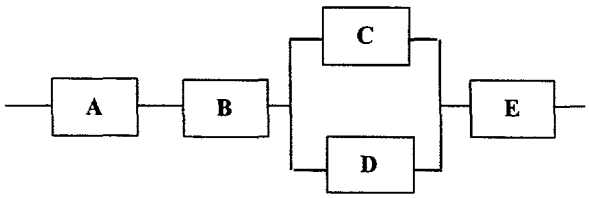
System fails if A, B, C, both D and E, or F fails. That is

$$Q_S = P[A \cup B \cup C \cup (D \cap E) \cup F]$$

Define **minimal cut sets** as all (smallest) combinations of component failures that can cause system failure. Then the minimal cut sets are:

A, B, C, DE, and F.

The following example calculates the reliability of a series/parallel system, using the indicated component reliabilities.



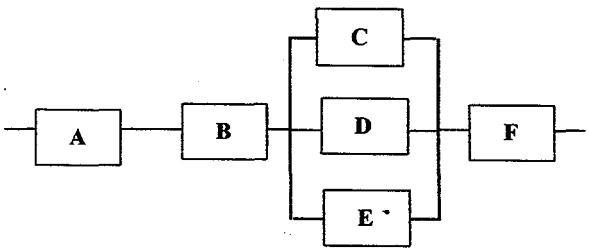
If

$R_A = 0.99$, $R_B = 0.95$, $R_C = 0.70$, $R_D = 0.70$, and $R_E = 0.95$,

then

$$R_S = R_A R_B R_{CD} R_E = R_A R_B [1-(1-R_C)(1-R_D)] R_E$$
$$= 0.99 \times 0.95 \times [1-(1-.7)(1-.7)] \times 0.95 = 0.81$$

Another example of a reliability calculation for a series/parallel system is presented below.



If

$R_A = 0.99$, $R_B = 0.95$, $R_C = 0.70$, $R_D = 0.70$, $R_E = 0.70$, and $R_F = 0.95$,

then

$$R_S = R_A R_B R_{CDE} R_F$$
$$= .87.$$

If a fourth redundant component of the same reliability is added, $R_S = .89$.

The effects of adding additional redundant components to parallel series are shown in **Figure E-21**.

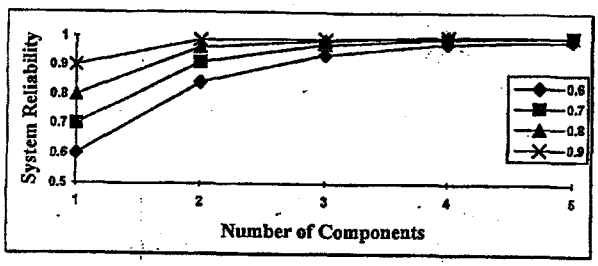


Figure E-21. The Reliability of a Parallel System as a Function of the Number of Components

4. Summary

This chapter is best summarized by working a demonstration problem that incorporates many of the concepts previously discussed. The following example problem assesses the reliability of three different designs.

It is estimated that the minimum column load to be supported on piles for a structure is 50,000 lb. The maximum load is estimated at 100,000 lb., and the average load is 70,000 lb. Three different pile configurations are being considered:

(1) One 100,000-lb capacity

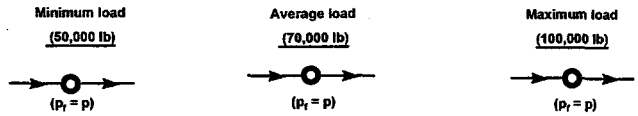
(2) Two 50,000-lb capacity

(3) 35,000-lb capacity

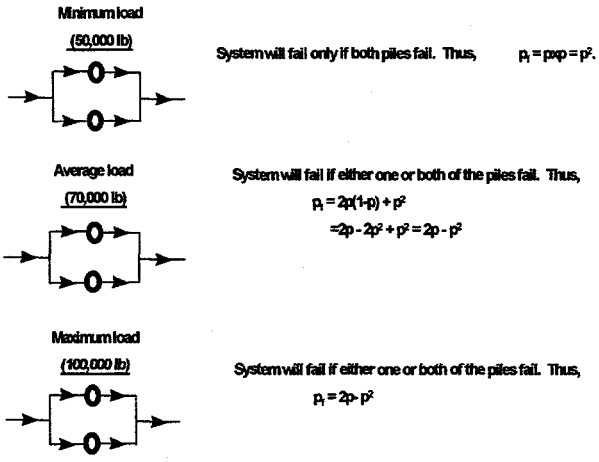
To consider the reliability of each design for each of three models, it is assumed that all piles are equally reliable and that cost is not a factor.

One 100,000-lb Capacity Pile Configuration:

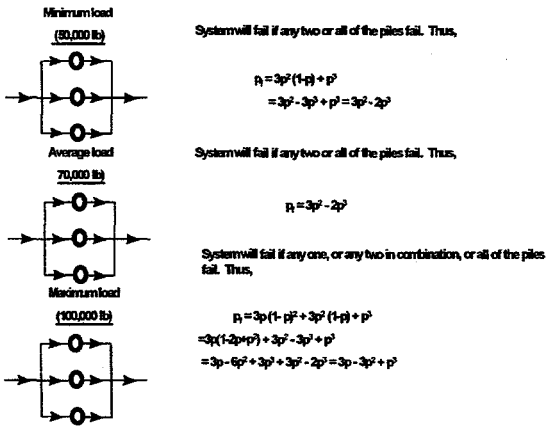
Let $p_f = p$ be the probability of failure for each pile. Then for a one 100,000-lb capacity pile configuration, the system will fail under each load only if the 100,000-lb capacity pile fails. Thus,



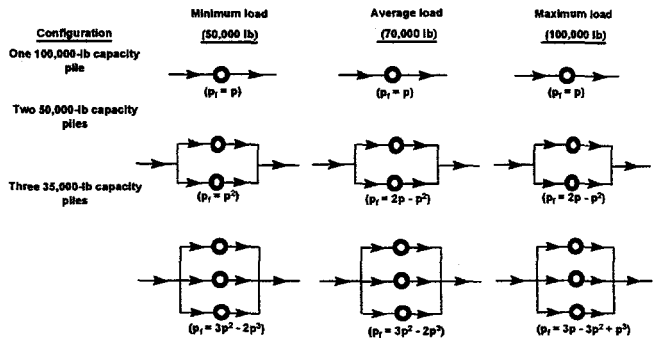
Two 50,000-lb Capacity Pile Configuration:



Three 35,000-lb Capacity Pile Configuration:



Solution:



What is the best design?

- For the maximum load (100,000 lb.), the best design is 2/50,000. (Note that 3/35,000 is better than 1/100,000 if $0<p<.5$.)
- For the average load (70,000 lb.), 1/100,000 is the best design if $.5<p<1$. Otherwise, 3/35,000 is the best design.
- For the maximum load (100,000 lb.), the best design is 1/100,000. 2/50,000 is better than 3/35,000.

5. Further Reading

A. H.-S. Ang and H.-F. Ma, *On the Reliability of Structural Systems*, Third International Conference on Structural Safety and Reliability, 1981.

Milton E. Harr, *Reliability-Based Design in Civil Engineering.* McGraw-Hill, New York, 1987.

Steve Hoffman, Enhancing Power Grid Reliability, in *EPRI Journal*, pp. 6-16, November/December 1996.

Charles W. Lockhart and William J. Roberds, Worth the Risk?, in *Civil Engineering*, pp. 62-64, April 1996.

Taylor Moore, Tighter Security for Electronic Information, in *EPRI Journal*, pp. 17-21, November/December 1996.

Priscilla Nelson, The National Science Foundation's Focus on Infrastructure Research, presented at the Geosynthetic Research Institute Conference, Drexel University, Philadelphia, PA, December 12-13, 1995.

Henry Petroski, *To Engineer is Human.* St. Martin's Press, New York, 1985.

Proceedings of Specialty Conference: Probabilistic Mechanics & Structural Reliability, American Society of Civil Engineers, Reston, VA, 1996.

Scott Sagan, *The Limits of Safety.* Princeton University Press, Princeton, NJ, 1993.

Scientist urges infrastructure repairs, *(Worcester, MA) Telegram & Gazette,* August 8, 1996.

Palle Thoft-Christensen, *Application of Structural Systems Reliability Theory,* Springer-Verlag, New York, 1986.

Appendix F

Risk Management

Objectives

The objectives of this lecture, presented by Allen Camp of Sandia National Laboratories on March 10, 1997, are to:

- Understand basic risk concepts
- Learn a limited amount of probability theory
- Discuss different risk assessment tools
- Understand fault tree analysis
- Understand quantification processes and results presentation
- Learn about possible uses of risk assessment

This lecture serves as an introduction to the theory, tools, techniques, and actual and potential uses of risk assessment. This technology has broad application to infrastructure design.

1. Introduction

Probabilistic risk assessment is used to determine the susceptibility of a system or set of systems to the occurrence of events that could lead to the failure of the system. The tools of probabilistic risk assessment include Venn diagrams, fault trees, event trees, computer modeling, simulation, and various other mathematical and calculational techniques. According to the *Probabilistic Risk Assessment Procedures Guide* (NUREG/CR-2300), system modeling techniques used in probabilistic risk assessment should:

- Be capable of predicting the unavailability of complex systems in a manner that can be employed by a variety of practitioners
- Be proceduralized to the extent that it can be used for a wide variety of systems in a manner that is traceable, repeatable, and verifiable
- Provide reasonable assurance of completeness
- Enhance understanding, communication, and the use of results
- Produce a model that promotes understanding of the principal ways in which the system can fail and the way in which failures can be prevented or their impacts reduced

While these requirements were written to describe the risk concerns of nuclear facilities, they are just as applicable to other infrastructure systems. Today's design professionals will

benefit by adding the tools of probabilistic risk assessment to their portfolios.

2. Theory and Principles

Before risk can be assessed, it must be defined. For the purposes of probabilistic risk assessment, **risk** is the frequency with which a given set of consequences would be expected to occur. Examples of risk statements that illustrate this definition include:

- The risk of cancer death is 2E-3/yr
- The risk of a dam failure killing more than 1000 people is 0.02/yr
- The risk of a nuclear reactor meltdown is 1E-4/yr/plant

In discussions of probabilistic risk assessment, **risk** usually refers to **consequence-weighted risk,** the product of an event's frequency and its consequence. Thus,

Risk = Frequency x Consequence

Consequence-weighted risk is summed over possible scenarios, as shown in **Table F-1**.

Table F-1. Determining Consequence-Weighted Risk

Accident Scenario	Estimated Frequency (acc./yr)	Estimated Consequences (deaths/acc.)	Consequence-Weighted Risk (deaths/yr)
S_1	2.0×10^{-5}	1	2.0×10^{-5}
S_2	0.2×10^{-5}	3	0.6×10^{-5}
S_3	0.6×10^{-5}	7	4.2×10^{-5}
S_4	0.3×10^{-5}	5	1.5×10^{-5}
Total	3.1×10^{-5}		8.3×10^{-5}

To quantify risk, consequence measures must be identified. Consequence measures are problem-specific and can include:

- Fatalities
- Injuries
- Cancers
- Cleanup costs
- Lost production time
- Environmental damage

Risks can be separated into those affecting the facility and workers as opposed to those affecting the public.

Risks can also be distinguished by whether or not they are voluntary. **Voluntary risks** are those which we choose to accept with at least some knowledge or understanding of the hazards, such as:

- Driving a car
- Working in a coal mine
- Skydiving

Involuntary risks are those that are imposed upon us without our consent, such as:

- Storage of hazardous chemicals
- Transportation of nuclear weapons
- Food additives

Voluntary and involuntary risks can not be directly compared in decision-making.

People will accept much higher levels of voluntary risk.

Now that risk has been discussed, the definition of probabilistic risk assessment can be presented. **Probabilistic risk assessment (PRA)** is the systematic process of:

- Identifying possible undesirable events

- Estimating the frequencies of such events
- Estimating the consequences of such events

Another way of describing PRA is to say that it answers the following three questions:

- What is possible?
- How likely is it?
- What are the consequences?

Risk assessment considers the combined response of hardware, software, and humans to potential system challenges. **Figure F-1** illustrates this concept.

Probability theory involves determining the likelihood of a particular occurrence. The basic terminology of probability theory includes the following terms:

- **Sample space**—set that contains all possible outcomes
- **Random variable**—a quantity with a value determined by the outcome of a probability experiment
- **Event**—any element of the sample space
- **Complement**—all of the outcomes not contained in the event
- **Independent**—the probability of an event is not affected by the occurrence of another event
- **Dependent**—the probability of an event varies depending on the occurrence of another event
- **Mutually exclusive**—the occurrence of one event precludes the occurrence of another

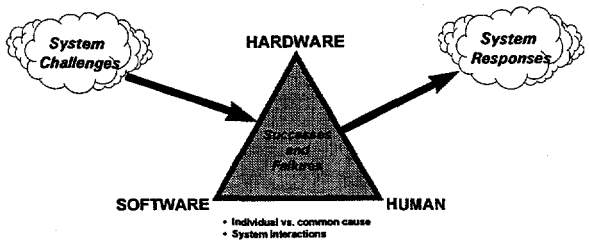


Figure F-1. Evaluation of Combined System Response

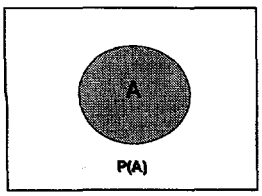
Venn diagrams are one method of describing these probability relationships. **Figure F-2** shows five simple Venn diagrams.

A variety of risk-assessment tools are available, depending on the complexity of the problem. There are simple methods, such as:

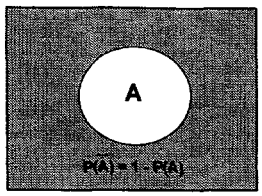
- Checklists
- Hazards analysis
- Failure modes and effects analysis

There are also more complex methods available, such as:

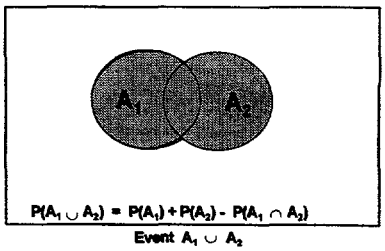
- Event trees
- Fault trees
- Other logic-based diagrams
  - neural networks
  - decision trees
  - influence diagrams
- There is no single technique that is suitable for every analysis, so the designer who is serious about risk management must be able to apply the correct tool to each problem. Now that the student is familiar with the basic terminology and techniques of PRA, it is appropriate to examine some applications of these tools.



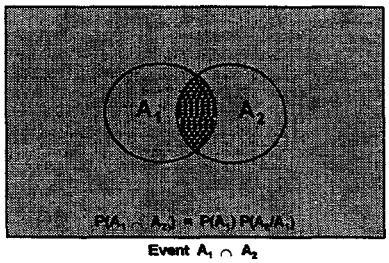
a. Venn Diagram Showing the Probability That Event A Will Occur



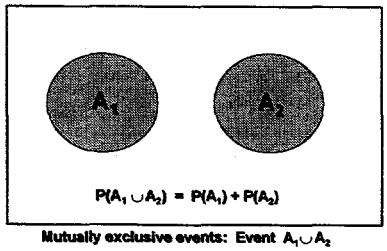
b. Venn Diagram Showing the Probability That Event A Will Not Occur



c. Venn Diagram Showing the Probability That Event A_1 or Event A_2 Will Occur



d. Venn Diagram Showing the Probability That Event A_1 and Event A_2 Will Occur



e. Venn Diagram Showing Event A_1 and Event A_2 as Mutually Exclusive Events

Figure F-2. Samples of Venn Diagrams

3. Applications

For identification of hazards within or to a facility or process. Hazards to be example, a Hazards/HAZOPS analysis is a commonly performed risk assessment analysis. It involves a systematic identified and assessed may include chemical, fire, tornado, etc. The analysis is based on design information and involves a preliminary examination and categorization of the hazard under study. Often, a HAZOPS analysis provides a starting point for more detailed risk assessments.

Another frequently employed analysis is the Failure Modes and Effects Analysis (FMEA). **Table F-2** is a simplified FMEA table that shows the elements of this kind of analysis.

Table F-2. Simplified Sample Failure Modes and Effects Analysis Table

Component	Failure mode	Effects
Pipe	Leak	Loss of system pressure; spray electrical equipment
	Rupture	Loss of fluid; spray electrical equipment; mechanical pipe whip
Valve	Valve body rupture	Same as pipe rupture
	Fails to open	Coolant not delivered
	Fails to remain open	Coolant flow interrupted

NOTE: Actual FMEA tables should be specific and detailed

Another type of analysis is the screening or bounding analysis. The purposes of this type of analysis are to eliminate hazards from consideration, develop a conservative basis for design, and identify areas for more detailed study. There are a number of ways that a hazard may be eliminated from consideration, including:

- Absence of the hazard—for example, a pipeline accident need not be considered if there is no pipeline involved in the system.
- Physical limits—for example, a toxic release need not be considered if the quantity of material is below a hazardous threshold.
- Bounded by other hazards within design basis—for example, if the effects of tornadoes have been considered, it is not necessary to also include thunderstorm effects.
- Low probability of occurrence—for example, the effects of a meteorite may be eliminated from consideration as the occurrence of a meteorite is highly unlikely.

The following example works through a bounding analysis for aircraft impact. The example has been simplified for purposes of illustration.

The defined problem is to determine the frequency of aircraft impacts on structures near an airport.

$$Fk = \sum_i \sum_j N_{ij} \lambda_j d_j \frac{A_{kj}}{A_{pj}}$$

where

N_{ij} = number of aircraft of type j along airway i

λ_j = crash rate of aircraft type j

d_j = distance traveled by aircraft where site is within striking distance

A_{kj} = crash area of the structure

A_{pj} = area where aircraft may crash

Then determine the wall thickness necessary to prevent failure from a given impact.

$$T = 2.47 \frac{w^{0.4} v^{0.67}}{d^{0.2} f_c^{0.4}}$$

w = weight of missile

v = velocity of missile

d = effective missile diameter

f_c = ultimate strength of concrete

A_c = contact area of missile

Data for the equations are available from several sources, including:

- Local airports
- FAA Statistical Handbook on Aviation
- Annual Review of Airport Accident Rates (NTSB)

Determine the frequency of crashes that could cause failure and determine if the frequency is acceptable; if not, relocate or strengthen.

More detailed analyses are possible. **Figure F-3** shows a structural response and fragility analysis, for example.

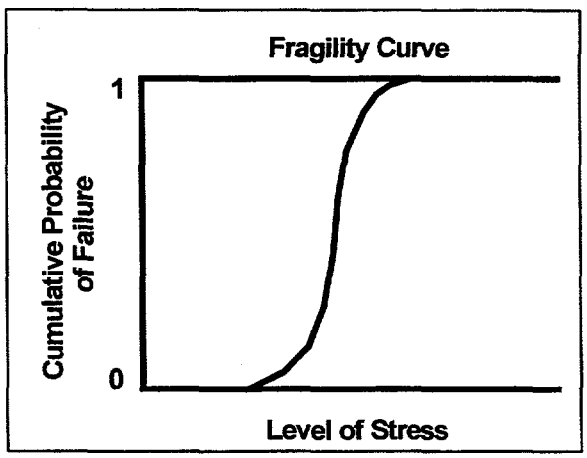


Figure F-3. Structural Response and Fragility Analysis

Event trees are another available method for assessing risk. This logic model is well suited for treating sequences of events. **Figure F-4** shows a power outage event tree. Models can be developed for each event on the tree.

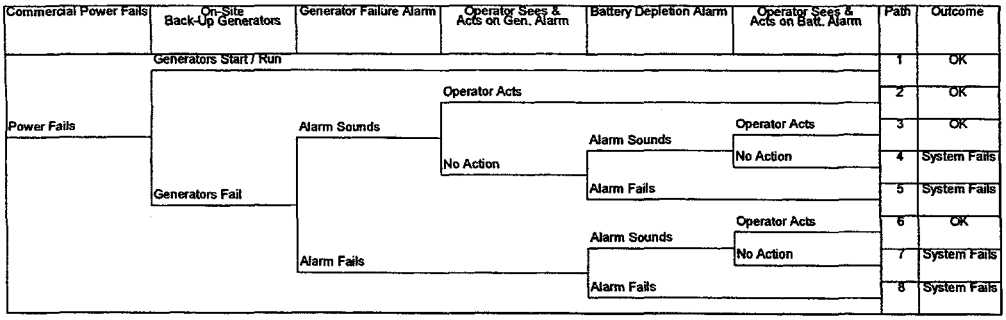


Figure F-4. Power Outage Event Tree Showing Eight Paths

Fault trees are another very useful tool in risk assessment. The best single book we know of for describing the **how** and **why** of fault tree analysis is the *Fault Tree Handbook*. This book holds everything you need to know about fault tree analysis, one of the most important risk assessment techniques available. The following brief introduction to fault tree analysis is intended to whet the appetite.

What is a fault tree? A **fault tree** is a diagram that graphically and logically depicts the interrelationships of elementary events that lead to an undesired event (called the "top event" of the fault tree). **Figure F-5** shows a plan drawing of a system and a fault tree of the same system.

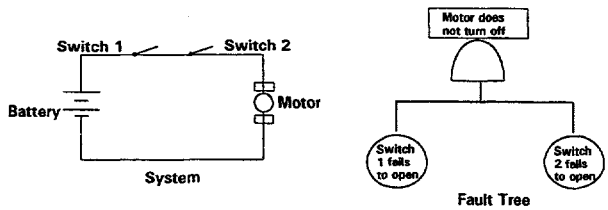


Figure F-5. System and Fault Tree Representation of System

The two major activities in fault tree analysis are constructing the fault tree and then evaluating it. Constructing a fault tree involves developing a graphical representation of the failure to be modeled. Symbols are used in these fault tree models. There is a well-defined thought process for constructing a fault tree, which will be introduced as we work examples. There are a number of software packages that are available to aid in building fault trees.

Evaluating the fault tree involves mathematically evaluating the system to determine the primary causes of system failure. This evaluation may be quantitative or qualitative. Again, there are software packages available to help you perform the evaluation. Fault tree evaluation will include determining which events drive the results, which will involve evaluating the fault tree uncertainty and importance measures.

There are many types of failures that are well modeled by fault trees. Some of these failures include:

- Component failure on demand
- Component failure to run
- Structural failure
- Test or maintenance unavailability
- Dependent failure
- Human error of omission
- Human error of commission

Fault trees are constructed using symbols to represent the occurrence of various events that may contribute to an undesired outcome. The primary event symbols are shown in **Figure F-6**. **Figure F-7** shows the fault tree gate symbols, and **Figure F-8** illustrates a number of miscellaneous symbols used in fault tree analysis.

Basic Event (BE) — An initiating fault requiring no further development

Undeveloped Event (UE) — An event which is not further developed either because it is of insufficient consequence or because information is unavailable

Developed Event (DE) — An event that could be further developed or is developed elsewhere but is treated here as a primary event

External Event (EE) — An event that is normally expected to occur (usually an event having probability of 1 or 0)

Figure F-6. Primary Event Symbols for Fault Trees

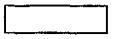
"AND" Gate — Output fault occurs if all of the input faults occur

"OR" Gate — Output fault occurs if at least one of the input faults occurs

"Exclusive OR" Gate — Output fault occurs if exactly one of the input faults occurs

"Priority AND" Gate — Output fault occurs if all of the input faults occur in a specific sequence (the sequence is represented by a CONDITIONING EVENT drawn to the right of the gate)

Figure F-7. Gate Symbols for Fault Trees



Description — Contains the description of an event

Transfer — Indicates that the tree is developed further at the occurrence of the corresponding TRANSFER OUT (usually on another page)

Transfer Out — Indicates that this portion of the tree must be attached at the corresponding TRANSFER IN

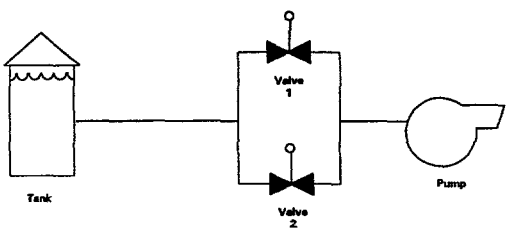
Figure F-8. Miscellaneous Symbols for Fault Trees

Figure F-9 uses these symbols in a fault tree representation of a pump system.

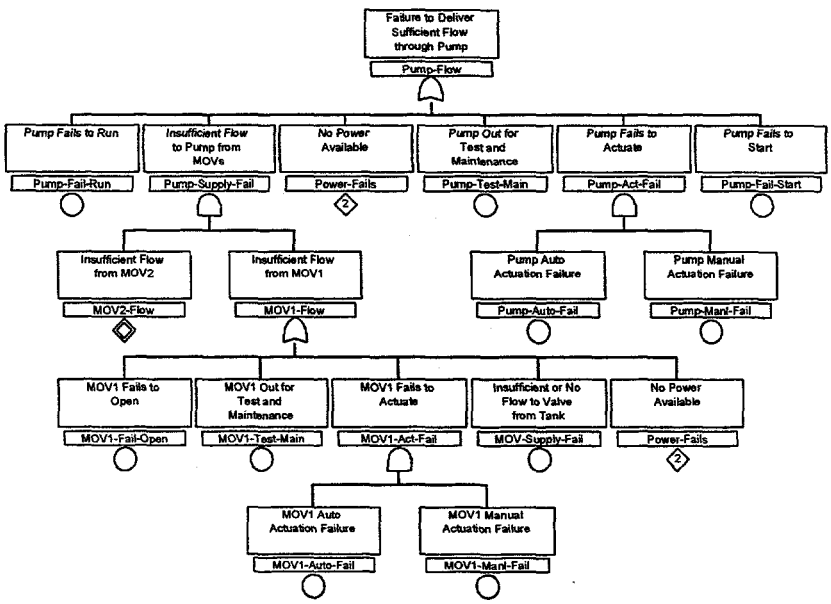
Another very significant concept associated with fault trees is that of minimal cut sets. A **minimal cut set** is the smallest combination of primary events sufficient for the top event. Another way to think about this is that a **minimal cut set** for the top event of a fault tree is a smallest set of primary events that must all occur in order for that event to occur. For example,

TOP EVENT = A + B * C (two cut sets)

WARNING: Cut sets containing complement events may not be



a. Pump System



b. Fault Tree

Figure F-9. Pump System/Fault Tree Example

minimal! For example,

$$A*C + A*C' = A*(C + C') = A$$

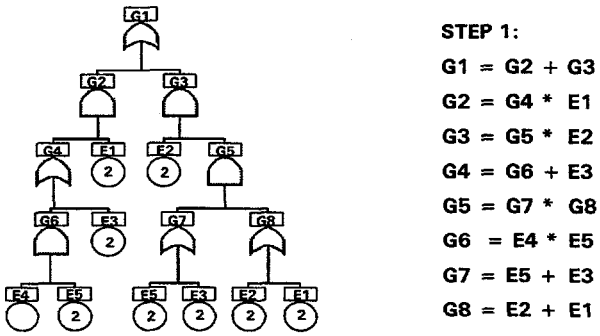
A process for determining minimal cuts sets is:

- Step 1—generate the intermediate event equations for the fault tree
- Step 2—generate an equation for the top event that is a function of only primary events
- Step 3—apply the identities

$$P * P = P$$

$$P + P * Q = P$$

Figures F-10 through **F-12** illustrate the steps used to solve for minimal cut sets.

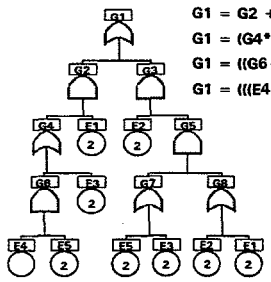


STEP 1:

G1 = G2 + G3
G2 = G4 * E1
G3 = G5 * E2
G4 = G6 + E3
G5 = G7 * G8
G6 = E4 * E5
G7 = E5 + E3
G8 = E2 + E1

STEP 1: Generate the intermediate event equations

Figure F-10. Solving for Minimal Cut Sets—Step 1

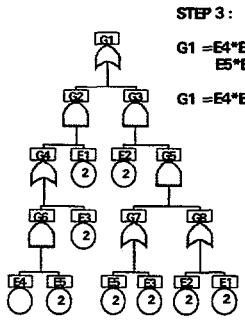


STEP 2:

G1 = G2 + G3
G1 = (G4*E1) + (G5*E2)
G1 = ((G6+E3) * E1) + ((G7*G8) * E2)
G1 = (((E4*E5) + E3) * E1) + (((E5+E3) * (E2+E1)) * E2)

STEP 2: Generate an equation for G1 that is a function of only primary events.

Figure F-11. Solving for Minimal Cut Sets—Step 2



STEP 3:

G1 =E4*E5*E1 + E3*E1 + E5*E2*E2 + E5*E1*E2 + E3*E2*E2 + E3*E1*E2

G1 =E4*E5*E1 + E3*E1 + E5*E2 + E3*E2

STEP 3: Apply the identities:

P * P = P and
P + P * Q = P

Figure F-12. Solving for Minimal Cut Sets—Step 3

Sequences are the next fault tree concept under discussion. A **sequence** contains:

- One initiating event
- One or more system failures
- Possibly one or more systems operating successfully

Some sequence characteristics are:

- Each sequence represents one endstate from an event tree that models the systems available to prevent the top event.
- Each system is generally represented by a fault tree model.
- The failure or success status of each system in the sequence is defined by the path traced through the event tree.

A Boolean minimal cut set expression is obtained for the defined sequence.

In concept, a sequence model is a fault tree:

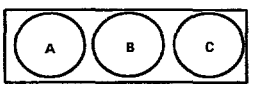
- With an AND gate as its top event, and
- Whose top event inputs are
  - the initiating event
  - the system fault trees for each failed system, and

– the **complements** of the fault trees for each system that is known to be operating successfully.

The resulting cut sets represent all the ways the accident sequence can occur.

Fault tree analysis offers some quantification options, such as the rare event approximation. Minimum cut set upper bound and exact solutions are two other quantification options. Events that cannot happen at the same time are called **mutually exclusive,** as illustrated earlier in the discussion of Venn diagrams. (A charming illustration of this concept is the restaurant industry's ubiquitous offer of soup OR salad. The diner cannot have both!) The probability of this type of event is often found using the "addition rule of probabilities."

(A or B or C) = P(A) + P(B) + P(C)



Events that are <u>not</u> mutually exclusive require a more general formula.

P(A or B or C)=P(A)+P(B)+P(C)-P(A*B)-P(A*C)-P(B*C)+P(A*B*C)

Ignoring the possibility of any two or more events occurring simultaneously, the equation reduces to what is called the "rare event equation." It is accurate to within about ten percent of the true probability when $P(Event_i) < 0.1$.

In most fault tree analysis codes, quantification of cut set expressions is done by **approximation.** Two methods are generally used:

- SETS—rare event approximation, as discussed above

$$\sum_{cut\_sets}\{\prod(basic\_event\_probabilities)\}$$

(Using this technique can produce "probabilities" greater than 1!)

- IRRAS—minimum cut set upper bound

$$1-\prod_{cut\_sets}\{1-\prod(basic\_event\_probabilities)\}$$

(Essentially, this technique yields the rare event approximation in complement space. The results look better, in that all of the "probabilities" are less than 1, but it is not necessarily more accurate!)

One problem common to both of these techniques is that they ignore "cross terms" in the quantification.

P(A *or* B) = P(A) + P(B) - P(A *and* B)

Cut sets must be made disjoint before either quantification technique will yield exact results. **Disjoint** implies that "cross terms" have been eliminated. For example,

ABC + ABD + E

could become

ABCD /E + ABC /D /E + AB /CD /E + E

A Venn diagram would show that there is no overlap between these four cut sets. They are equivalent to the original three.

The Sigma-Pi algorithm generates and quantifies disjoint cut set expressions.

The inputs to risk models are quantified in four distinct ways: experiments, data, analysis, and expert judgment. While actual experiments and test data are best, each of the four methods has its own shortcomings. For example, there are many problems in interpreting experimental data, such as problems of scale, completeness, integral and/or synergistic effects, aging effects, instrumentation errors, or atypical quality.

Using data to quantify fault tree inputs presents a different set of problems. We rarely have sufficient operating data for an individual component, system, or structure. Therefore, we are usually using grouped or inferred data. Many groupings are possible:

- Manufacturer
- Facility
- System
- Location

Many factors can render such groupings questionable:

- Material variations
- Variations in maintenance
- Variations in environment

The difficulties of analyzing fault tree inputs are not negligible. The most common problems with analysis are:

- Different levels of modeling tools, e.g.,
  - detailed three-dimensional models, such as finite element models
  - empirical models
  - system-level models
- Type of analysis limitations, e.g.,
  - number of calculations
  - incomplete physics
  - assumption of "perfect" materials and construction

In many cases, expert judgment is the best of these methods, although at first glance it may seem to be the weakest, due to its overtones of subjectivity. After all, experiments, data, and analysis are "hard science," while expert judgment can be mistakenly dismissed as opinion.

In fact, expert judgment is not just "guessing." It involves a formal probability elicitation process and combinations of experts, and the integration of knowledge from multiple sources. Expert judgment allows inference, interpolation, and limited extrapolation. The formal expert judgment process employs the following steps:

- Selecting and defining technical issues
  - tractable number of issues
  - decomposition into smaller issues
- Selection of experts
- Probability training and calibration
  - control of biases
- Meetings and information exchange
- Elicitation of probability distributions
- Processing and documentation

In addition to the quantification of fault tree inputs, **uncertainty** must be considered. Uncertainty denotes imprecisions in the PRA

analyst's knowledge or available information about:

- The input parameters to PRA models
- The PRA models themselves
- The outputs from such models

Uncertainty can affect decision-making, for example, when comparing two estimates. A clear explanation of the uncertainties presented is essential. Please note that properly developed uncertainty distributions are usually wider than preconceived notions would indicate.

Another factor to be considered in risk analysis is that of importance calculations. The four groups of importance calculations are risk reduction, risk increase, uncertainty importance, and partial derivative calculations. Each of these importance calculation groups is discussed briefly below. Sample calculations are provided for the risk reduction and risk increase factors using the following sample problem as the example.

Sample Problem

Minimal cut sets:

G1 = E4*E5*E1 + E3*E1 + E5*E2 + E3*E2

Data for basic events:

E1 = 1.00E-02
E2 = 1.00E-03
E3 = 5.00E-03
E4 = 1.00E-04
E5 = 1.00E-03

Top event frequency:

G1 = 1E-9 + 5E-5 + 1E-6 + 5E-6 = 5.6001E-5

This sample problem is based on rare event approximation.

The **risk reduction importance measure** is a change in the output variable, resulting from setting a particular probability to zero. It can be done as a ratio or difference.

Fussel-Vesely is a normalized version:

$$FV = [F(x) - F(0)]/F(x)$$

Variables with high risk reduction values are the ones that drive the magnitude of the risk. Therefore, those component failures, human errors, and initiating events with high risk reduction values are candidates for efforts to improve reliability and reduce risk.

Sample Calculation for the Risk Reduction Importance Measure

Using the sample problem, one by one, set events to zero and recalculate:

Event Set to Zero	G1	Risk Reduction
E1	6.0000E-06	5.0001E-05
E2	5.0001E-05	6.0000E-06
E3	1.0010E-06	5.5000E-05
E4	5.6000E-05	1.0000E-09
E5	5.5000E-05	1.0010E-06

Which event is most important to risk?

The **risk increase importance measure** is a change in the output resulting from setting a particular probability to 1.0. It also may be done as a ratio or a difference. The risk increase importance measure is not appropriate for initiating event frequencies.

Variables with high risk increase values are ones that could most increase risk if their probability

should unexpectedly increase. The risk increase measure is useful for assessing which elements of the risk model are the most crucial for maintaining risk at current levels.

Sample Calculation for the Risk Increase Importance Measure

Using the sample problem, one by one, set events to 1.0 and recalculate:

Event Set to One	G1	Risk Increase
E1	5.0061E-03	4.9501E-03
E2	6.0500E-03	5.9940E-03
E3	1.1001E-02	1.0945E-02
E4	6.6000E-05	9.9990E-06
E5	1.0560E-03	1.0000E-03

The **partial derivative importance measure** measures the sensitivity of the output (usually core damage frequency) to a particular input. Birnbaum structural importance is:

$$B = F(1) - F(0)$$

Birnbaum is exactly correct only if the expression is linear in the selected input and the selected input is independent of all other events. Partial derivative measures tend to overemphasize the importance of variables with small values.

The **uncertainty importance measure** measures the contribution of the uncertainty in particular inputs to the uncertainty in the output. It is determined by fixing an input at its expected value and repeating the sampling analysis. Results may be volatile. This is sometimes done on a log scale and sometimes done by comparing ratios of fixed quantiles. The uncertainty importance measure can help analysts identify areas where more information is needed.

Figure F-13 shows a cumulative distribution function curve, and **Figure F-14** shows its complement.

Figure F-15 shows a risk curve, and **Figure F-16** shows cost-benefit studies.

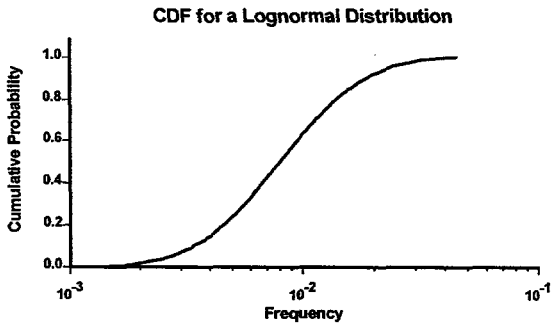


Figure F-13. Cumulative Distribution Function

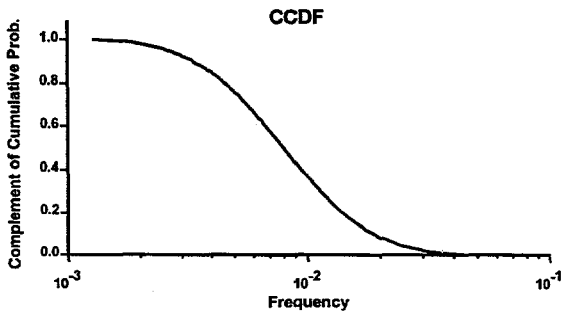


Figure F-14. Complementary Cumulative Distribution Function

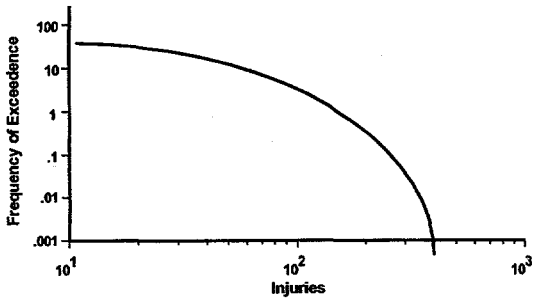


Figure F-15. Risk Curve

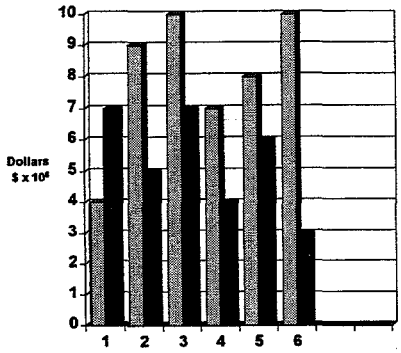


Figure F-16. Cost-Benefit Studies

4. Summary

This chapter presented an introduction to probabilistic risk assessment. The student should come away with the critical understanding that:

- Risk is very system—and location—specific
- "Worst case" is seldom an important contributor to risk
- Contributors to risk can be isolated and importance ranked
- System insights, not just numbers, are important results
- Risk can and usually should be modeled from the top down
- Multiple failures, dependencies, and human response can dominate the risk of highly redundant systems
- Understanding uncertainty is important to risk management and decision-making

The vocabulary and techniques of risk assessment and analysis were also introduced.

5. Further Reading

Analysis of the LaSalle Unit 2 Nuclear Power Plant: Risk Methods Integration and Evaluation Program, External Event Scoping Quantification, NUREG/CR-4832, Vol. 7, July 1992.

Roger J. Breeding, Timothy J. Leahy, and Jonathan Young, *Probabilistic Risk Assessment Course Documentation, Volume 1: PRA Fundamentals*, chapters 1-7, NUREG/CR-4350/1 of 7. Division of Risk Analysis and Operations, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, D.C., August 1985.

Flood Risk Management and the American River Basin: An Evaluation. National Academy Press, Washington, D.C., 1995.

David F. Haasl, Norman H. Roberts, William E. Vesely, and Francine F. Goldberg, *Probabilistic Risk Assessment Procedures Guide* (NUREG/CR-2300) *Fault Tree Handbook*, NUREG-0492. U.S. Nuclear Regulatory Commission, January 1981.

Post-Challenger Evaluation of Space Shuttle Risk Assessment and Management. National Academy Press, Washington, D.C., 1988.

Product Liability and Innovation: Managing Risk in an Uncertain Environment. National Academy Press, Washington, D.C., 1994.

A Review of NRC Staff Uses of Probabilistic Risk Assessment, NUREG-1489. U.S. Nuclear Regulatory Commission, Washington, D.C., 1994.

Risk Assessment and Risk Management for the Chemical Process Industry, Van Nostrand Reinhold, New York, 1991.

Paul C. Stern and Harvey V. Fineberg (eds.), *Understanding Risk: Informing Decisions in a Democratic Society.* Committee on Risk Characterization, National Research Council, Washington, D.C., 1996.

Uses of Risk Analysis to Achieve Balanced Safety in Building Design and Operations. National Academy Press, Washington, D.C., 1991.

Appendix G

Modeling and Simulation-Based Life-Cycle Engineering

Objectives

The objectives of this lecture, presented by Russell Skocypek of Sandia National Laboratories on March 24, 1997, are to:

- Understand the engineering process
- Become familiar with modeling and simulation-based life-cycle engineering

The engineering process is described, including

- The objectives of the engineering process
- The engineering approach—tools for making decisions
- The revolution in engineering—new tools and approaches

One of the most significant new approaches, Modeling and Simulation-Based Life-Cycle Engineering (MSBLCE), is defined, its requirements are specified, and its applicability to architectural surety℠ is discussed. Examples of the current state-of-the-art MSBLCE are given, as well as how its power may be harnessed for the future. The surety principles inherent in MSBLCE are also illustrated.

1. Introduction

Webster's Dictionary defines **engineering** as "the science by which the properties of matter and the sources of energy in nature are made useful to man in structures, machines, and products." How do we define **useful**? Useful is a concept that can vary over time, across cultures, and between individuals. It's a value-based idea. How we make things useful is more straightforward, fortunately, We make things useful by applying tools and using materials. Mankind has been doing this for ages. The history of engineering can be traced by identifying the tools and materials used to make things useful in particular eras and the defining event of that era that influenced the governing values. The following list shows the evolution of engineering tools and materials as the needs and interests of mankind changed.

- 8000 B.C.–1000 B.C.: **New Stone Age**
  - people evolved from nomadic hunters/gatherers to planters
  - tool: stone-based plows, cutters for food production
- 3500 B.C.–400 B.C.: **Bronze Age**
  - evolution to imperial expansion
  - tool: bronze (molten copper and tin) tools and weapons

- 1400 B.C.–present: **Iron Age**
  - evolution to infantry
  - tool: smelted iron (less brittle) tools and weapons
- 1450–present: **Era of the Printed Word**
  - mass communication, literacy, and knowledge transfer (science, history, religion)
  - tool: printing press and movable type
- 1304–present: **Era of Modern Warfare**
  - more powerful weapons
  - tool: gunpowder, explosives, rifles, cannons
- 1564–present: **Era of Modern Science**
  - understanding of natural world
  - tool: Galileo (father of modern science) used the telescope
- 1750–present: **Industrial Revolution**
  - change in the way people worked to factories using machines and standardization
  - Tool: science and technology-based increases in productivity with new materials (steel/iron), power sources (electricity, petroleum), transportation (steamboat, railroads), and communication (telegraph, telephone)
- 1802–present: **Transportation Revolution**
  - long-distance transportation with non-human energy sources
  - tool: 1890 steamships, 1908 assembly-line cars, 1905 airplanes, 1957 satellite in space
- 1837–present: **Communications Revolution**
  - rapid communication over distances
  - tool: 1837 telegraph, 1876 telephone, 1878 phonograph/microphone, 1890 movie projector, 1896 wireless communication (radio), 1908 television concept, 1948 transistor, 1971 microprocessor (computers)
- 1942–present: **Atomic Age**
  - harnessing of nuclear fission
  - tool: atomic bombs, nuclear power
- 1946–present: **Information Age**
  - change in the gathering and processing of information
  - tool: computers used primarily for access
- 1957–present: **Space Age**
  - presence of man beyond Earth
  - tool: spacecraft
- 1997–future: **The Engineering Revolution**
  - change in the way engineering decisions are made
  - tool: high-performance computing, experimental validation, and science becomes the next telescope, microscope. New knowledge is generated with science-based algorithms and information.

Engineers define a **problem** as something to be solved, a problem to be overcome. Engineers are problem solvers. Engineering solutions involve a **decision**, a choice from among a set of options or an irrevocable allocation of resources. Engineering design is decision-making.

The elements of decision-making are options, expectations, and values. The fundamental rule of decision theory is

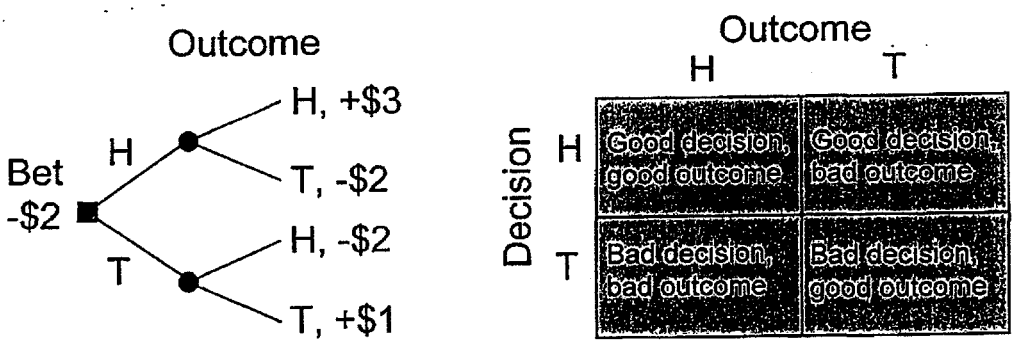


Figure G-1. Distinction Between Decisions and Outcomes

that the preferred choice is the option whose expectation has the highest value. Remember, there is a difference between good or bad decisions and good or bad outcomes. **Figure G-1** illustrates this difference, using the example of a two-dollar bet on the flip of a fair coin. You win five dollars if you choose heads and heads occurs. You win three dollars if you choose tails and tails occurs. You win nothing otherwise.

Knowledge is the basis for good decision-making. **Knowledge** is defined only in the context of a specific decision. The **state of knowledge** can be defined as the probability that the preferred decision will indeed result in the most valued outcome achievable, given the options. The state of knowledge for a specific decision depends on values. For example, say

Figure G-2. Improvement in Knowledge Through Modeling

that you're playing a competitive game of guessing how many M&Ms are in a jar. The winner is the closest guess that does not exceed the exact number. If you value winning, your best guess has only a small chance of obtaining the best outcome. However, if you value losing, your best guess can be assured of getting the desired result.

Knowledge can be improved. One way to improve knowledge is by modeling. **Figure G-2** shows the improvement in knowledge that can be achieved through modeling.

2. Theory and Principles

Keep in mind that values are an important part of the decision-making process and the fundamental rule: the preferred choice is the option whose expectation has the highest value. Preferences of the form

$$A>B>C$$

imply the existence of a real scalar u such that

$$u_A > u_B > u_C .$$

u is called utility. There is a well-developed theory of utility, based on a set of axioms, in the literature of economics.

If

$$A>B>C>A,$$

then the implication is that

$$u_A > u_B > u_C > u_A.$$

But since u is a real scalar, this is impossible. A decision-maker with these preferences is said to be irrational. The preference ordering is intransitive. No decision can be made in accord with these preferences.

If

$$A>B>C,$$

then also

$$A>C.$$

If this condition is met, the decision-maker is rational, the preferences are transitive, and decisions are possible.

Von Neumann-Morgenstern utility provides a measure of value valid under risk. There are six axioms associated with utility:

- Outcomes can be ordered in terms of preferences of the decision-maker, and the ordering is transitive.
- Compound lotteries can be reduced to simple lotteries.
- Continuity of preferences exists.
- A lottery consisting of several possible outcomes can be reduced to an equivalent lottery that has only two possible outcomes.
- Preferences among lotteries are transitive.
- Given two otherwise identical lotteries, each with two possible outcomes, the preferred lottery is the one whose probability of the preferred outcome is higher.

Von Neumann-Morgenstern expected utility theorem yields results. The utility of a lottery is the sum of the utilities of every possible outcome of the lottery, each weighted by its probability of occurrence. Remember: the utilities of each outcome must be generated in accordance with the axioms of von Neumann-Morgenstern utility, that is, they must be valid utilities.

The bottom line is that the mathematics of utility theory are well developed. It is grounded in several more-or-less accepted axioms. Utility theory has been studied since at least the time of Bernoulli (1738). Engineers make common use of utilities. To get correct results, however, the math must be done correctly. Nearly all engineering use of utility theory is incorrect.

The question becomes how these attributes can be engineered into a structure. The three engineering approaches are compared in **Table G-1**.

Table G-1. Comparison of Engineering Approaches

Engineering Approach	Advantages	Disadvantages
Test-Based	People trust the data used to make the decisions	Expensive, time-consuming; data are limited to only a few conditions; must extrapolate.
Experience-Based	People trust the experts used to make the decisions	The capability disappears when the experts leave.
Modeling and Simulation-Based	This is the only true predictive engineering approach	This is hard! We must know a lot about the structure and how it responds to its environment. Predictive tools must be validated before they will be trusted.

Experience-based and test-based approaches are not sufficient to provide infrastructure surety. Current engineering analyses conducted in support of design are off the mark, in the following ways.

- They fail to include uncertainty and risk.
- They fail to incorporate values in analysis of decision making.
- They don't compute the necessary quantities.
- They fail to include consideration of competition.

Arrow's Impossibility Theorem illustrates several of these problems. Groups, in general, do not have utilities, as shown in **Table G-2**. The final row, summarizing group preferences, shows the impossibility.

Table G-2. Flawed Attempt at Deriving Group Preferences

Individual	Preferences	Choices		
		A vs. *B*	*B* vs. *C*	*A* vs. *C*
I	*A>B>C, A>C*	*A*	*B*	*A*
II	*B>C>A, B>A*	*B*	*B*	*C*
III	*C>A>B, C>B*	*A*	*C*	*C*
Group	**Preferences:**	*A>B*	*B>C*	*C>A*

As shown in the derived group preferences, a group consisting of rational individuals need not have transitive preferences. Arrow's Impossibility Theorem shows that voting doesn't work. If all members of the group have the same preferences, voting is unnecessary. If the members of the group have different preferences, there is no group preference and, therefore, voting cannot find it.

The consequences of Arrow's Impossibility Theorem impacts engineering design in the following ways.

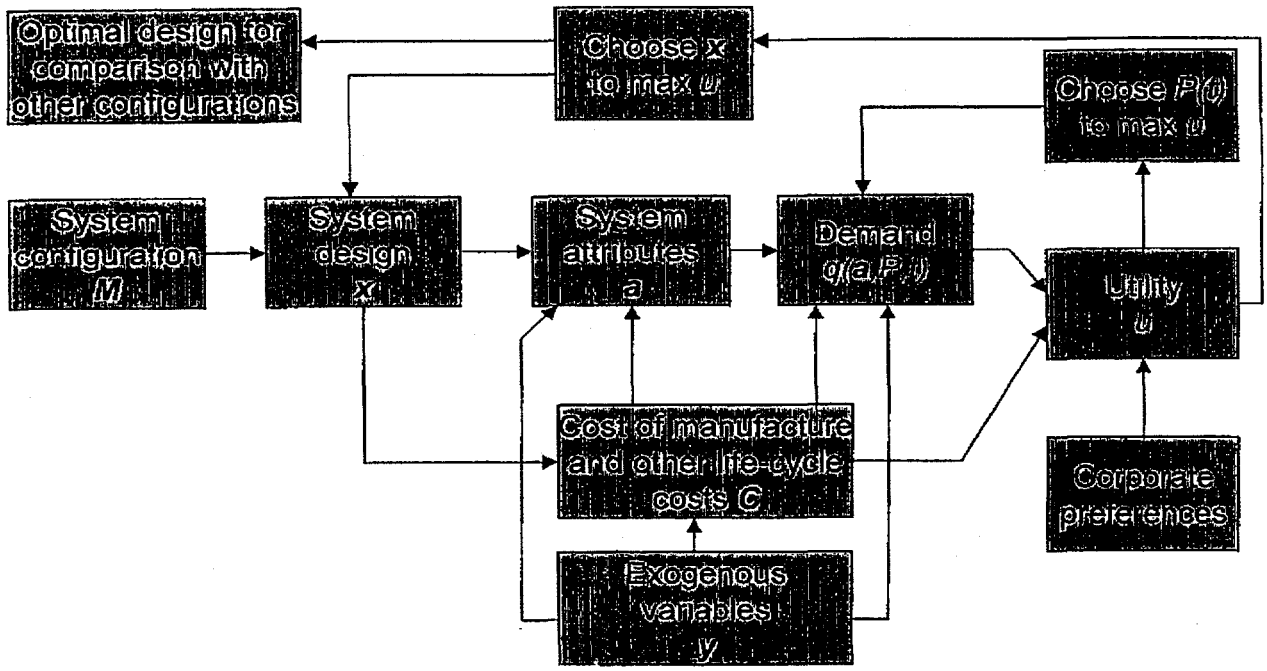


Figure G-3. A Framework for Decision-Based Engineering

- There is no such thing as a customer-centered view of value.
- Designs cannot be optimized for customers.
- Ad hoc methods, such as quality function deployment, do not work and, in fact, produce misleading results.

There is a need for a rigorous approach to engineering design and analyses. **Figure G-3** outlines one such rigorous approach.

3. Applications

The current state of the U.S. infrastructure is worrisome, to say the least. Just a few examples of the problems we face include:

- 4,000 commercial aircraft, 30% of which reach their 20-year design life in the year 2000
- 16,000 utility-scale wind turbines, with a 3-month stress equivalent to a 30-year aircraft stress
- 10,000 railroad bridges between 85 and 100 years old
- 500,000 highway bridges (200,000 deficient; 150–200 collapses each year)
- 200,000 offshore platforms in the Gulf of Mexico; scores were damaged during Hurricane Andrew
- Thousands of buildings that require inspection after every California earthquake

For success in the future, infrastructure surety needs as-built structures that are:

- Affordable to design, build, own, operate, and maintain
- In conformance with all regulations as well as the performance requirements of the owners and users of the structure
- Reliable, reliable, reliable
- Safe, secure, and controllable for owners and users
  - during normal environments (intended use)
  - under abnormal environments (e.g., storms, fires, earthquakes)
  - under hostile scenarios (e.g., terrorist threats)

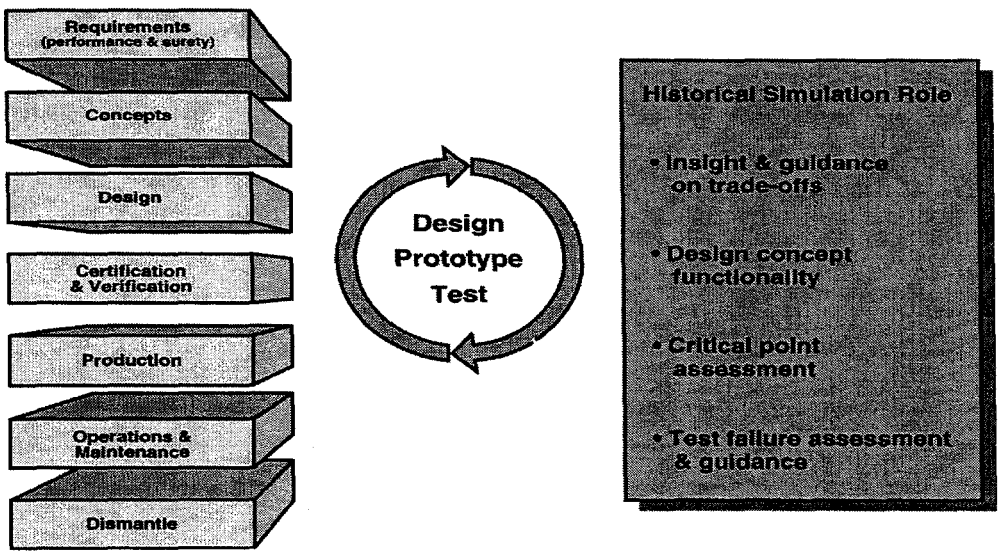


Figure G-4. Traditional Peripheral Role of Simulation in Life-Cycle System Engineering

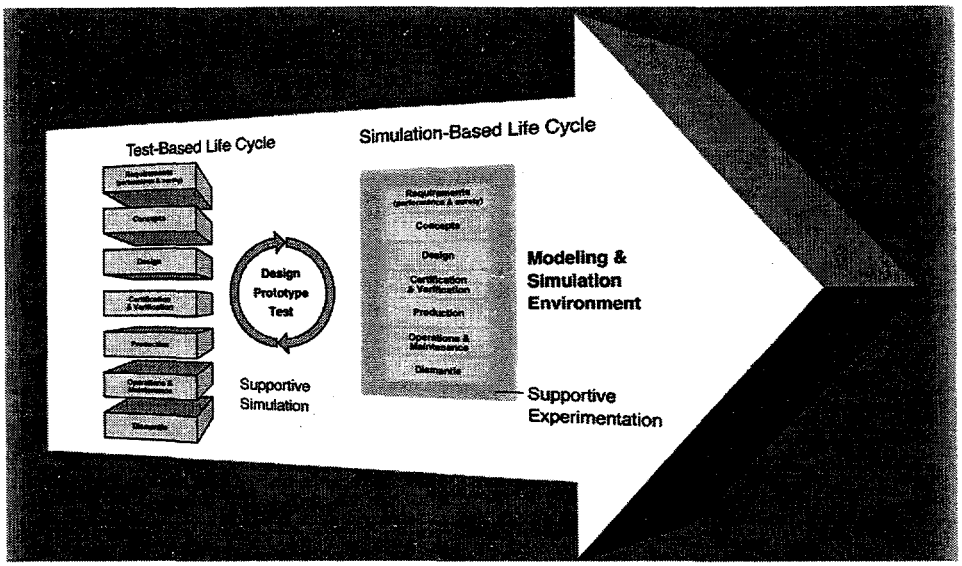


Figure G-5. Proposed Central Role of Modeling and Simulation in Life-Cycle System Engineering

- Environmentally compliant throughout the life of the structure
- Profitable when used as a business asset
- Appealing to occupants and the public

Life-cycle system engineering is the current approach to engineering design. **Figure G-4** shows the historical role of simulation in this approach, while **Figure G-5** shows the new role that simulation and modeling can assume in engineering design.

Powerful computers are the most important tool available for the complex modeling and simulation required for decision-based engineering. The supercomputer developed by Intel under the direction of the Department of Energy for the Accelerated Strategic Computing Initiative (ASCI) is a valuable tool in the new engineering approach. It would take someone operating a hand-held calculator about 57,000 years to calculate a problem the teraflops computer could compute in one second. The teraflops (so called for the nearly two trillion floating point operations per second it is capable of performing), designed to develop the higher-resolution, three-dimensional physics modeling needed to evaluate the aging nuclear stockpile without actual testing, has many other applications. The $55 million teraflops computer and its more powerful successors under the ASCI program promise to revolutionize computational science in many disciplines.

Using the teraflops, analysts can quickly run full-system, three-dimensional simulations of complex accident environments, such as an airplane crash followed by a fuel fire, an earthquake-precipitated tidal wave, or blast effects on densely populated urban structures. Sandia scientists and engineers have achieved the following calculations so far on three-fourths of the full machine:

- 100 million-cell calculation models performance of ballistic weapon system
- Computer model of comet striking the ocean shows teraflops capabilities to DOE

- Complex cylinder-crushing problem that shows the power of measured scalability in conducting finite-element simulations of unprecedented resolution in areas such as nuclear stockpile stewardship problems, reservoir modeling, and structural dynamics problems.

An example of an application that provides information for decision-based engineering design is using the teraflops (and its successors to be developed by the ASCI program) as part of an integrated triad of technologies for computational fire simulation. (The other two component technologies are experimental diagnostics and data and phenomenology.) The teraflops is capable of simulating a multitude of highly nonlinear, tightly coupled physics phenomena spanning a broad range of scales and modeling systems or material responses. Teraflops is also capable of quickly running the advanced computational algorithms and platforms required for accurate, highly resolved solutions. This capability has been demonstrated simulating aircraft engine fires, weapon system and facility performance, and smoke and fire spread in aircraft cabins, among other problems.

Another teraflops use, with even more direct application to architectural surety℠, is a blast-effects problem that examines ways to systematically implement model simulation techniques for enhancing the surety of federal buildings and other critical infrastructure systems, with special attention to antiterrorist considerations. The goal of this program is to simulate explosive effects on a large structure, using coupled computer codes. This is an enormous computational problem that would be difficult (too time-consuming and expensive) to solve without a supercomputer.

4. Summary

Our current approach to modeling in support of life-cycle engineering must change to incorporate uncertainty, risk, values, and competition. The new approach must also provide knowledge. Engineering education must also change, in that we must teach students how to obtain knowledge for design decision-making.

Life-cycle engineering is a lot harder than we have admitted to date. We must develop a rigorous approach using rigorous tools. Theory that can and should be applied to decision-based engineering exists. The tools that can and should be applied to decision-based engineering exist. High-performance computing hardware and software are a critical enabler for engineering design analysis. The revolution in engineering design made possible by modeling and simulation-based life-cycle engineering will enhance the surety of our nation's infrastructure by providing the information necessary to make the engineering decisions that increase structural safety, security, and reliability.

5. Further Reading

Russell D. Skocypek, A Competitive Advantage for Assuring the Performance of Buildings and Critical Infrastructure, in *A Conference on Architectural Surety℠: Assuring the Performance of Buildings and Infrastructures Proceedings*. Sandia National Laboratories, Albuquerque, NM, May 1997.

Appendix H

Project Planning and Case Histories

Objectives

This lecture, presented by Rudy Matalucci on April 7, 1997, analyzed failed structures and structural components to:

- Demonstrate the need for and issues of surety planning and surety evaluation in the design, planning, and approval phases of a construction project.
- Examine the effects of unanticipated abnormal and malevolent threats to buildings and structures.
- Present recommendations that will mitigate the consequences of such threats.

Summary case histories of several noteworthy failures and a more extended examination of two truck bomb attacks yield information to be considered for the surety aspects of the planning and approval phases of the construction project life cycle. The American Society of Civil Engineers (ASCE) and the Federal Emergency Management Agency (FEMA) offer specific recommendations for new structures and facilities based on the lessons learned from the Oklahoma City federal building bombing. The bombing of the USAF Khobar Towers dormitory in Saudi Arabia is used as a comparison for surety purposes. Its structural integrity after the attack is an indication of the safety features of modular components.

1. Introduction

Incorporating surety concerns and considerations at the beginning of the construction life cycle is critical to enhancing the safety, security, and reliability of facilities and structures. **Figure H-1** shows the first two phases of the construction project life cycle. The lessons learned from the failures of the past can inform and guide engineering design judgment on the predictable threats and risks considered in surety planning for future projects.

A review of historical failures and threats will familiarize the design and

Figure H-1. The Planning and Approval Phases of the Construction Project Life Cycle

construction planner with the kinds of surety issues to be considered. Identifying risks and evaluating threats are most effectively done at the outset using the team approach method. Following the completion of a surety plan, it is advisable to include the document in the approval stage as a critical acknowledgment of its purpose and content.

2. Theory and Principles

Natural disasters, such as windstorms, earthquakes, and floods, present grave risks to infrastructure buildings, systems, and facilities. For example, **Hurricane Iniki** struck Kauai in the Hawaiian Islands on September 11, 1992, destroying 90% of the island's wood-frame buildings. Fortunately, the loss of life was minimal (4 deaths), but 6,000 downed power and telephone poles prevented distribution of power, even though the cogeneration plants and substations were largely operational. What are the surety implications of this natural disaster? What lessons can we learn that we can use when planning infrastructure projects?

A closer examination of the effects of Hurricane Iniki show that building damage was confined to those of poor design and construction. Knowledge of wind effects was used in the well-engineered buildings that withstood the winds. Power and telephone services could have been restored quickly had the utilities been buried rather than dependent on wind-susceptible poles. This information can be used to make infrastructure surety engineering decisions in other hurricane zones.

Surety issues are inherent in other abnormal threat situations. When **Hurricane Andrew** pounded South Florida on August 24, 1992, 85,000 dwelling units were destroyed, leaving hundreds of thousands of people homeless. Almost one and a half million customers suffered the loss of power, water, communications, and sewage facilities (in varying degrees), and 38 people died.

The wind speed of Hurricane Andrew was within the design criteria of the stringent South Florida Building Code, and such massive building damage was unanticipated. There has been some controversy whether the Code should be improved or whether Code enforcement should be improved. In either case, many buildings that were expected to withstand hurricanes did not survive Hurricane Andrew. Hurricane risks, like those from fire and earthquake, are quantifiable and controllable. Appropriate decisions with regard to siting, design, construction, and improving facilities can provide good protection from such losses.

The **Northridge (California) earthquake** on January 17, 1994, was the second most costly disaster in U.S. history (after Hurricane Andrew). This much-studied earthquake caused extensive and unexpected damage to steel buildings. This earthquake yielded significant new information on the vulnerability of specific structural designs, and resulted in increasingly expensive and sometimes unavailable earthquake insurance. Again, the steel buildings did not respond as predicted. Higher levels of safety were expected than were actually experienced and code revisions are currently under consideration.

Washington's **Tacoma Narrows Bridge** ("Galloping Gertie") collapsed on November 7, 1940, a few months after completion. This event was a massive

failure that had an enormous impact on the way we design suspension bridges. This beautiful and slender suspension bridge failed after resonating in torsion for some time under wind loading. The tie-down cables and inclined stay cables did not prevent the 45° twist that occurred in the 42 mph wind. The river valley acted as a wind tunnel that focused lateral forces on the bridge structure. The collapse of the Tacoma Narrows Bridge resulted in a five-point bridge design plan to prevent twisting:

- "Open" stiffening trusses
- Increased ratio of width/span
- Increased bending stiffness of truss/girder
- Increased dampening of structure
- Employment of a dynamic damper to reduce resonance

Despite the lessons learned from the spectacular and widely publicized collapse of "Galloping Gertie" and the obvious surety applications to bridge design, it was not until 1967 when the **Silver Bridge** collapsed over the Ohio River between West Virginia and Ohio, killing 46 people, that the formation of the National Bridge Inspection Standards (NBIS) was spurred. The Silver Bridge failed because structural redundancy was lacking. One support failed, and the bridge collapsed. The U.S. has been inspecting its bridges ever since, and many of these bridges are in poor condition due to the effects of aging. Many others were poorly designed and pose safety risks in abnormal conditions. Most are vulnerable to malevolent threats.

The **Kemper Arena roof failure** in Kansas City, Missouri, on June 4, 1979, resulted in no casualties, due to serendipitous timing. The building was empty when the roof fell in, but just 24 hours earlier the $23.2 million arena was filled with thousands of people who were attending the American Institute of Architects convention. The progressive failure was caused by a lack of redundancy. Rainwater accumulated on the roof during a downpour and, aggravated by two wind effects, caused a deflection in the stiff horizontal structure, thus allowing more water to pond and eventually causing bolt failure.

A year and a half earlier, on January 17, 1978, the **Hartford (Connecticut) Arena roof collapse** had also occurred without injury, also due to timing. Six hours before its roof failed, 5,000 fans were watching a basketball game in the arena. Progressive collapse could have been prevented by adding fewer than 50 more bars (to the 5000+-bar structure) to brace the top outer horizontals and prevent bar-buckling. Indications of trouble during construction were dismissed by the engineer and construction contractor.

The November 18, 1996, **Chunnel fire** is a more recent example of a dangerous failure to predict and prevent risks. An open truck loaded with polystyrene broke into flames in the English Channel Tunnel. The 31-mile undersea link between England and France is considered Europe's top engineering feat. It comprises two train rail tunnels and a service tunnel. The burning truck was on a freight train with 31 passengers and three crew members. The flames spread rapidly to five other carriages. As many as 14 carriages were affected by the fire. All 34 people aboard the train were overcome by smoke and fumes before being evacuated. South tunnel damage from fire temperatures

of 2700°F that destroyed the tunnel lining and electrical system in a 1,600-foot section took over six months to repair. Severe economic impact was experienced as a result of the closure of the Chunnel over this repair period.

What are the surety issues of the Chunnel fire? Some suspicion of arson had been mentioned early in the investigation. IRA bombing threats also underscored the vulnerability of the Chunnel. Although there was no indication that the Chunnel fire was the result of a terrorist attack, the early concerns indicated the security system may have been flawed.

Chunnel safety features included a central service tunnel, electric pumps for possible flooding, smoke detectors, and exhaust fans, but no sprinklers. After the fire, the wisdom of eliminating sprinklers and the safety of the open wagon design were under question. An important point to consider was that the security and safety of the Chunnel had been demonstrated to the satisfaction of rigorous inspectors. Once again, reliance on codes, guidelines, and other existing authority had not prevented failure. Surety issues are beyond the scope of existing standards.

Another recent failure with surety implications is the **New Orleans (Louisiana) Riverwalk barge accident on** December 14, 1996. A barge crashed into a shopping pier thronged with tourists, Christmas shoppers, and schoolchildren on winter holiday. This accident caused minor injuries and more significant property damage. The surety issues are primarily safety-based. The barge pilot had been involved in several accidents before. Neither the barge nor the shopping center had adequate alarm systems, so warning was haphazard. Evacuation was chaotic.

The infamous **Hyatt Regency skywalk failure** killed 114 people in Kansas City, Missouri, on July 17, 1981. The two-level catwalk failed under a live load of spectators swaying and dancing to the music from the band in the lobby below. Suddenly, nuts tore through the overloaded members, plunging most of the walkway and the audience to the lobby floor. There were a number of surety issues regarding the skywalk that failed under what was planned as normal conditions. The original design called for nuts where they could not actually be installed on single rods that penetrated the upper and lower catwalks. The substitution of offset rods proved disastrous. The upper catwalk supported itself and the lower catwalk, by means of the substituted rods, which were offset from one another and thus induced torque. The original design used a much more stable single rod as support.

Although the live load applied by people dancing may have caused harmonic oscillation, even the static load exceeded the design load (which was not what was actually built). There was plenty of blame and liability for failure to spread around. Some professional licenses were revoked, indicating that this failure was caused by human error that could have been averted.

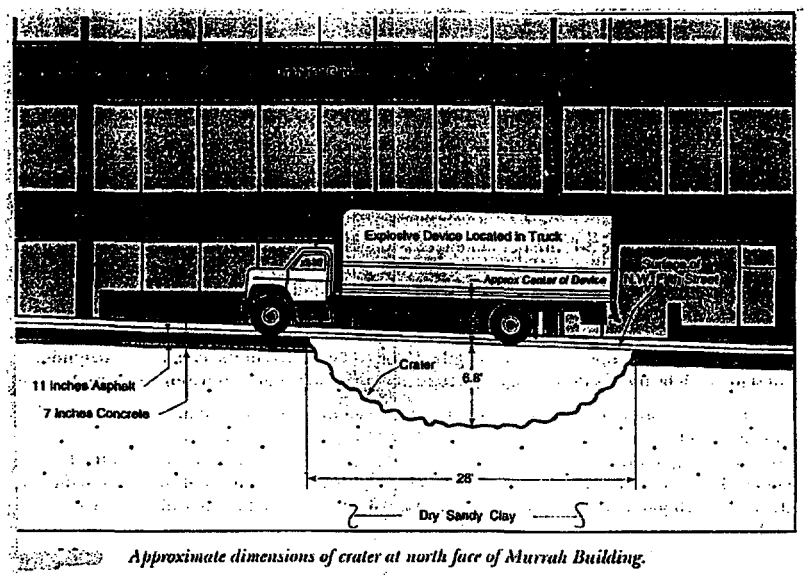
New York's **Citicorp Center** building was an averted disaster. Thanks to serendipity, a timely surety evaluation, and the professionally ethical behavior of a host of principals led by William Lemessurier, the Citicorp Center was neither devastated by a hurricane nor the site of injury and death. (For a fascinating account of the story, please

see Morgenstern) In Huber's 1995 (The Risk Digest) assessment, the Citicorp vulnerabilities to risk occurred because of the following:

- An unusual or novel design aspect that was affected by a church located on the northwest corner of the property.
- A creative and innovative solution that required new design and analysis. (Putting the main support columns in the middle of each side of the building, rather than at the corners.)
- Not quite getting all the implications and analysis of the innovations right. The reviewers of the design treated some special new diagonal wind braces as trusses rather than columns, thereby disregarding a required standard.
- A critical change in the specification made by the contractor during construction to save time and money was not reflected back to the designers and/or reanalyzed and reviewed for its impact, which greatly weakened the design.
- A resulting flaw that would only show up under heavy load and not under normal use or test.

The Citicorp vulnerabilities provides a checklist of potential concerns for surety planning and evaluation. Unfortunately for LeMessurier et al., the Citicorp Center was not only constructed but operating before the concerns were detected. Fortunately for everyone involved, no expense was spared in correcting the problem quickly. Considering the potential surety issues before construction would have saved time, money, and stress.

The **Oklahoma City federal building bombing** on April 19, 1995, horrified America. Domestic terrorism entered the public awareness when 4,800 pounds of explosive material concealed in a rental truck exploded 15 feet from the Alfred P. Murrah Federal Building in downtown Oklahoma City. The explosion and partial collapse of the 9-story building killed 168 people, injured hundreds more, and resulted in millions of dollars in losses.



Approximate dimensions of crater at north face of Murrah Building.

Figure H-2. Approximate Dimensions of Crater at North Face of Murrah Building

The Murrah Building was constructed in 1976 by the General Services Administration. It had nine stories, an ordinary moment frame, ten 20-foot east-west bays, two 35-foot north-south bays, vertical circular tube columns at the corners, and a transfer girder beam at the third-floor level. When the truck bomb exploded, it blew through almost a foot of asphalt and seven

inches of concrete to create a crater 28 feet long and nearly seven feet deep in the street adjacent to the building. (See **Figure H-2**.)

The damage to the building is shown in **Figure H-3**.

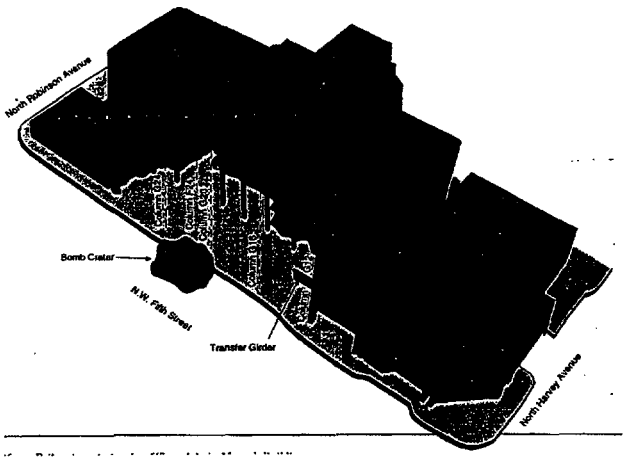


Figure H-3. Failure Boundaries of Roof/Floor Slabs in Murrah Building

An August 1996 ASCE/FEMA study (REF) of the tragedy reached the following conclusions:

- The Murrah Building was designed and built in accordance with code.
- No blast or earthquake load protection was required.
- The approximately 4,800 pounds of explosive were detonated adjacent to a critical support column.
- The column support to the transfer girder shattered.
- The adjacent two column supports failed due to overstress.
- The progressive collapse of the structure above the failed transfer girder followed.

The same study issued the following recommendations:

- Public buildings should be partially protected, and access should be controlled.
- Compartmentalized construction is encouraged to reduce progressive collapse and isolate effects to local areas.

In addition:

- FEMA supports earthquake-resistant designs even in non-earthquake zones, as this will help protect structures against blast effects and other potential threats.
- HUD supports reducing progressive collapse, which would isolate damage to directly affected areas.
- Special moment frames and dual or redundant systems would reduce vulnerability.

The cost for incorporating these recommendations into the design and construction of new buildings was estimated to increase total costs by one to two percent.

The Oklahoma City bombing brought surety issues to the forefront of America's consciousness. Infrastructure vulnerability to malevolent threats became apparent. Research and development projects focusing on blast protection and mitigation of public buildings and systems and post-stress safety became featured stories in the news media.

Just over a year later, when a truck bomb blasted through an eight-story apartment building at the **Khobar Towers,** an apartment complex serving American soldiers in Dhahran, Saudi Arabia, American awareness was raised another notch. Building #131 was 80 feet from the bomb crater, which was 55 feet in diameter and 15 feet deep in fine sand. (Building

#133, 400 feet away from the blast, also sustained major damage.) Although the explosive quantity and type remain uncertain, the best guess is that the blast was two to four times as powerful as the Oklahoma City bomb. The Khobar Towers construction design featured pre-cast bearing concrete panels, bolted ductile joint connections, and Jersey barriers along the street edge. While 168 people died and the building suffered progressive collapse in Oklahoma City, 19 people were killed in Dhahran and the structure survived major damage without collapse, despite the larger bomb. A security guard about 125 feet from the explosion also survived the attack.

A DSWA/WES study on the Khobar Towers concluded:

- The primary structural damage to Building 131 was that the front facade was destroyed and debris filled the rooms.
- There was extensive glass and frame damage
  - glass fragments were responsible for 80% of the 450 injuries
  - window damage occurred up to 1,000 feet away.
- The Jersey barriers deflected the shock front, possibly saving the security guard.
- The same study made the following recommendations:
- Terrorist threat protection is a necessary consideration, especially for buildings like the Khobar Towers that house politically vulnerable American soldiers on foreign soil.
- Standoff distance should be increased to reduce fatalities in the event of an attack.
- Retrofit hardening should be considered, as well as hardening for new designs.
- Construction materials should be hardened.

Camouflage, concealment, and deception can also protect soldiers and structures from malevolent attack.

3. Applications

The bomb attacks in Oklahoma City and Dhahran galvanized research in the areas of blast effects and terrorist threat protection. **Figure H-4** shows the damage to a structure caused by explosives of varying weights detonating at 150 feet from the target and **Figure H-5** shows the predicted damage caused by a 5,000-lb-

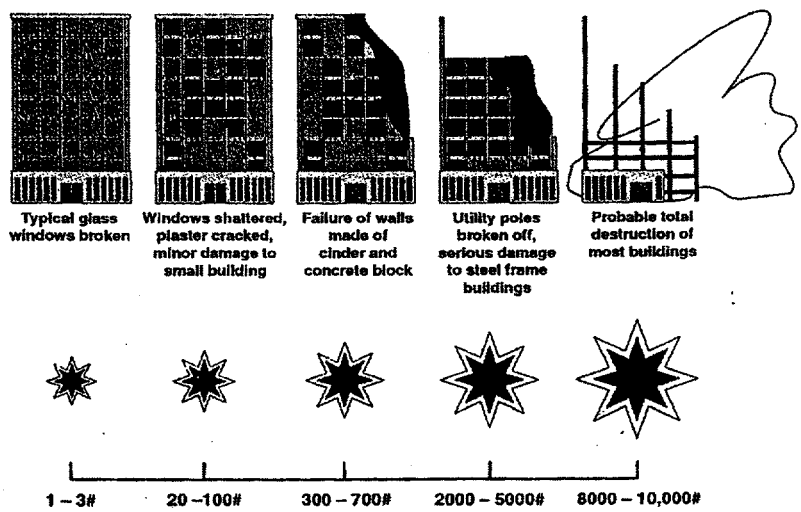


Figure H-4. Structural Damage vs. Detonated Explosive Weight

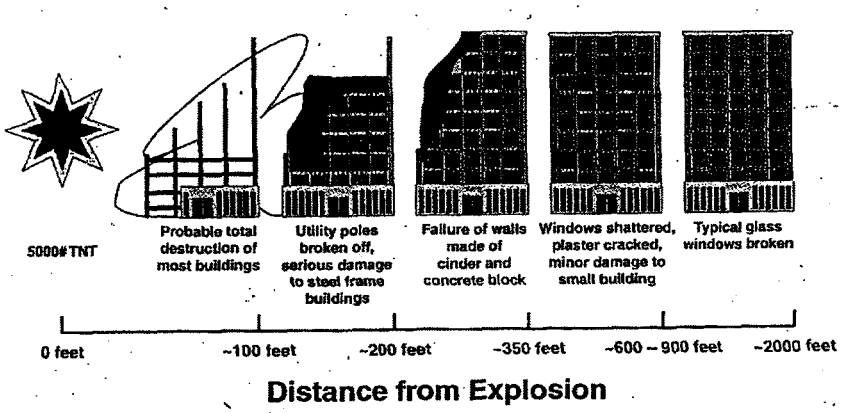


Figure H-5. Structural Damage Caused by a 5,000-lb TNT Explosive Charge at Varying Distances from the Target

equivalent TNT explosion at varying distances from the target, the results of a blast effects study.

The discovery that most blast injuries are from shattered glass has spurred researchers to evaluate and test new materials and methods to mitigate the injuries caused by glass response to explosions.

Failure Analysis Associates, a forensic engineering firm with a large professional presence at the Oklahoma City site in the aftermath of the bombing, prepared the following recommendations to enhance the surety of buildings (Hinman, 1996).

Checklist for Protecting Buildings Against Car-Bomb Attack

(1) It is best if the building is set back from the street. Create a secured perimeter at the curb by using bollards or heavy decorative planters to keep vehicles away from the building. If possible, restrict or eliminate street parking adjacent to building.

(2) For new buildings, minimize the size and number of windows. Place larger windows facing directions which offer more protection from an external threat (overlooking an inner courtyard, for instance). If this is not possible, use Mylar coating on the back of windows to hold glass shards together if breakage occurs. Other alternatives are to use specially designed curtains to capture glass shards or to replace existing panels with tempered glass or laminated security glazing.

(3) Avoid underground parking. If this is not possible, limit underground parking to building occupants and physically limit the size of vehicles that enter the garage. Place public parking away from the building, or localize public parking areas in one area so that these may be identified as vulnerable areas where extra security precautions are needed.

(4) Avoid straight-away access to the front entrance by locating the main lobby away from the oncoming street. Also, use obstacles at the entrance such as staircases, winding driveways, trees, or reflecting pools to keep vehicles from gaining access to building interior.

(5) Locate heavily occupied office areas and critical functions away from windows that face the street. Interior offices are the safest.

(6) Place air conditioners and other equipment low to the floor, not near the ceiling where they could become projectiles.

(7) Keep the locations of vulnerable areas such as control rooms and executive suites confidential. Do not list the locations in public directories in the lobby.

(8) Simple building geometries work best to mitigate blast pressures. Ornamental additions to the building should be constructed of light-weight materials, such as wood rather than heavy materials like metal. Light materials will be less lethal if they become flying debris.

(9) Construct new buildings using poured-in-place reinforced concrete with ductile connections at the joints, such as is used in seismic design. Employ progressive-collapse measures to add redundancy to the structural design. This will ensure that if a portion of the building fails, the damage will remain localized and the entire building will not collapse. This will facilitate evacuation, rescue efforts, and structural repairs.

(10) Avoid building shapes with reentrant corners, for instance L-shaped or U-shaped buildings where the pressure could become confined or trapped, enhancing airblast effects.

The new awareness of the vulnerability of the infrastructure, that is, the public buildings and systems that support our national interests, has rendered surety planning and evaluation an important part of design.

4. Summary

What do we learn from engineering failures? According to Graham et al. (1996), we can learn a great deal from engineering failures, including the following.

- Most of them involve a lack of checks in the design and implementation of whatever failed. Such checks would have cost time, or money, or both. Cutting corners prevents the correction of design flaws that were detected or suspected (such as the Hubble telescope and the *Challenger*) and those that could have been detected before failure (such as the Hyatt Regency skywalk) before failure, if not before being put into service.
- Some failures may be initiated by a single cause and propagated or accelerated by more than one, falling down like a house of cards. The Citicorp Center would have been just such a failure.

How can engineering failures be avoided? Again, Graham et al. (1996) have the following recommendations with applications to surety planning and evaluation.

- A failure is not the same as a malfunction. In the latter case, the thing may well work the next time you turn it on.
- Build redundancy into design. Redundancy is also a function of reliability and availability.
- Be aware of details, such as (for structures) corners, connections, and reinforcements. In those instances, there are stress concentrations. A structure has, in general, a safety factor: that factor is only as good as the weakest part of the structure.

- "I did what I was told" is a poor excuse for following a poor course of action. The engineer must avoid throwing work "over the wall" and fearing management reprisal for warnings of potential failure.
- Independent verification does not guarantee that errors will be detected.

5. Further Reading

Ron Graham (ed.) et al., 1996. This FAQ (frequently asked questions) on engineering failures is available on the internet at the following URL: http://www.indchem.metro-u.ac.jp/SSPEJ/Failures.html.

Frank J. Heger, Assurance of Public Safety Should Be a Priority Issue for Structural Engineer Associations, in *Structure*, pp. 14-16, Fall 1996.

Eve Hinman, Approach for Designing Civilian Structures Against Terrorist Attack, presented at the *Structures for Enhanced Safety and Physical Security Specialty Conference of the American Society of Civil Engineers*, Arlington, VA, March 8-10, 1989.

Eve Hinman, Checklist for Protecting Buildings Against Car-Bomb Attack, Failure Analysis Associates Inc., Menlo Park, CA, 1996.

Andy Huber, *The New Yorker* article on "Potential Building Collapse: The 59-Story Crisis," Forum on Risks to the Public in Computers and Related Systems, ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator, in *The Risk Digest*, Volume 17, Issue 16, Friday 2 June 1995.

Richard Little, Risk Factors and the Performance of Constructed Facilities, in *A Conference on Architectural Surety℠: Assuring the Performance of Buildings and Infrastructure* proceedings. Sandia National Laboratories, Albuquerque, NM, May 1997.

Joe Morgenstern, The Fifty-Nine-Story Crisis, in *The New Yorker*, vol. LXXI, no. 14, May 29, 1995, pp. 45-53).

Appendix I

Engineering and Construction Issues

Objectives

The objective of this lecture, presented by Rudy Matalucci on April 14, 1997, is to provide an examination of potential engineering or construction failures.

This lecture presents a review of the requirements for surety students and the place of surety in the construction project life cycle. In addition, potential construction and engineering failures are listed for consideration.

1. Introduction

The student of infrastructure surety is required to develop a new approach to engineering and construction, as shown in **Figure I-1**.

This new approach leads to new areas of consideration in the construction project life cycle. **Figure I-2** shows the surety considerations incorporated into the construction project life cycle.

This new approach to engineering design and the incorporation of surety considerations into the construction project life cycle increases the safety, security, and reliability of the project invisibly. Surety is only evident in its absence, as illustrated by **Figure I-3**.

This tongue-in-cheek figure holds an element of truth. The need for surety does become most obvious when there is a failure

2. Theory and Principles

To understand the failures of structural systems, we must first consider the purpose and requirements of such systems. Structural systems are intended to help mankind live better lives by guaranteeing, within limits, improved comfort and safety. The requirements of structural systems are to maintain stability and equilibrium and incorporate redundancy, which allows loads to be supported in more than one way. Thus we can see that in practice, all structural failures may be considered the result of a lack of redundancy.

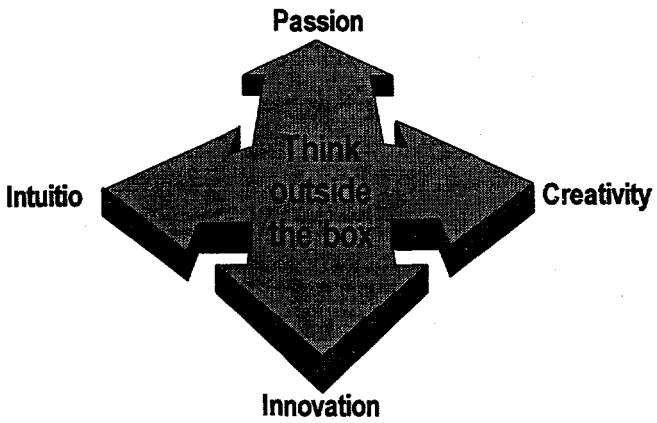


Figure I-1. Thinking Outside the Box

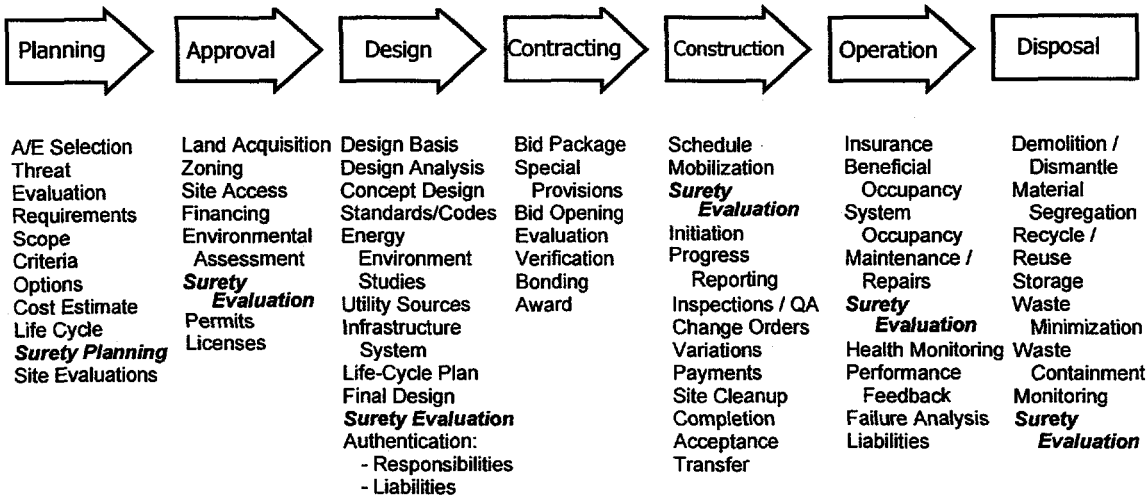


Figure I-2. Components of Construction Project Life Cycle Phases

The Risk / Reward calculation for engineers looks something like this:

Risk: Public humiliation and the death of thousands of innocent people.

Reward: A certificate of appreciation in a handsome plastic frame.

Figure I-3. Cost/Benefit Analysis of Incorporating Surety Considerations

(Chain reaction leads to progressive collapse.)

What are the design loads for buildings or other structures? There are four main categories of loads:

- Earth attracts (gravity)
- Wind blows (pressure and suction)
- Earth's crust moves (shakes and settles)
- Sun's radiation (thermal stresses)

As **Figure I-4** shows, there are numerous loads that fit into these broad categories.

Other loads that must be considered in the design of a structure or system may be added to this list. The intention of considering loads in the design and construction process is, of course, to assure against failures. Some areas of failure due to design errors include:

- Errors in design concept
- Lack of structural redundancy
- Failure to consider all loads
- Deficiency in connections
- Calculational errors
- Misuse of computer software
- Selection of incompatible materials

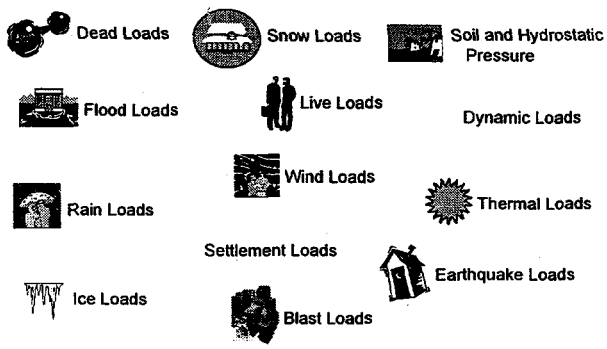


Figure I-4. Design Loads for Buildings and Other Structures

or assemblies

- Failure to consider maintenance requirements or durability
- Inadequate specifications and lack of quality controls
- Unclear design intent

Failures may also occur as a result of construction errors. Some areas of failure due to construction errors include:

- Excavation accidents
- Failure of construction equipment
- Incorrect construction sequence
- Inadequate temporary support
- Premature removal of formwork and shoring
- Noncompliance with design intent

The incidence of these failures can be reduced markedly by incorporating surety considerations into the design and construction process.

3. Applications

The 1985 ASCE conference made several recommendations for reducing the severity and frequency of failures. These recommendations include:

- Improved structural integrity (ductility, continuity, redundancy)
- Certification of completed building as safe (certification of occupancy)
- Project peer review
- Definition and assignment of responsibility
- Unified risk insurance (combined risk policy)
- Better code enforcement (regulatory function)
- Discourage competitive bidding for A/E
- Improved education (disseminate failure data)
- Creation of repository for failure information
- Development of journal (case studies and failures)
- Improvement of quality assurance and control

4. Summary

Incorporating surety considerations into the construction project life cycle will reduce the likelihood of failures and meet the objectives of the ASCE recommendations.

5. Further Reading

Eurotunnel, Summary of the Eurotunnel Internal Inquiry into the Fire on 18 November 1996: Measures to be Taken for the Resumption of the HGV Service, April 1997.

Eve E. Hinman, The Bombing of the Oklahoma City Federal Building: A Failure Analysis, Failure Analysis Associates, 149 Commonwealth Drive, Menlo Park, CA, 1996.

J. E. N. Jensen, Arch History and Architecture, National Park Service, Washington, D.C.

H. S. Lew, N. J. Carino, and S. G. Fattal, Cause of the Condominium Collapse in Cocoa Beach, Florida, National Bureau of Standards, Construction Engineering Group, Center for Building Technology.

Sue Mallonee, Sheryll Shariat, Gail Stennies, Rick Waxweiler, David Hogan, and Fred Jordan, Physical Injuries and Fatalities Reulting From the Oklahoma City Bombing, in *The*

Journal of the American Medical Association, vol. 276, pp. 382-387, August 7, 1996.

R. E. Melchers, Human Error in Structural Reliability Assessments, in *Reliability Engineering,* vol. 7, pp.61-75, 1984.

Kenneth Silber, Technology: Robot 'Insects' Create a Buzz, in *Insight,* p. 38, April 7-14, 1997.

The World Trade Center Bombing, in *Parking,* pp. 23-25, October/November 1994.

Appendix J

Performance Codes, Standards, and Guidelines

Objectives

This lecture, presented by Rudy Matalucci on April 21, 1997, is intended to prepare the student for the performance-based codes that are likely to be the guidelines of the future.

A comparison of prescription-based codes versus performance-based codes will familiarize the student with both the strengths and weaknesses of the performance-based codes that are developing a following in the design community and the traditional prescriptive-based codes that are in use today.

1. Introduction

The International Building Code (IBC) Performance Committee of the AIA has been created to address two primary goals:

- To develop the intent of a performance-based building code for one or more levels of accepted risk
- To develop the related functional objectives and performance requirements to achieve the defined goals

In addition, close attention must be given to the development of the prescriptive requirements of the IBC to assure a consistent level of performance is achieved.

Prescriptive-based codes are defined by the IBC Performance Committee as "Requirements which have been **empirically derived** utilizing the accumulated judgment of a group of experts or by actual field experience . . ." This is contrasted with performance-based codes, which are defined as "Codes which state the **intended functional results** and also may include the analytical tools or methodologies (standards of practice) used to demonstrate an **end result** as dictated by the functional statement . . ."

The IBC Performance Committee was convened to prepare recommendations for the development of performance-based codes and methods.

2. Theory and Principles

According to the IBC Performance Committee, performance code development will include identification of:

- Societal goals
- Functional objectives
- Performance requirements
- Verification methods
  - deemed-to-satisfy requirements
  - performance-based methods

Societal goals include the surety values of:

- Health, safety, and welfare
- Life safety
- Structural stability
- Controlled egress and access
- Protection of adjacent properties
- Limited property losses

Deemed-to-satisfy requirements are very like the prescriptive codes currently in use. A solution to the performance objective is presented and, if followed, the regulators consider the requirement and objective to have been met. In prescription-based codes, this is the only way to verify "meeting code." In performance-based codes, the deemed-to-satisfy requirement is not the **only** solution. While it is one way to be sure of achieving the specified performance objective, the prescribed, deemed-to-satisfy method is not the only way.

Alternative solutions to achieving the performance objective can be verified by a number of methods:

- Laboratory tests
- Tests in situ
- Computer modeling
- Engineering design methods

Because performance-based codes will include deemed-to-satisfy requirements, which are basically the same as the current prescriptive code requirements, as well as the possibility of using alternative methods of achieving the performance objectives, the architects and engineers of future structures will have more design options than are currently available. Most smaller projects will probably use the deemed-to-satisfy prescriptive approach because, for about 90% of all projects, the cost of determining, specifying, and validating performance methods will be too high. However, larger and atypical projects will likely use alternative methods to satisfy performance criteria, if the cost can be shown to be lower.

One of the issues that must be addressed is risk acceptance versus risk avoidance. Who will allow design professionals to assume the risk (and attendant liability)? Under performance-based codes, who will be responsible for final liability? The role of regulators has not yet been established under a performance-based system.

For a performance-based approach to work efficiently and cost-effectively, certain processes and procedures should be included:

- Goals and objectives must be identified early and agreed-upon by the design team and the owner.
- Performance statements must be developed.
- Early meetings with attorneys are essential to establish validation criteria
- Acceptance criteria are critical to success.

Ongoing review and regulation are also givens with performance-based design methods. Structures designed and built using performance-based methods will often have complex systems (such as smoke control, for example) that require ongoing monitoring and periodic testing after occupancy. "Cradle-to-grave" regulation is a part of using performance-based codes. Performance freedom versus standardization becomes an issue for the regulators, as

verification and approval of alternative forms of meeting performance objectives become much more complex. The previously mentioned issue of liability is also a consideration for regulators.

Performance-based codes will change the way structures are designed in several ways. The need for specialization will increase because the alternative methods possible to meet the performance objectives are certain to be more creative, sophisticated, and ingenious than the standard method. In addition, verification methods will need to be developed and accepted. These are likely to include peer review and third-party checking. Also, assignment and acceptance of liability must be decided, along with the other roles of the professionals versus the regulators.

Fire safety is a specific area in which performance-based codes have been explored.

3. Applications

The current trends in fire safety are toward:

- Cost effectiveness
- Technological advancements
- More specialized products
- Availability of calculation methods
- Maturity of fire protection engineering
- Performance-based design methods

These trends provide a nearly ideal breeding ground for performance-based codes. Recognizing the changing needs, the Society of Fire Protection Engineers (SFPE) developed a focus group to identify the action items associated with the current trends. The SFPE focus group made the following recommendations:

- Extract and quantify goals and objectives from the current codes (code organizations)
- Develop policy-level goals (all parties)
- Develop tools and techniques to measure performance (professionals)
- Develop an engineering guide for developing performance-based solutions (SFPE)
- Develop common vocabulary and definitions
- Educate the building and fire community

The current codes for fire safety are prescriptive-based regulations. These prescriptive fire-based codes:

- Address generic occupancy groups
- Provide fire safety through a combination of prescriptions
- Are rooted in the 19th century
- Are based largely on judgment, experience, and empiricism rather than on science and engineering

There are weaknesses inherent in any prescriptive code, and the fire safety code is no exception. These weaknesses include:

- The level of safety is not identified
- The effects of the requirements are not measured
- Safety factors are not quantified
- Increased building costs result

There are also some strengths associated with prescriptive codes, which is one of the best reasons that

we continue to use them. These strengths include:

- They work
- They have an established comfort level
- They require less of an initial effort to implement
- They are comparatively easy to enforce

The performance-based approach offers a number of advantages in the fire safety realm. Some of the reasons that performance-based guidelines are under development by fire safety engineers are that performance-based approaches:

- Achieve specific fire safety goals for a specific application
- Measure performance of the entire fire safety package
- Identify safety factors employed
- Rely heavily on scientific and engineering principles
- Provide greater design flexibility
- Encourage more cost-effective solutions
- Better address complex arrangements

Of course, performance-based approaches are not perfect. Weaknesses of the performance-based approach include the following objections:

- Not a new concept
- Currently employed through "equivalency options" found in many codes and standards
- Standardized procedures and definitions are lacking
- The "equivalency option" does not properly serve performance-based design

The strengths of performance-based approaches to fire safety are undeniable. These advantages include the following:

- Establishes fire safety goals, including objectives and criteria
- Evaluates the characteristics of the people or property exposed (identifying assumptions)
- Identifies potential hazards and defines appropriate fire scenarios
- Selects suitable design tools (calculation methods, computer models, fire tests)
- Develops and accesses a proposed solution
- Obtains verification of proposed solution

The NFPA intends to find a way to have their cake and eat it too. Their plan is to combine the strengths of the two approaches and eliminate the weaknesses of each. To this admirable goal, the NFPA recommends a dual-track approach. Future NFPA documents will include both performance-based and prescriptive-based design options. The key elements to be incorporated into NFPA documents are:

- Fire safety goals, objectives, and criteria
- Assumptions
- Fire scenarios
- Reference to design tools

The NFPA observes that prescriptive-based methods are likely to continue as the primary design option, but that development and implementation of

performance-based methods will increase. Other NFPA observations and recommendations for the future include the following:

- The "equivalency option" is not sufficient
- Guidance is needed for verification of performance-based designs (increased scientific basis)
- Cooperation with the industry is essential
- The consensus process must be preserved
- A managed evolution should be pursued

4. Summary

As illustrated by the example of the fire safety industry, performance-based approaches are a significant future trend. While there are significant advantages to the performance-based codes over the prescriptive codes that are in use now (and have been since the dawn of regulation), no one wants to "throw out the baby with the bath water" and lose all the proven strengths of the existing approach. An amalgamated code that offers more options and alternatives, both performance and prescriptive options, offers the best opportunity for improving the design process.

5. Further Reading

Objective-Based Codes: A New Approach for Canada. Institute for Research in Construction, National Research Council of Canada, Ottawa, Canada, 1995.

David A. Lucht, Charles H. Kime, and Jon S. Traw, International Developments in Building Code Concepts, in J. *of Fire Prot. Eng.*, 5(4), pp. 125-133, 1993.

Intentionally Left Blank

Appendix K

Ethics, Responsibilities, and Litigation

Objectives

On April 28, 1997, Lyman Sandy of the Miller, Stratvert & Torgerson law firm presented a lecture on the changing face of professional liability, with the purpose of familiarizing the student with the potential for legal actions resulting from surety failures.

Professional ethics and responsibilities are reviewed in light of the same. The traditional litigation issues of the design professional are introduced and the emerging professional legal issues are considered.

1. Introduction

Sandia National Laboratories (REF) specifies six components of professional ethics and responsibilities for the engineers, scientists, and administrative staff. These components, which apply equally well to the surety engineer, are:

- Quality
- Integrity
- Leadership
- Respect for the individual
- Teamwork
- Self-assessment

Quality includes exceeding customer expectations for performance, costs, and schedule and explicitly planning for and achieving continuous improvement. **Integrity** comprises honesty, fairness, objectivity, openness, and candor. There are several significant aspects of **leadership**, including:

- Anticipating the needs of the nation
- Conveying vision
- Executing innovative and integrated solutions
- Understanding and managing risk
- Setting the standard
- Being courageous
- Being driven by the desire to be the best

Respect for the individual involves trusting and empowering the individual; benefiting from individuality; being sensitive to individual needs and aspirations; and expecting, encouraging, and rewarding accomplishments. The ethical and responsible professional manifests **teamwork** by ensuring shared values and focus, conducting internal and external teaming, and creating mutual benefits and mutual respect. **Self-assessment** involves two major areas: recognizing excuses and self-questioning.

Typical excuses for unethical or irresponsible behaviors include:

- No one will get hurt.
- Well, maybe just this once.
- Everyone does it.
- No one will ever know.
- What's in it for me?

The responsible and ethical surety engineer will neither offer nor accept these excuses. They are warning signals that flag trouble. Questions to be asked in a self-assessment include:

- Are my actions legal?
- How will I feel about myself afterward?
- Am I being fair and honest?
- Will my actions stand the test of time?
- How will it look in the newspaper?
- What would I tell my child to do?

The replies to these questions will expose any ethical problems. Legal problems, however, are becoming more difficult to anticipate.

2. Theory and Principles

Design professionals have not typically been the target of many lawsuits in the past. Contractors get sued far more often than architects, engineers, or other structural designers. A lawsuit is brought to seek legal redress when a legal duty is breached. There are two kinds of **legal duties**, contracts and torts. A **contract** is a binding agreement. A **tort** is any legally wrongful act other than a breach of contract. Examples include defamation, personal injury, and malpractice.

When a lawsuit is brought for breach of duty, the court is called upon to consider the nature of duty. In the eyes of the court, duty considerations (that is, whether a duty is owed and violated) are based on:

- **Magnitude** of injury
- **Probability** of injury
- **Burden** of taking precautions against injury

Professional negligence legally exposes one to third parties, rather than just to the contractual obligor. Design professionals are subject to the **professional negligence standard,** which is a very general standard (i.e., what everyone does) that does not demand perfection. The exception to consider is that professionals may be held to what should have been done (rather than what everyone does). This is exemplified by Judge Learned Hand's "lagging profession" case, in which a professional was held liable for not adhering to what should have been the industry standard.

There are other criticisms of the practice of using professional standards to determine legal liability for design professionals, including:

- It discourages innovation (as do codes)
- It is imprecise. (How can professional standings be defined? Any ranking is a curve. When does someone fall outside a curve?)
- It does not require licensing for professionals who work in house.

3. Applications

A new concept, the **informed standard,** is beginning to come into play. This standard considers whether the professional has kept up with

changes in the field. Continuing education is one way to demonstrate meeting the informed standard. This concept is creeping into the courtroom, although there have not yet been any decisions based on breaching the informed standard. The requirement that one keeps up with the current knowledge in the field is gaining ground. Who defines the current state of engineering knowledge? The courts are the arbiters of informed standards.

Strict liability, which means liability whether or not negligent, is another legal concern for design professionals. Under strict liability, a product deemed to be unreasonably dangerous, despite reasonable care or standard behavior, may subject its manufacturer or designer to a lawsuit. (State-of-the-art is a potential defense, but it is timed to mean the time of the trial, which does not always work in the favor of the defendant.) (Although there has been much popular discussion and comment on a trend toward imposing strict liability, this does not seem to be the case in actual practice. Nonetheless, it is an issue the architect/engineer community should consider.)

There are some changes observable in practice that do affect the design professional. One of these is the new approach to **natural disasters**. In the past, the act-of-God defense was widely used to protect against liability for loss resulting from hurricane, tornado, landslide, lightning, wind, volcano, or earthquake. In these cases, the argument has gone, the cause isn't any fault on the part of the builder or designer, but rather an unpredictable natural occurrence. Fortunately or unfortunately, predictors such as meteorologists, seismologists, geologists, vulcanists, and the like are getting better, and so are designers and engineers. Acts of God are less likely to be a legally determined precipitating event, and professional negligence is thus a more likely decision.

Where is the line drawn and who draws it? The line varies from locality to locality. Local standards prevail, as determined by the court.

Similarly, courtroom attitudes toward **terrorists** and acts of terrorism are changing. After Oklahoma City's tragic Murrah Building bombing, it has become painfully clear that federal/public buildings are fair game in the guerrilla war that some radical individuals and groups are waging against the government. Terrorism is a new concept for many Americans, but the World Trade Center, Oklahoma City, and Khobar Towers bombings have changed our perception. The changing standards make everyone responsible for protecting against both foreign and domestic terrorism.

The defenses of the past, forseeability and proximate cause, are less compelling. While no court is likely to find that a designer is responsible for a third-party crime, it is no longer credible to present a bomb blast as a totally unexpected, random act that could not have been protected against.

4. Summary

The Citicorp Center case discussed earlier, wherein, at great financial and professional expense, William LeMessurier and officials of the Citicorp corporation corrected dangerous errors in design and construction immediately upon discovery of the flaw, is an inspiring example of ethical professional behavior and responsibilities met head on. By contrast, the *Challenger* shuttle

tragedy is an example of a lack of compliance with professional engineering standards. Morton Thiokol engineers warned NASA not to launch under 53 degrees because of the unreliability of the O-ring sealant at cool temperatures. It was 18 degrees. Morton Thiokol management knuckled under to NASA's strong resolve to launch and reversed the engineering decision. Adhering to and enforcing engineering ethics and responsibilities reduce loss.

The changing approach to liability evidenced in our courtrooms would indicate that ethical and responsible behavior on the part of designers who are committed to building surety into their structures would certainly be less vulnerable to lawsuits based on professional negligence. It makes good professional, ethical, and legal sense for today's design professional to ensure the safety, security, and reliability of the as-built environment.

5. Further Reading

Avoiding Liability on Shop Drawings, in *Structure,* pp. 9-12, Summer 1994.

Stanley H. Goldstein and Robert A. Rubin, Engineering Ethics, in *Civil Engineering,* pp. 41-44, October 1996.

Lyman Sandy, Design Professionals, Litigation, and Architectural Surety℠, in *A Conference on Architectural Surety℠: Assuring the Performance of Buildings and Infrastructures Proceedings.* Sandia National Laboratories, Albuquerque, NM, May 1997.

Appendix L

Student Projects

Objectives

The five term projects, submitted by individual students and student teams, show the application to historical events of the surety principles and concepts presented and developed over the course of the semester. The intent of these projects is to provide students with the opportunity to apply aggregated surety information to real-world situations. This experience is expected to provide the student with new tools that can be used in engineering design.

This chapter provides a summary of the five term projects submitted by the graduate students of the Infrastructure Surety class offered at the University of New Mexico in the spring 1997 semester. These subject of these projects include the John Hancock Mutual Life Insurance Building, the Citicorp Center, the St. Francis Dam, the World Trade Center, and the Alfred P. Murrah Federal Building. Surety assessments, analyses, and reports are discussed for each of these subjects.

1. Introduction

Students were informed early in the semester that a term project would be required. They were provided with the following instructions.

Choose one of the case histories mentioned in class, such as the Canadian parking garage, Korean department store, Chunnel fire, Citicorp Center crisis, Oklahoma City bombing, Hyatt Regency aerial walkway collapse, World Trade Center bombing, Hancock Building problems, Kemper Arena roof collapse, Northridge earthquake devastation, Hurricane Andrew, or any of a number of other significant or spectacular failures with surety implications. Please be sure to choose a widely reported failure, so that you are able to gather enough information to draw informed conclusions. Topics must be approved.

At the very least, the study should include:

- Background information with surety importance, such as the geography, location, structural points, size, magnitude of failure
- A thorough description of the engineering features that played a part, for better or worse, in the failure
- A history of the failure. What happened? Why? How far back can the problem, error, or oversight that "caused" the failure be tracked?
- What lessons were learned? What inferences can be drawn? What changes resulted?
- What are the surety issues involved? Were ethics or principles violated? Is this primarily a safety, security, or reliability issue, or is it a combination?

- What recommendations would you make to prevent this from happening again? Are there processes that could be improved or corrections that could be made?

Please bring your knowledge and experience to bear on this project. Your training and talent can bring very significant insights to the surety issues of not only this term paper, but also our industry.

The following five reports were submitted. Figures have been deleted and other minor revisions to the originals have been incorporated.

2. The Murrah Building Surety Assessment

prepared and presented by John F. Wagner and William L. Barringer

Background

Overview

The Alfred P. Murrah Federal Building was built in Oklahoma City, Oklahoma in the mid 1970s. This building was built for the GSA Public Buildings Service. The building was designed for a nine story office building with ancillary buildings. It was located, as most federal buildings, in the downtown area. The site plan for the building is presented in Exhibit 1, which was extracted from reference 1. On April 19, 1995, the building was devastated by an act of terrorism. A total of 759 persons sustained injuries, 167 persons died (163 in the Murrah Building and 4 in other locations), 83 survivors were hospitalized, and 509 persons were treated as outpatients. Of those fatalities, 19 were children. This is the largest number of fatalities of any terrorist act in the United States. (2)

Description

Following this incident, the Federal Emergency Management Agency (FEMA) deployed a Building Performance Assessment Team (BPAT) to conduct a field investigation. Results of findings by this team were published in FEMA Document 277 (1). This document is the prime basis for the following description of the event.

The structural design was a nine story frame with an Ordinary Moment Frame supported on columns. An important feature of the structural system was a transfer girder at the third floor level. The transfer girder supported intermediate columns, thereby providing 40-foot column spacing for the first two levels of the North side. In addition, the curtain wall was set back several feet providing a cave-like space over the first two levels on the North. Ordinary Moment Frame construction and other design features were consistent with current practice and codes of the State of Oklahoma (and Oklahoma City) for buildings in this area and category. The design was for an office complex, therefore a design based on "compartments" would not have given the best use of floor space.

During the investigation by FEMA, it was determined that the design was consistent with other structural designs in the Oklahoma City vicinity for seismic and wind loadings. The investigation found that the building construction was in conformance with current practices and project specifications. Samples of concrete and reinforcing steel were analyzed for conformance and found to meet specifications of the project. The building was designed employing an Ordinary Moment Frame method of design. This method was determined to not provide sufficient redundancy for the building to survive with the loss of

support provided by Column G20. Recommendations from the BPAT suggested that Special Moment Frame designs, or Dual Systems would have been more appropriate for the design of Federal Buildings. These design methods were not available at the time of construction of the Murrah Building, they were available in the mid 1980s - a decade after the construction of the Murrah Building.

History

The blast that destroyed the building was from explosives in a truck parked approximately 15.6 feet from Column G20. The TNT equivalent of the explosives was estimated to be 4,000 pounds. This force caused the removal of Column G20, by brisance, as well as the shear failure of Columns G16 and G24. With the loss of these three columns, the transfer girder supporting the upper portion of the building on the north side collapsed. Most of the devastation was due to progressive collapse rather than the direct results of the explosion. Limit analysis of Column Line G indicated that the frame does not have the capacity to resist its self-weight if any one of the first-story columns on Column Line G is lost.

Column G20 is the key support element is the event. This column was one of the supporting columns of a transfer girder at the third level. The loss of Column G20 caused the transfer girder to collapse. The loss of the transfer girder contributed to the subsequent progressive collapse of the building. The explosion also caused an upward stress on the floor slabs. This type of stress is not normally accounted for in the design of ordinary office type complexes. When the floor slabs were caused to rise, the reinforcing steel was ripped from the slabs which caused them to fail upon rebound. Had the design been compartmentalized, the building possibly would not have sustained such severe damage.

Surety Issues

Overview

The identification of the Surety issues associated with the destruction of the Murrah Building and the loss of 167 lives is the core element of this Surety report. These issues form the basis for determining the Lessons Learned. The Lessons Learned, in turn, drive the process of developing the Recommendations.

In a typical Surety process, the Surety analysis and evaluation would be performed as an integral part of the "design and build" activities. Clearly, application of this discipline at the front end is the most advantageous since it causes safety, security and reliability to be considered from the inception of the project. Surety, in the sense of *prevention,* is the result. In the case of the Murrah Building, the essence of the analysis and evaluation is to determine from the event how Surety can be improved in the design, construction and operation other buildings through Lessons Learned.

In a normal Surety process, equal weight would be given to each of the three constituent areas of Surety: safety, security, and reliability; and all of the various aspects of evaluation within each of these areas would be examined and treated. Basic reliability is demonstrated by the fact that the building was 20 years old and in acceptable operating condition at the time of the incident. In light of the fact that this study is a post mortum of the

terrorist bombing event, the report is focused on two areas:

- Security—Terrorist Threat
- Safety—Post Explosion Activities.

Surety issues are addressed through a three step process.

(1) The first step, as was clearly emphasized in CE 551, is the articulation of the threats.

(2) The second step consists of the examination of the capabilities of the entity in question, in this case the Alfred P. Murrah Building, with respect to the threats. For new construction this step is a requirements development activity. For the examination of an event related to an existing building, such as the bombing of the Murrah Building, this step is, in essence, a vulnerability analysis.

(3) The third step addresses the application of the results of steps 1 and 2 to the facility or building. For new construction, this step would be a part of the design iteration, construction and operation process for the project. In the case of the Murrah Building, this step is a post mortem evaluation.

To structure the discussion of Surety issues related to the Murrah building incident, three key Surety questions are posed:

- **Threats**—What are the Surety threats of today and how do they compare to the Surety threats of the time when the building was designed and built?
- **Vulnerabilities**—What Surety vulnerabilities existed at the time of the bombing?
- **Impact of Surety Considerations**—How would the design, construction and operation of the Murrah Building change with the consideration of today's threats and the knowledge gained from the Murrah Building experience?

The discussion that follows is structured to correspond to these three questions.

Murrah Building Surety Threats

In support of new construction or in the performance of a full blown Surety evaluation, the threat determination process would address all threats and all of the threat environments that would be relevant to the structure. As noted above, this report is focused on the terrorist bombing of the Murrah Building. The threat question in this report, therefore, is directed towards the terrorist. Other threat considerations, such as the natural environment, etc. are not presented.

Two sets of threats: (1) the threats that were in existence and were recognizable at the time that the Murrah Building was designed, and (2) the threats that exist today are considered. The "design" threat is examined because it is important to ascertain whether there were inherent vulnerabilities in the building resulting from not addressing a threat known at the time of design. Of even greater significance from the standpoint of Lessons Learned and Recommendations is the threat of more recent origin that became a reality - a terrorist-initiated 4,000 pounds equivalent surface burst created by an ammonium nitrate and fuel oil ("anfo") bomb contained in a truck.

To succinctly summarize the adversary threats, the Threat Matrices presented in the security portion of CE551 have

Table L-1. Security Threat Matrix, Security Threat, Outsider Adversary Murrah Building circa 1972

		Type of Adversary		
		Terrorist	Criminal	Extremist
Potential Action Likelihood	Theft	VL	H	L
	Sabotage	VL	VL	VL
	Other Hostage	VL	VL	L
Motivations	Ideological	VL	VL	L
	Economic	VL	M	VL
	Personal	VL	M	L
Capabilities	Number	Very Few. Almost no record of attacks by terrorists.	Sufficient to warrant basic concern.	Very few. Sparse record of attacks.
	Weapons	Not sophisticated. Guns, possibly grenades.	Guns, possibly grenades.	Guns, possibly grenades.
	Equipment & Tools	Not sophisticated.	Could have communications, break-in, and/or surveillance eqpt.	Not sophisticated.
	Transportation	Auto; truck, hand carry.	Auto; truck, hand carry.	Auto; truck, hand carry.
	Technical Expertise	Low. Not well organized.	Medium.	Low.
	Insider Assistance	Low probability.	Medium. If money is involved, could be an issue.	Very low probability.

Key: VL = Very Low; L = Low; M = Medium; H = High

been employed. To deal with the issue of initial design threats vs. recent threats, two sets of threat matrices have been created, one for the "as built" condition (circa 1972), and one for the "current threat" condition (circa 1995). They are presented in **Tables L-1** through **-4** below.

Table L-1 presents the Outsider Threat Matrix for the 1972 time period, when the building was designed and constructed. Note that the potential for Terrorist activity is rated as Very Low. There were few terrorist groups known at that time. The rest of the evaluation presented under the column entitled "Terrorist" further supports the conclusion that terrorism was not a major factor in the U. S. or in the Surety of the Murrah Building when it was built.

Table L-2 presents the Insider Threat Matrix for the 1972 time period for the Murrah Building. Under the major heading "Opportunity" all of the evaluation blocks are rated as "High". Opportunity is defined as the conditions and the set of circumstances that make it easy to commit an act of theft, sabotage or collusion. It is not the probability that the event will occur. Because all of the Insiders are indeed inside, are able to come and go as they please and generally, in a stable organization, have the confidence and trust of their

coworkers, Opportunity is understandably high. The key to this High rating is that they are considered trustworthy.

Tables L-3 and **4** present the threat matrices for the 1995 timeframe. Note that **Table L-4**, the Insider Threat Matrix, contains rankings identical to the 1972 Insider Threat Matrix,

Table L-2. Security Threat Matrix, Insider Adversary, Murrah Building, circa 1972

	Access			Opportunity		
Insider	**Asset**	**PPS***	**Vital Eqpt.**	**Theft**	**Sabotage**	**Collusion**
Guard	High	High	High	High	High	High
Nonfederal Company Manager	Low	Low	Low	High	High	High
Nonfederal Company Employee	Low	Low	Low	High	High	High
Federal Manager	High	High	High	High	High	High
Federal Employee	Selective, depending on duties	Selective, depending on duties	Selective, depending on duties	High	High	High
Delivery Personnel	Medium to high	Low	Low	High	High	High

*PPS = Physical Protection system

Table L-3. Security Threat Matrix, Outsider Adversary, Murrah Building, circa 1995

		Type of Adversary		
		Terrorist	**Criminal**	**Extremist**
Potential Action Likelihood	**Theft**	L	H	M
	Sabotage	H	L	M
	Other *Hostage*	H	H	M
Motivations	**Ideological**	VH	VL	H
	Economic	VL	H	VL
	Personal	H	M	M
Capabilities	**Number**	Few to many. Several organizations exist. Few can do extensive damage.	Few to many. Several organizations exist. Few can do extensive damage.	Few to many. Several organizations exist. Few can do extensive damage.
	Weapons	Wide range of weapons easily available.	Wide range of weapons easily available.	Wide range of weapons easily available.
	Equipment & Tools	Sophisticated.	Sophisticated.	Sophisticated.
	Transportation	Auto; truck, hand carry.	Auto; truck, hand carry.	Auto; truck, hand carry.
	Technical Expertise	Adequate to very high level.	Adequate to very high level.	Adequate to very high level.
	Insider Assistance	Medium to high.	Medium.	Very low probability.

Key: VL = Very Low; L = Low; M = Medium; H = High

Table L-2 presented above. Again, the key to the ratings is the "trustworthiness" factor, discussed above, which is the same in both cases.

The Outsider Adversary Threat Matrix, **Table L-3**, for the 1995 timeframe contains important differences from the 1972 matrix of **Table L-2**. In the area of Potential Action Likelihood, the Terrorist threat has increased from Very Low to High under Sabotage and Other - Hostage. Clearly, this condition is a reflection of both the general conditions within the U. S. (and the world) concerning terrorism and the specific event at the Murrah building. Note that the ratings for Criminal and Extremist have also escalated. The Motivations ratings also reflect the heightened present day conditions. In the area of Capabilities, today's terrorists are well prepared, generally well equipped, and most importantly, have easy access to a wide range of weapons, such as rapid fire assault weapons (e.g. AK47's). They have easy access to explosives and to constituents such as ammonium nitrate (fertilizer) and fuel oil, as demonstrated in the Murrah Building bombing, as well as grenades, shaped charges, dynamite, etc. Additionally, as recently demonstrated in the Los Angeles bank robbery shoot out, terrorists have access to highly effective protection gear which

further enhances their capability and their bravado. Table L-2. Security Threat Matrix, Insider Adversary, Murrah Building, circa 1972.

In summary, the terrorist threat is considerably more potent and more probable today than it was in 1972. The weapons of concern include the anfo used in the attack on the Murrah Building, the mixture employed in the bombing of Khobar Towers (a 26kt equivalent blast), very small shaped charges (which in the hands of skilled technicians can cause the same

Table L-4. Security Threat Matrix, Insider Adversary, Murrah Building, circa 1995

	Access			Opportunity		
Insider	**Asset**	**PPS***	**Vital Eqpt.**	**Theft**	**Sabotage**	**Collusion**
Guard	High	High	High	High	High	High
Nonfederal Company Manager	Low	Low	Low	High	High	High
Nonfederal Company Employee	Low	Low	Low	High	High	High
Federal Manager	High	High	High	High	High	High
Federal Employee	Selective, depending on duties	Selective, depending on duties	Seiective, depending on duties	High	High	High
Delivery Personnel	Medium to high	Low	Low	High	High	High

*PPS = Physical Protection system

progressive building collapse as the anfo), and the well known explosives such as dynamite.

Delivery systems range from driving a vehicle to the proximate vicinity of the building for large bombs to hand carrying shaped charges in small cases to critical points in the building or facility. *One of the major findings of the Murrah Building incident is that the destruction of a single support column initiated a progressive collapse that was devastating in its consequences. The well skilled knowledgeable terrorist could produce the same result with a properly placed, very small shaped, charge.*

Vulnerabilities of the Murrah Building

The advantage of a post mortem evaluation is that one can, in some sense of the term, reverse engineer the event to ascertain the vulnerabilities of the structure. In examining the available data, studying the report prepared by the American Society of Civil Engineers and FEMA team (1), taking advantage of the knowledge of the instructors and the guest lecturers in CE 551 (Ms. Eve Hinman and Mr. Tobias Flatlow), and the instructor-led classroom discussions, the following eight vulnerabilities are deemed to be of significance:

- The transfer girder design employed in the north entrance area of the building
- The lack of reinforcing steel in the upper portion of the concrete slab flooring
- The proximity of the building to the street and the ability to park in front of the building at the curb
- The general open bay design of the structure
- The loose mounting of ceiling panels and of ceiling light fixtures
- The use of a glass curtainwall system that shattered in the incident
- Lack of emergency egress keyed to this type of event
- Lack of emergency access for medical, fire etc. personnel.

These vulnerabilities are discussed below. Again, it is most important to recall that this evaluation is a retrospective view - an examination after the event with the advantage of being able to utilize the results of many experts' analyses.

It is instructive initially to consider the first three vulnerabilities from the list: Transfer Girder, Lack of Reinforcing Steel, and Proximity to the Street together. These three vulnerability elements constitute the major factors that, in concert with the detonation of the bomb, led to the progressive collapse of the Murrah Building. To obtain a more concise view of a interrelationship of these factors, a Fault Tree has been developed. The fault tree for building collapse compactly depicts the interaction of these factors as they relate to catastrophic failure of the Murrah Building. The Fault Tree graphically illustrates via the "AND" gating process how these factors must work together to produce the failure.

Transfer Girder Design—As noted in the History section of this report, the north entrance of the Murrah Building was constructed using a transfer girder at the third floor level. The girder supported intermediate columns, enabling 40 foot column spacing for the first and second levels on the north side of the building. The bomb completely demolished one of the

40 foot spaced columns. The transfer girder could not sustain the 80 foot span load and the progressive collapse of the building resulted.

Lack of Reinforcing Steel in the Upper Portion of Floor Slabs—This type of construction is standard for concrete flooring slabs. Reinforcing steel is placed in the lower portion of the slab to provide strength in tension. The normal loading of the floor produces tension in the lower portion. However, the explosion produces overpressure inside the building lifting the floor slabs and putting the upper portion of the slab in tension. Without the rebar in the upper portion, the slab structure failed.

Proximity of the Building to the Street—The building was situated in the downtown area of Oklahoma City. Vehicles are allowed on the street and were allowed to park in the street next to the building. The truck containing the bomb was 15 feet from the supporting column that was destroyed.

General Open Bay Design—This type of design is common to office structures since the open bays afford the user of the facility maximum configuration flexibility. However, compartmentalized design provides a more robust structure under the conditions produced by the explosion of a bomb.

The next four elements lend themselves to evaluation via a Hazard Analysis, a process used in evaluating the safety of a building or facility. The hazard analysis was performed and is summarized in the table presented in **Table L-5**.

The first two rows in the summary table relate to the objects and the debris that are sent flying by the blast of the bomb and the progressive collapse of the structure. These hazards were one of the main causes of injury in the incident.

Loose Mounting of Ceiling Panels and Light Fixtures—These items became flying debris in the explosion and caused many injuries.

Use of Glass Curtainwall Construction—The forces resulting from the explosion shattered the glass. Shards were blown through the office areas, causing injury and death.

The last two items on the list and entered in the Safety Hazards Analysis Summary in Exhibit 9 relate to the access to and from the facility in an

Table L-5. Safety Hazard Analysis Summary for the Murrah Building

Topology/Function	Hazard	Occurrence Likelihood	Severity of Consequence
Loosely Mounted Light Fixtures and Ceiling Panels	Fixtures and panels come loose and cause injury.	Low	Minor to Major - Depending on event.
Glass Curtainwall Construction	Blast loading will shatter glass. Flying shards cause injury and death.	Low	Minor to Major - Depending on event.
Catastrophic Event Egress Routes	Lack of routes in major incident occurrence.	Low	Major - Could cause loss of lives.
Emergency Assistance Access Routes	Lack of routes in major incident occurrence.	Low	Major - Inability of rescue crews to access injured.

emergency situation. Robust entry/exit capability can save lives.

Lack of Emergency Egress—The analysis of the locations and causes of death and serious injury indicated that planned, robust, well marked emergency egress routes can reduce the loss of life.

Lack of Emergency Access—Emergency crews had a difficult time in trying to enter the building and in getting to injured survivors.

Impact of Surety Considerations

The results of the Vulnerability Assessment presented in Section 3.3 above provide the basis for examining the impact that the incorporation of Surety provisions would have on the Murrah Building were it to be designed and constructed today. Accordingly, the discussion that follows is structured to address how Surety can be applied to each of the identified vulnerabilities.

An important point to highlight is the objective of the application of Surety. As Ms. Eve Hinman stated (3), the objective of incorporating Surety provisions is to save lives. Assuring that the facility can continue to be used subsequent to this type of event is not the focus of Surety or of this evaluation.

Transfer Girder Design—The bombing demonstrated that there is no redundancy in the transfer girder design. The loss of one support column led to the progressive collapse of the structure. A more safe design is the use of columns at 20 foot intervals across this entry area.

Lack of Reinforcing Steel in the Upper Portion of Floor Slabs—The "standard" floor slab design considers tension stresses only in the lower portion of the slab. To assure that an explosion and the resultant overpressure which produces upward forces on the slabs will not cause slab failure, reinforcing steel should be used in the upper as well as the lower portions of the slab.

Proximity of the Building to the Street—There are basically three ways to protect the building from an explosion. One is to harden the facility such that it can withstand the forces impinging on it. The second is to create open space between the structure and the location of the bomb. The overpressure drops as a function of the cube of the distance between the bomb and the building (5). However, it must be recognized that achieving the required separation is neither easy nor cost effective in metropolitan areas. As CPTED (Crime Prevention Through Environmental Design) becomes more popular, the creation and use of well designed open spaces may well provide the element of separation that leads to less vulnerable facilities. The third approach is to place blast deflectors in the space between the building and the potential location of the bomb. The analysis of the Khobar Towers bombing (6) provides first order evidence that the Jersey barriers in the proximity of the vehicle carrying the explosives deflected the blast wave and consequently lessened the effect of the explosion.

General Open Bay Design—This design results in large areas that are not directly supported by columns. In the Murrah Building, the bays were 20 feet by 32 feet. From a use standpoint, this configuration provides a large amount of flexibility.

Compartmentalized design, such as that used in the Khobar Towers, provides considerably more robust structural configuration for events such as the Murrah Building bombing.

Loose Mounting of Ceiling Panels and Light Fixtures—The open bay configuration is often accompanied by loose mounting of ceiling panels and ceiling lighting fixtures. Office partitions within the bay are designed to be moved and reconfigured easily. The easy repositioning of lights and ceiling panels is a part of this "ease of configuring" capability. However, in an incident such as the Murrah Building explosion, these loose panels become flying, dangerous objects. A configuration in which there is some "clamping down" of these panels is worthwhile investigating.

Use of Glass Curtainwall Construction—This type of construction is in normal use. In an explosion, the shards and pieces of glass become dangerous and lethal flying objects. Shatter resistant glass, and other types of glass that do not create hazards are preferable for use in office buildings from a safety viewpoint. Cost, however, will be higher.

Lack of Emergency Egress—A key to reducing the number of fatalities and serious injuries is having quick, straightforward routes for exiting the building in this type of emergency situation. As Mr. Tobias Flatow pointed out in his description of the design of the new Federal courthouse in Albuquerque (4), that particular design contains robust emergency stairways that serve as emergency exit routes. Such routes should be designed into buildings.

Lack of Emergency Access—A second key to the minimization of casualties is having access for emergency personnel to get to the injured. Again, Mr. Flatow noted (4) that the emergency stairwells in the Federal Courthouse also serve as the emergency access routes for fire, and medical personnel. As noted above, these routes need to be designed into buildings such as the Murrah Building.

In summary, there are Surety elements that can and should be incorporated in these types of buildings that would considerably reduce the potential for loss of life if an attack of the type perpetrated on the Murrah Building were to occur.

Lessons Learned

Overview

From the specific vulnerabilities determined from examining the events, information, analyses, and evaluations related to the bombing of the Murrah Building, a set of Lessons Learned have been extracted. These Lessons Learned are general in nature. The specific aspects of the event have been discussed in Section 3.4 above. These general Lessons Learned are listed and are discussed below:

- Threats need to be reviewed on a continuing basis.
- Standards and specifications need to be evaluated and revised periodically.
- Key facilities need to be assessed with respect to new and evolving threats on a regular basis.
- Retrofit and upgrade options for existing facilities need to be examined on a periodic basis.

Threat Review

Regrettably, the world is becoming a more perilous place in which to live.

Terrorism is on the rise. Terrorists are becoming more capable, better equipped, and more bold in their activities. The terrorist threat - who, how capable, how well equipped - is in a continuous state of change. To assure that people are as safe as possible, the new and emerging threats must be discovered, recognized, and considered in the design, construction and operation of buildings and facilities. Only by conscious attention on a regular basis will these new threats be identified and placed before the facility designers and architects.

Periodic Review of Standards and Specifications

As the threats evolve, standards and specifications for buildings, facilities, etc. need to be analyzed to assure that they are responsive to the new needs. A periodic Surety review and revision of the codes, etc. that govern the design and construction of facilities needs to be implemented.

Facilities Assessment

Facilities can only be designed to cope with the threats defined at the time of design. As threats evolve, periodic assessments need to be performed. These assessments will highlight the new vulnerabilities that arise as the threat becomes more intense.

Evaluation of Upgrade Options

The major concern, in terms of both vulnerability and of sheer numbers, are the currently existing facilities. To assure that these facilities do not become "Sitting Ducks" - valuable (in use) vulnerable (not robust with respect to the new threats), facility upgrade options need to be developed and tested. A capability to substantially enhance the security and robustness of existing facilities is key to addressing the terrorist threat.

Recommendations

The recommendations presented in this section are broadly based. Specific recommendations focused on just the Murrah Building are of very limited utility since there is no plan to rebuild it. The real pervasive value of performing a Surety evaluation of the Murrah Building and of the bombing is to look beyond the particular event. The Recommendations derive directly from the Lessons Learned. Thus, there is a recommendation corresponding to each lesson learned.

- Set up a panel that will define the Surety Threats and that will review and update those threats on a periodic basis.
- Institute a process in which agencies responsible for standards and specifications will review and revise them on a periodic basis.
- Institute a process for assessing existing structures in the light of new and revised threats.
- Develop a suite of facility upgrade options designed to enhance the robustness of government office facilities to Surety threats.

Implementation of these recommendations will assure that Surety threats are kept up to date with the evolving capabilities of terrorist organizations and other adversaries. Implementation will also provide a process to update specification, standards, etc. to reflect the changing threats and to incorporate new techniques for enhancing performance.

The last two recommendations specifically address existing facilities. Periodic assessment will assure that

buildings initially deemed acceptable do not unknowingly move into the vulnerable category due to changed in the threats. The last recommendation provides a set of upgrade options that can be used as the basis for enhancing the robustness of existing buildings.

References

(1) *The Oklahoma City Bombing: Improving Building Performance Through Multi-Hazard Hazard Mitigation,* The Federal Emergency Management Agency Document 277, August 1996 in conjunction with the American Society of Civil Engineers.

(2) Mallone, Sue; Shariat, Sheryl; Waxweiler, Rick; Hogan, David; and Jordan, Fred, *Physical Injuries and Fatalities Resulting From the Oklahoma City Bombing ,* The Journal of the American Medical Association, August 7, 1996 Volume 276, No. 5.

(3) Hinman, Eve E., Failure Analysis Associates, Class presentation April 14, 1997 @ University of New Mexico.

(4) Flatow, Tobias, Architect, Class presentation April 21, 1997 @ University of New Mexico.

(5) Hinman, Eve E. "Approach for Designing Civilian Structures against Terrorist Attack", *Proc. Structures for Enhanced Safety and Physical Security,* Specialty Conference, American Society of Civil Engineers, Arlington VA, March 8-10, 1989

(6) *Report of Khobar Towers Bomb Damage Survey,* Document provided to CE551 Class by instructors, source unavailable.

Bibliography

Chen, W. F., Editor, *The Civil Engineering Handbook,* CRC Press, New York, NY, 1995

Brauer, R. L., *Safety and Health for Engineers,* Van Nostrand - Reinhold, New York, NY, 1990

Arsenault, J. E., and J. A. Roberts, *Reliability and Maintainability of Electronic Systems,* Computer Science Press, Rockville, MD, 1980

Northrop, J. A., Editor, *Handbook of Nuclear Weapons Effects,* Defense Special Weapons Agency, Alexandria, VA, 1996

Vesely, W. E., and F. F. Goldberg, *Fault Tree Handbook,* NUREG-0492, United States Nuclear Regulatory Commission, Washington, D. C., 1981

Appendix: Khobar Towers Bombing

On June 25, 1997, the Khobar Towers, one of several buildings that were being utilized for military housing in Dhahran, Saudi Arabia, was subjected to a terrorist bombing. Nineteen lives were lost in the attack. The appendix briefly compares the salient aspects of this bombing with the bombing of the Murrah Building. The purpose of this comparison is to determine the additional Lessons Learned that can be extracted from this event. The key elements for the comparison are:

- Threat—What was the size of the bomb?
- Distance—How far was the building from the bomb?
- Protection—Was there any protection from the blast?

- Area Security—Was the area secured and patrolled?
- Causalities—How many people were killed?
- Construction—What was the basic construction of the building?

To address these issues, the Table Presented in **Table L-6** was developed. It compares Khobar Towers and the Murrah Building with respect to these key elements.

As the Table points out, there were important differences in the two events. The Khobar Towers truck bomb was five to seven times more powerful. When evaluating the robustness of the designs of future facilities, these larger values need to be considered. As noted by Eve Hinman, the overpressure drops with the cube of the distance. Thus, Khobar Towers illustrates that separation is a key element in providing robustness. The Jersey Barriers near the blast point deflected the blast wave and provided some protection. This use of blast deflectors, particularly in the retrofit of existing facilities, deserves serious consideration. The area around Khobar Towers had military guards on duty. The truck initially tried to enter the complex but was turned away by the security force. This provided added protection to the complex. The Khobar Towers building utilized compartmentalized construction, which limited the progressive collapse of the structure. The Murrah Building's transfer girder had to support an 80 ft span when the G20 column shattered. The loss of even one human life is a major tragedy. However, is important to note that the combined elements of the Khobar Towers complex limited the losses there to 19 lives as opposed to the 167 lost in the Murrah Building incident.

3. The World Trade Center Bombing: Surety Perspective

prepared and presented by Andrew Gallegos and Thomas Johnston

Background

The World Trade Center occupies a 16 acre site located in lower Manhattan within a very crowded urban area. The site is bounded by West Street and the Hudson River on the west, Barclay and Vesey Street on the north, Church Street on the east, and Liberty Street on the south. The World Trade Center was constructed to "bring together, at one central location, the activities of government agencies and private firms involved in foreign trade, and coordinates under one roof all of the marketing and service aspects of this trade." Located within this facility are agencies such as the United State's

Table L-6. Khobar Towers and Murrah Building Bombing Comparison

Key Element	Murrah Building	Khobar Towers
Threat	4,000 lbs. Bomb	20,000 to 30,000 lbs. Bomb
Distance	15.6 ft	80 ft
Protection	None	Jersey Barriers
Area Security	Military Guards	None
Construction	Transfer Girder Key	Compartmentalized
Casualities	168 Deaths	19 Deaths

Customs, the Commodities Exchange Center, international banks, rail, truck and air carriers. In short, the World Trade Center is New York's headquarters in the Port of New York-New Jersey for America's export-import business.

The construction of the entire site was a very complex procedure which involved many revolutionary concepts due its size and the surrounding environment. The design of the facility also incorporated some concepts that had never been used before. For example, the exterior walls of the World Trade Center were designed as loadbearing walls with most of the steel placed outside instead of inside. Consequently, few interior columns carrying a large percentage of the dead load of the structure were designed or constructed. The reason this concept was used was to provide resistance to large wind loads that were expected. Outside of this application, no extra surety measures to either withstand or detect a terrorist attack were incorporated into the design or construction of this facility due to the fact that at that time, the United States had not experienced a terrorist attack of any kind on American soil.

Description of Event

The World Trade Center was always considered a large threat for a terrorist attack due to its importance, high occupancy rate and the large composition of government agencies within the building. As a matter of fact, in the early 1970's, Central Intelligence Agency (CIA) agents compiled a list of potentially vulnerable sites that they believed might be a high-value terrorist target and the World Trade Center was near the top of the list.

The United States has long had a very poor relationship with the Muslim population of the world. These Muslim groups are known for their tendency to protest the involvement of opposing countries through the use of terrorist acts. One such group is known as Al-Fuqra, which means "the impoverished" in Arabic and is considered the most dangerous fundamentalist sect operating in the United States. One of the leaders of this group, Sheik Omar Abdel-Rahman frequently developed plots and targets that he determined would result in large amounts of damage and fatalities in order to emphasize the determination and power of his organization. Members of this group, such as Nidal Ayyad, a chemist, had technical backgrounds. Others, such as Ahmad Ajaj, allegedly brought manuals on bomb-making into the United States. Others, such as Mahmud Abouhalima, Mohammed Salameh, Ramzi Yousef, and Abdul Yasin lived within the United States and masterminded attack plans. When all of these members put their knowledge together, their potential for large amounts of destruction and death was substantial and their plans and actions resulted in catastrophic events that affected many lives. All of these individuals believed strongly in their cause, were prepared to die for the cause and cared little about the individuals their actions would harm.

The Al-Fuqra, led by the individuals mentioned above, developed a plot to bomb the World Trade Center, the United Nations headquarters, FBI headquarters and the Lincoln and Holland Tunnel. All of these targets were high profile structures within New York City containing large occupancy rates with high government officials and connections. The purpose of the destruction of these targets was to

serve was to cause large amounts of fatalities of both the general public and government employees and officials and to create chaos within the United States government making it difficult to function. Fortunately, the World Trade Center was the only structure that was bombed. If this plot had been executed, it would have created an unprecedented public emergency in New York. In general, the purpose of these bombings was to protest the United State's stance against Muslim actions by causing destruction and death within the United States itself.

The goal of the World Trade Center bombing was to attempt to either destroy the entire structure causing large amounts of fatalities or damage the structure enough to make it non-functional. The terrorists created a large, powerful bomb made of everyday materials that are usually not associated with explosives. These materials were mixed into a paste, placed into plastic bags, and then packed into cardboard boxes. Blasting caps and detonators were then attached to the boxes. These boxes were then loaded into a van that had been rented from the area. This van was then parked on the 2nd parking level below the Vista Hotel within the World Trade Center underground parking facilities. The bomb was positioned to wreak maximum damage to the infrastructure of the building and the commuter network below. The explosives were then triggered from a remote site. This plan was executed very easily due to the lack of security within and around the World Trade Center.

History of Failure

As stated before, the van containing the explosive device was strategically placed to create the most structural damage possible with the hopes that total destruction would occur resulting large loss of life. Despite the fact that the blast created a crater 200 feet by 100 feet wide and five stories deep, the structural integrity of the building withstood the blast reasonably well. The columns, beams and floor slabs within the basement level closest to the center of the blast experienced the greatest amount of damage. Although the explosion ripped apart a giant bracing diagonal between the perimeter steel box columns that form the tower's structural steel tubular framing system, the building was not endangered in any way. According to Eugene Fasullo, the port authority's chief engineer, "The structure took the hit well. One reason is that the towers were deliberately designed with redundancy. They far exceeded the (city) building code requirements for the time." One of the greatest concerns of the structural engineers was the condition of the slurry foundation that was used during the construction of the World Trade Center. At the time, this marked the first use of the slurry foundation-wall method in the United States. Therefore, the structural engineers were uncertain about its reaction to the explosion. Fortunately, the foundation was never compromised due to only minor damage occurring in this area. Although smaller structural damage did occur, such as walls pulling away from columns and shifted elevator shafts, the structural design of this facility never jeopardized the complete integrity of the structure. This design probably minimized the damage to the structure saving many lives.

The most extensive and significant damage as a result of the bombing was not related to the structural integrity of the facility. The most significant problems were caused by the smoke

filling up the structure and the failure of the operational systems within the building. Immediately after the blast, fires quickly broke out launching thick, acrid smoke up hundreds of stairwells and elevator shafts. The explosion hit the communications-operations center for the structure making it difficult to reach police and fire department officials and knocked out power to the entire center. Ruptured pipes dumped approximately 1.8 million gallons of water in the lower levels of the complex. The resulting flooding knocked out all of the emergency backup generators. Due to danger of electrocution and explosion, all remaining power and gas to structure had to be cut off. At the same time, lobby windows exploded onto the plaza below and marble slabs fell from the walls. With no power to the building, people in the elevators at the time of the blast were stranded and those on higher floors were forced to use the stairwells that were quickly filling with smoke with no lighting. Consequently, the area associated with the evacuation of the occupants of the World Trade Center with the loss of power and presence of smoke throughout the structure posed the greatest problems due to the bombing.

All told, the World Trade Center bombing resulted in six fatalities and approximately 1040 injuries. Four of the dead were Port Authority workers whose offices and locker rooms were located on the lower levels that sustained the most damage. Most of the injuries to the occupants occurred due to falling debris, inhalation of smoke or injuries sustained during evacuation. Considering the fact that the World Trade Center contains 50,000 plus occupants and tens of thousands visitors daily and encompasses 12 million square feet, these numbers seem acceptable. The structural integrity of the building was never compromised with the most severe damage occurring near the origin of the blast. Although backup emergency equipment was provided, these systems were located near the blast and were rendered inoperable. Despite the fact that surety issues focused on terrorist attacks were not incorporated into the design or construction, the structure responded well to the incident with minimal loss of life and property.

Surety Issues Before and Immediately After the Bombing

Immediately after the bombing, the safety of the survivors in the building became the most important duty of the rescue team. Unfortunately, when the bomb exploded, it damaged the telephone system, the fire suppression system, and the electrical power. The Port Authority had been in the process of implementing a new safety evacuation plan for just such an emergency. However, the plan was not complete. This left thousands of occupants of the building trapped without any emergency lighting to find their way down the stairwells. It even left one of the principal designers of the World Trade Center, Eugene Fasullo, now with the Port Authority, trapped in an elevator near the 61st floor.

Fortunately, most of the occupants of the building escaped relatively unharmed. There were 1,040 injuries from the blast, most due to smoke inhalation, and only six deaths. Of the six deaths, four were caused by the blast itself and the other two were from debris. One of the major causes of injuries, smoke inhalation, occurred because of the design of the elevator shafts. The shafts helped funnel smoke from fires burning on basement levels

B2 and B5 up to the upper floors. To compound the problem, panicky occupants began smashing out windows in the upper floors, hoping to relieve the smoke. This did not help, however; it merely caused a chimney effect, causing more smoke to enter the upper floors.

The main threats to any bystanders near the building were flying glass and parts of the facade crumbling. Passers by on the street were assaulted by the shards of shattered glass from the panicky occupants of the building, as well as the shattered front window of the Vista Hotel. Inside the lobby of the Vista, marble facades had come loose and some had plummeted to the lobby floor.

In the hours after the building was evacuated, the Port Authority assembled a task force of employees. Their goal was to help the tenants relocate and resume business as soon as possible, as well as to aid in the cleanup of the bomb debris and stabilize the structure. The task force created seventy tenant groups of ten members each to retrieve their valued assets, and later to use free phones and faxes set up in one of the command posts. Since most of the tenants' assets, such as records, were subject only to soot damage, most of the records survived well.

Security before the bombing occurred was wildly different from what it is after the bombing. The World Trade Center was an open building, with over 100,000 people passing through it daily. There were clients, tenants, Port Authority workers, and passengers on the PATH trains that ran under the complex. Access to any public portion of the World Trade Center was open to any person who chose to enter the building. This became an issue before the bombing, when in 1990, the Bureau of Alcohol, Tobacco and Firearms listed the World Trade Center as one possible terrorist threat. The Port Authority decided against any action at the time, fearing a possible loss of business to the tenants.

The parking garage was also raised as an issue concerning terrorist attacks. The parking garage was open to the public at the time, to accommodate the tenants. The Port Authority decided against closing the parking structure to the public, in the interest of the tenants.

The World Trade Center had security systems in place, but they were designed with a different set of threats in mind. The security system was maintained to protect against fire, blackout, or theft. However, the duct banks for the security system as well as the system control room itself were damaged in the explosion. With the loss of communication as well as electrical power, the security system was completely useless.

From a terrorist's standpoint, the bombing of the World Trade Center was not a great success. The building did not come crashing down, nor were there many people killed. However, it was not due to a small or malfunctioning bomb. The main reason for the survival of the World Trade Center lies in the redundancy of the design. At the time of the design of the World Trade Center, there wasn't a second thought given about the possibility of a terrorist attack on the building. Situations such as those had never occurred on U.S. soil, and were unlikely to ever occur. The World Trade Center was designed, however, well above and beyond what the building codes required at the time. Structurally, the building performed

extremely well. After the blast, only those columns that had been left unsupported when the slabs between them were destroyed needed to be braced. In fact, with the explosion occurring on a Friday, the columns were evaluated and braced by the following Sunday.

The heart of the failure of the systems of the World Trade Center lay in their proximity to the bomb site and to each other. Since the telephone, power, fire suppression, and security systems all had duct bank traveling through basement level B2 as well as command centers near B2, they were all rendered useless by the blast. With the loss of all of the systems, evacuation efforts were slowed considerably.

Changes and Recommendations

After the bombing, the task force that the Port Authority formed began to evaluate their current emergency plan as well as to reevaluate the possible threats against the World Trade Center. The task force reversed the previous decision of the Port Authority and made the World Trade Center a closed building. They implemented several changes in the operation of the World Trade Center to harden the structure without expensive structural changes.

As far as the protection of the occupants of the building is concerned, the Port Authority chose to do two things. First, the separate vital systems of the building, daily operations control and security, have been split up and located in different areas. This allows for greater redundancy in an emergency. Second, a beefed-up evacuation plan which includes battery pack emergency lighting and photoluminescent signing for all of the stairwells has been implemented.

Bystanders around the building did not fare badly in the blast since the main danger to people located outside the building was flying glass falling from the building. The Port Authority did not feel the need to upgrade the type of glass used in the building or to apply a mylar coating to the windows. The only other danger was from a marble facade that had come loose in the lobby of the Vista Hotel and fell to the floor. Again, the Port Authority chose not to upgrade the marble, since the damage it caused was merely incidental.

The most important issue to the tenants of the building became their assets. These were often their records. Another part of the emergency plan, which was included in the 1993 bombing, was to protect the tenants' assets and allow them access to their assets as soon as it appeared to be safe for the tenants to proceed into their offices. In response to the full cooperation of the Port Authority, the tenants accepted a closed building policy.

In order to reduce the possibility of another terrorist attack, the Port Authority turned its weaknesses into strengths. The Port Authority decentralized its vital operations and relocated them away from the basement parking areas. The Port Authority removed all on-street parking around the World Trade Center complex and added large concrete planters. This drastically reduces the possibility of a vehicle parking near the complex on the street as well as restricting access to the plaza area with a vehicle. The planters also act as a partial deflection to any bomb blast that may occur from a vehicle on the street.

Below ground, the Port Authority also eliminated parking by the public. The World Trade Center now only accepts monthly tenant parking. The parking spots are only given out after background checks are completed. Each driver is issued a photo identification card and a vehicle placard. A pen-based bar code will identify the driver and the vehicle, and eventually the computer system will monitor the vehicle until it has reached its designated parking space. The Port Authority has also installed anti-ram barriers similar to the ones used in overseas embassies at the entrances and exits to all subgrade parking. The loading docks also have the anti-ram barriers and on-street inspections. For emergency situations, battery-pack emergency lights and photoluminescent paint were also installed in the garage area.

As mentioned before, the structure of the World Trade Center held up remarkably well to a 1,500 pound explosive device. This is due to the design of the World Trade Center. The support for the structure does not rely on a central core, such as an elevator shaft. The support columns are dispersed and linked for moment transfer. The only weakness to the design is the use of floor slabs to provide lateral bracing for the columns. When the floor slab is not reinforced for tension in the top of the slab, and the slab receives blast pressure from below, it will fail. The bombing caused the floor slab above ground zero to fall for this reason. However, retrofitting a slab for this configuration is extremely costly, so it is more important to reduce the risk of an attack.

The Port Authority is looking very seriously at a terrorist attack as one of its possible threats. As previously mentioned, the World Trade Center knew it was a possible target before the bombing occurred, and was in the process of upgrading emergency plans when the bomb exploded. However, the bombing caused the Port Authority to take the matter of a terrorist attack into much stronger consideration as a possible occurrence. The Port Authority now has a plan in place that helps reduce the possibility of a terrorist successfully planting a bomb of significant size inside the World Trade Center complex. The Port Authority focused on the most feasible method terrorists would use to transport a bomb, which is a vehicle, and substantially reduced the ability for an outsider to bring a bomb near to or inside the complex.

By reducing the possibility that a terrorist could bring a bomb into the World Trade Center complex and by providing a buffer zone from a terrorist on a public street, the Port Authority has also reduced the possible consequences of a bombing. A bombing that occurs on the street outside the World Trade Center would be partially deflected by the planters located around the perimeter of the building and would cause a minimum amount of injuries and deaths. Given that this bombing caused six deaths, all to people located near to the bomb, it is likely that a similar bomb would cause only injuries to passers by. Of course, it is impossible to say just how large of a bomb a terrorist might use, since it is hard to gauge what consequences that terrorist wants as a result.

After examining the measures that the Port Authority has implemented, we are in substantial agreement with their plans. However, we believe that further reinforcing, or "hardening" of the parking structures should be performed. It is always possible, given the large number of people who work

in the World Trade Center, that an insider who has access to the parking garage may have malevolent intentions or may be persuaded or coerced into performing a terrorist action. If the insider succeeds in bringing a bomb into the subgrade garage again, the lessons learned may actually aid the terrorist. Since this terrorist event was widely covered by the media, many descriptions of the event and possible failure modes have been published. Without further hardening of the structure, a terrorist with a civil or structural engineering background would be able to determine a better area to locate a car bomb to do much greater damage. While hardening is expensive, it is the best solution, other than removing parking completely, to the insider problem.

Conclusions

For the specific case of the World Trade Center, it was relatively easy to make some recommendations and agree with the plans that have been implemented. One reason for this is that the bombing of the World Trade Center was not much of a success. When compared to other terrorist acts in and outside the United States, this bombing did not cause much damage or loss of life. However, we now live in a more dangerous world, one where government buildings are prominent targets for terrorists. Since many of the public buildings have already been built, designing surety into new buildings will account for only a few of the many targets. One of the solutions for the terrorist threat is to retrofit existing buildings, but this is expensive. Hardening existing buildings also causes excessive esthetic problems. Often a retrofitted hardening of a building would cause it to appear as a bunker. It is unlikely that this will occur unless it is mandated by law. However, the approach that the Port Authority of New York and New Jersey took combined the desire to reduce, not eliminate, the threat, with some compromises by both the Port Authority and the tenants to produce a solution that was cost effective and relatively attractive, although some people appear to dislike the appearance of the planters. This is an approach that someone faced with the task of "hardening" a building should study, since it appears to be a good solution.

Bibliography

Hosenball, Mark. "Another Holy War, Waged on American Soil." Newsweek, February 28, 1993, pp. 30-31.

Iglauer, Edith. "The Big Bathtub." New Yorker, March 16, 1993, p. 33.

Lacayo, Richard. "Tower Horror." Time, March 8, 1993, pp. 25-35.

Lacayo, Richard. "How Safe is Safe?" Time, May 1, 1995, pp. 68-74.

Morganthau, Tom, et al. "A Terrorist Plot Without a Story." Newsweek, February 28, 1994, pp. 28-29.

O'Leary, Jay. "Thinking the Unthinkable." Mechanical Engineering, May, 1993, p. 5.

Post, Nadine. "Much Done, More to Come." Engineering News-Record, February 28, 1994, pp. 30-34.

Post, Nadine, Janice L. Tuchman, Judy Schriener and Howard B. Stussman. "Anatomy of a Building Disaster." Engineering News-Record, March 8, 1993, pp. 8-16.

Puri, Satinder. "Trapped in an Elevator During the World Trade Center Bombing: A Personal Account." Journal of Performance of Constructed Facilities, November, 1994, pp. 217-228.

Ramabhushanam, Ennala, and Marjorie Lynch. "Structural Assessment of Bomb Damage for World Trade Center." Journal of Performance of Constructed Facilities, November, 1994, pp. 229-242.

Smolowe, Jill. "The $400 Bomb." Time, March 22, 1993, p. 40.

Tarricone, Paul. "After the Blast."Civil Engineering News, May 1993, pp. 44-47.

editors, "The World Trade Center Bombing." Parking, October/November 1994, pp. 23-25.

Author Unknown, "The World Trade Center: A Building Project Like No Other." Publisher Unknown -- Source: Rudy Matalucci/Sharon O'Connor, Sandia National Labs.

4. The Citicorp Center Crisis

prepared and presented by James A. MacCornack

Background

William J. LeMessurier, structural engineer, as a consultant to architect Hugh Stubbins, Jr. was involved in the planning for the new Citicorp Center beginning in the early nineteen-seventies. An old decaying church occupied the northwest corner of the one square block site desired by Citicorp. In order to secure the whole block, Citicorp agreed to demolish the old building and build a new church as a freestanding part of the new center.

To provide space for the new church, the fifty-nine story tower was set on four nine story high columns which were located at the mid-point of each side, rather than at the corners, which allowed the corners to be cantilevered out over the church and the plaza below. The structural steel frame is a tube design with lateral stability provided by six tiers of giant chevron braces on each side. The braces were designed to resist perpendicular winds which was the only calculation required by the New York Building Code. A 410 ton tuned mass damper was located near the top of the tower to reduce sway to make the building more comfortable for the occupants.

After the building was completed and occupied, LeMessurier, while responding to a question about the effect of winds hitting from forty five degrees, reexamined the structural system. His new calculations indicated that with a quartering wind four of the diagonals in each tier were unstressed while the other four were doubly loaded. He also became aware that the connections of the braces were

changed from welded connections to bolted connections which were not as strong. He also learned that the braces were designed as truss members rather than columns. The distinction was important because the American Institute of Steel Construction specification requires that connections in columns be designed with additional safety factors. With this new information it became clear that the connections of the diagonal braces, upon which the stability of the entire structure was dependent, were very seriously underdesigned.

The new calculations indicated that the tension force on certain diagonals would be increased by forty percent which resulted in a one hundred sixty percent increase on the connection bolts for the member.

Before making a final judgment on how dangerous the bolted connections were, he turned to the boundary layer wind tunnel laboratory, at the University of Western Ontario, that had performed extensive tests on scale models of the Citicorp structure. The wind tunnel experts confirmed that the forty percent increase in stress from diagonal winds was theoretically correct, but that it could go higher in the real world when strong winds lashed at the building. The wind tunnel experts provided LeMessurier with forces for each structural member in the building, with and without the tuned mass damper in operation.

Working through the wind tunnel members, joint by joint and floor by floor he determined that the weakest joint was at the 30th floor. If that joint failed, catastrophic failure of the whole structure would follow. Calculations of the probability of a storm severe enough to tear the joint apart told him that such an event had a statistical probability of occurring as often as once every sixteen years. When the steadying influence of the tuned mass damper was factored in, the probability dwindled to one in fifty five. But the machine required electric power which might fail during a major storm.

The engineer knew that the bolted joints were accessible and that with money and materials, the joints could be reinforced by welding heavy plates over them. As this was the end of July and the height of the hurricane season was aproaching, he would have to blow the whistle quickly - on himself. After considering his other options, silence or suicide, he decided in favor of disclosure of the problem.

The architect, insurance companies and the owner were informed of the problem and the possibility of a catastrophic failure. The bank's chairman offered his full support in getting the building fixed.

It was decided that the building would not be evacuated and that the repairs would have to be made at night. The city building officials, the Red Cross, and the mayor's Office of Emergency Management were informed of the problems and arrangements made to evacuate the building in the event of a wind alert. Strain gages were affixed to individual structural members and a remote communications center was set up to monitor the electrical impulses. Emergency generators were installed to provide power for the tuned mass damper in the event of a power failure and the manufacturer of the damper would provide full-time technical support.

An advisory group of weather experts, as well as two independent weather forecasters were assigned to provide wind predictions four times a day.

The welders started working seven days a week at night with the building fire alarm system shut off.

On September 1st the weather service received the news that everyone had been dreading - Hurricane Ella was heading to New York. By this time the most critical joints had been fixed and the building with its tuned mass damper operating, could withstand a two-hundred year storm. As it turned out, it did not have to as Hurricane Ella veered out to sea.

Welding was completed in October and the building was now strong enough to withstand a seven-hundred year storm even without the damper.

Structural Lessons Learned

The New York City Building Code required that the building only needed to be designed for perpendicular winds. By contrast, the Uniform Building Code has, since 1964 required that winds be considered coming from any direction. Wind tunnel studies were performed on models of the Citicorp Center and it is puzzeling that winds hitting from forty-five degrees were not considered, especially since in plan it was a perfect square.

It has been recognized for many years in the design of free standing towers, such as communication and microwave towers, that perpendicular winds produce the greatest forces in the diagonal braces and that winds at forty-five degrees produce the greatest forces on the corner columns.

The four columns of the Citicorp Center were located at the mid-point of each side rather than at the corners. In buildings where the columns are located at the corners, broadside wind controls the design of the diagonal braces. Conversely, in structures where the columns are at the midpoint of the four sides, it is the quartering wind that produces the greatest forces in some of the diagonal members. Under a quartering wind, four of the diagonals are unstressed while the other four are doubly loaded.

The designers intrepreted the New York Building Code in such a way as to define the diagonal braces as truss members instead of columns which would have required a greater margin of safety and more bolts.

Lack of Redundancy

The analysis of the Citicorp Tower when exposed to a quartering wind concluded that a catastrophic collapse could occur with the failure of single connection in one of the diagonals. Recognition of the problem in the design phase perhaps would have resulted in a different framing system with increased redundancy. Certainly more bolts would have been used in the connections. The elimination of the corner columns above the 90 foot level does not seem to be justified for either structural or architectural considerations. The presence of these corner columns would minimize the problem with the combination of doubly loaded and unstressed diagonals at the upper levels of the tower. There was apparently split responsibility for the structural design with one firm doing the conceptual design and another firm doing the final design and contract documents. If this was the case, a review system should have been established to maintain the involvement of the conceptual designer throughout the design and construction phase.

Surety Issues

Engineers and architects have the responsibility to minimize the risk to the public and user of the facilities which they design. The concept of infrastructure surety is a risk management approach to identify risk and insure performance of infrastructure when exposed to normal, abnormal malevolent threats. Normal threats could be considered reliabilty issues related to the proper operation and performance of building systems. Abnormal threats would include high winds, fire and earthquakes while malevolent threats would include acts of terrorists, criminals and extremists.

Wind

Wind could properly be considered a normal and abnormal threat. Wind induced movements of highrise buildings can cause discomfort to the occupants and lead to high vacancy rates. High winds having the potential to lead to a major structural failure with its catastrophic consequences is an abnormal threat. In the case of the Citicorp Tower the normal threat, building sway, was addressed with the tuned mass damper, but the abnormal threat, structural failure, was not identified.

Earthquake

In seismic design life safety is the issue, not comfort. In addition to avoiding major structural collapse, the collapse or failure of ceilings, partitions, stairs and elevators must be addressed. The New York City building code did not have any requirements for seismic design.

Fire

Fire in a high rise building is one of the greatest possible threats, because the floors are out of reach of firefighting equipment located at ground level and evacuation is very difficult if not impossible. The smoke from the fire may be more dangeous than the fire itself, therefore provisions must be made to retard the spread of smoke and to provide "safe havens" and smoke free exits.

Terrorism

While terrorism was not a consideration when this building was planned and built, it has elements which could make it a target today, particularity the four large supporting columns at each side. Some of these columns are adjacent to the street and a large bomb could destroy one of them, and compounded by the lack of redundancy in the superstructure have catastrophic results.

Engineering Ethics

The Citicorp crisis created a tremendous ethical problem for LeMessurier and it is commendable that after reviewing the risk that he notified the architect, owner and others about the problem and provided a remedial repair scheme which was undertaken. Problems of this nature, differing only by degree, are often encountered by practicing engineers who must resolve the ethical dilemma. LeMessurier set a high standard in the manner in which he faced his crisis.

Recommendations

Terrorism

Analysis of the wind problems and the implications of bombings such

as Oklahoma City and the Khobar Towers leads to the conclusion that there are strengths in the concept of the Citicorp Center that could be utilized in future buildings.

Buildings on limited sites, such as Citicorp Center, where standoff space is unavailable could be designed to take advantage of standoff height. The Oklahoma City and Khobar Towers explosions have demonstrated that structural damage to the upper levels was not significant. The base structure at the Citicorp Center is approximately as high as the Murrah Federal Building at Oklahoma City which suggests that if the base structure were hardened, the building could survive a bomb blast without collapsing.

The trussed tube rising above the base structure could have the strength to redistribute the vertical forces in the event that one of the four supporting columns was destroyed. The four supporting columns would necessarily have to be very large reinforced concrete elements with great resistance to explosions. The core which contains stairways, elevators and utility chases would be a reinforced concrete structure which because of its location and limited and protected openings have great resistance to an explosion.

The platform on which the trussed tube structure is located should be a heavy cellular reinforced concrete structure with great redundancy and resistance to the blast effects from below.

The structure could be made stronger and more redundant by providing the platform with corner columns in addition to the four at each side. With eight columns, the structure could be designed to survive with the loss of two or possibly more columns.

Cost

As always, the first question will be "what will it cost?"

The cost of the Citicorp Center crisis has been estimated at about 8 million dollars, or approximately 5 percent of the original construction cost, but fortunately, no lives were lost. We cannot put a dollar figure on the Oklahoma City and Khobar Tower bombings where many lives were lost. As engineers we can provide enhanced protection to our infrastructure, but It will be up to all of us to determine what should be the degree of risk that is acceptable and the willingness to pay the price of increased security.

References

Joe Morgenstern, The Fifty-Nine-Story Crisis, May 1995, The New Yorker Magazine.

Stanley H. Goldstein and Robert A. Bubin, Engineering Ethics, October 1996, Civil Engineering.

Max Zar, Towers, Structural Engineering Handbook, Section 24, Gaylord & Gaylord, Uniform Building Code, 1964 Edition.

5. Infrastructure Surety Report on the John Hancock Mutual Life Insurance Building

prepared and presented by Don MacCornack

5.1 Background Information

In 1967 the John Hancock Mutual Life Insurance Company commissioned Ieoh Ming Pei & partners to design their new headquarters building in Boston. Henry Cobb of Ieoh Ming Pei & Partners designed the prominent office tower totally clad in reflective glass. In August 1968 construction started on the Hancock Towers, headquarters for the John Hancock Mutual Life Insurance Company in Boston. The project was plagued with problems that started early and lasted over two years. Even with all of it's problems the building has received awards from the American Institute of Architects and the Boston Society of Architects.

5.2 Description of the Engineering Features

The sixty-two story steel-framed tower is totally clad with story high panels of reflective glass. The 790-foot tall building has an asymmetrical plan of 3 00 feet x 104 feet) The foundation consists of a reinforced concrete mat supported by steel piles driven to bedrock. 32,000 tons of structural steel was used in the original design, the most ever used in any building in New England. The project was occupied three years later than anticipated and at a cost $65 million over the original budget.

5.3. History of Failures

Little specific information is known about the failures because the legal settlement between the John Hancock Company and all the parties involved forbid all consultants from discussing the results of their investigations. What is known about the failures has been learned through the construction industry grapevine. In researching this project, the author contacted a prominent Boston area structural engineer and the regional engineer for AISC. No new information resulted from these contacts.

The Hancock Towers experienced failures in four major areas, failure of the excavation system, excessive movement due to wind, discovery of a potential overturning problem in the primary structural system, and dramatic failure of the glass facade.

5.3.1 Excavation System Failure

The first difficulty encountered in the construction of the building occurred during the site excavation. Because of the poor soil in the area, the building foundation consisted of a thick mat supported by steel piles driven to bedrock. The foundation excavation system consisting of sheet piling and lateral braces moved laterally as much as three feet causing damage to adjacent streets and to adjacent masonry structures. Two of the most severely damaged buildings were the Copley Plaza Hotel and the Trinity Church. The Hancock Company purchased the Copley Plaza Hotel thereby resolving the dispute. The dispute with the Trinty Church was not so easily resolved and the litigation began. After 17 years the litigation was resolved with a $11.6 million dollar award.

5.3.2 Structural Revisions

The building experienced several windstorms during the four years that the building was unoccupied. Each storm seemed to demonstrate another undesirable and unpredictable behavior of the tower. After conducted wind tunnel tests at the University of Western Ontario revisions were made to the structural bracing system. Several studies indicated that the building might have been at risk of overturning. Again the results of the testing and the specific actions taken to stiffen the building are not available to the public. Reportedly 1500 tons of structural steel may have been added to reinforce the building.

5.3.3 Glass Facade Failure

The most dramatic failure on the Hancock Tower was the failure of the glass curtain wall. The original glass panels were constructed of two sheets of glass separated by an air space. The panels of glass started breaking during the construction phase. A severe windstorm hit the Boston area on January 20, 1973 and a number of the glass panels were blown out. No injuries were reported. To avoid further glass failures about a third of the panels were replaced with sheets of plywood. The building soon was known as the "world's tallest wooden building."

After a year of research the decision was made to replace all of the glass panels with panels constructed of a single sheet of tempered glass. During 1974 and 1975 10,344 panes of glass were replaced at a cost of $8.5 million. The change from double pane glass to single pane glass also required upgrading the mechanical system, which reportedly cost several hundred thousand dollars.

There has been a great deal of speculation regarding the possible cause of the glass failure. The original design called for glass sheets larger than any used in past projects, so some speculated that the problem stem from the fact that the larger sheet of glass experienced higher bending stresses. More glass failure was observed near the base of the building, where historically designers have assumed lower wind pressures. Today advances in wind engineering have shown that horizontal vortices or tornadoes can occur near the base of tall buildings.

Others contended that the excessive building sway was the reason for the glass failure. The method of the construction of the double glazed panels is the most rational explanation for the glass breakage to date. The double-glazed panels had a reflective coating applied to the inside of the outer sheet of glass. Continuous lead spacers were soldered between the two panes of glass. Studies indicate that the outer pane of glass may have failed because the lead spacers bonded so effectively to the reflective material. At the time of the Hancock Tower project, reflective coatings on glass was a new concept.

5.4 Lessons Learned

The trend in high rise construction has been to design slender smooth buildings of glass, using fewer materials than previous designs. This trend has caused some buildings to experience motions during intense windstorms that cause discomfort to the occupants. Motion tolerance is subjective and varies from person to person. The wind motion discomfort problem is not new. In 1931 the concern for human comfort was made by a Structural Division Subcommittee

of ASCE. The recommendation of the subcommittee was " that structural frames be so designed as to ensure that deflections will be kept within such limits as to render buildings comfortably habitable." Years ago damping was of little concern of designers because the buildings were more massive and the exterior surfaces had setbacks or were rough which disrupted the wind flow. As the wind meets the face of a tall building air spins off the back of the building in vortices that push the building back and forth. Engineers routinely rely on the mass of the building to resist the force of the wind, the shape of the building to disrupt the wind flow and structural systems to provide the damping.

In some of the more recent high rise buildings something extra was required to steady the building. In the case of the Hancock Tower that something extra was two devices called tuned mass dampers.

Each tuned mass damper consists of three hundred tons of lead set on a thin layer of oil connected to the building frame by huge pneumatic springs. In the Hancock Tower the dampers were located at opposite ends of the 58 floor. Since these dampers were added after the construction of the building the column capacity dictated how high in the building the dampers could be placed. Two tuned mass dampers were used in the Hancock Tower to counteract not only the sway, but also the twisting motion in the wind. Reportedly the addition of the tuned mass dampers has cut the building motion in half. When included in the project design from inception tuned mass dampers reduce the building's motion less expensively than stiffen the structure's bracing system. The sway problem experienced in the Hancock Tower has led to advancements in wind engineering and refinements in wind tunnel testing. Wind testing was not performed as part of the original design of the Hancock Tower. Today wind testing is more common place, but the wind test can cost in the range of $25,000 dollars.

The lesson learned from the Hancock Tower project is that any time you use a system or component that does not have a proven track record, you should proceed with caution, because as T.Y. Lin has stated " extrapolation is extending your ignorance".

5.5 Surety Issues

Our role as engineers comes with an awesome responsibility. Whether we realize it or not, our designs assign involuntary risk to the public and the structures end user. In order to minimize these assign involuntary risks, designers need to embrace the ideas of infrastructure surety. Infrastructure surety is a risk management approach to the design of infrastructure to insure the infrastructure will perform as intended when subjected to normal, abnormal and malevolent threats. Abnormal threats would include earthquakes and high winds. Malevolent threats would include attacks from terrorists, criminal and extremists.

Unfortunately, in the case of the Hancock Tower, access to reliable information has been impossible. As previously stated, an oath of secrecy was included in the terms of the legal settlement. As a result all of the tests and technical analyses have been sealed. Dissemination of technical information about failures is the only way to avoid repeating costly mistakes of the past.

5.5.1 Risk Assessment

Risk assessment is the first step in the design of a project. In the design of buildings the building code provides some measure of risk assessment by providing minimum design loads. The 1964 uniform building code placed the Boston area in a 25 PSF wind zone and a seismic zone 2. Floor and roof loadings, which are considered normal loads, are also prescribed by the building code.

5.5.2 Building Sway

A threat in high rise design is excessive building movement in the wind. From the owner's perspective, if the excessive movement of the tower had not been addressed, continual complaints from the building tenants may have led to high vacancy rates. But more importantly, if not addressed the potential overturning problem may have resulted in a major structural failure with a huge potential loss of life.

Since severe windstorms have a higher probability of occurrence than earthquakes, human comfort and motion perceptibility of wind induced motion perceptibility of wind induced motion is important in the design of structures. Human comfort and motion perceptibility is relatively insignificant in seismic design, where the primary objective is to prevent loss of life and limit damage. However, drift control is essential in order to insure structural integrity and to minimize non-structural damage is essential to assuring life safety. One of the serious potential earthquake dangers is having partitions and ceilings collapse which injure people directly or may block the use of essential life safety services. Elevator shafts are yet another building element, which is vulnerable to distortion damage and is need for life safety after an earthquake. It is clear that adequate drift control is essential to the proper performance of all buildings.

5.5.3 Fire

Fire is another abnormal threat, which is considerably more dangerous in a high rise building, because the floors are out of reach of the firefighters ladders. Paramount in the design of a high rise building is how to safely evacuate the occupants during an fire. Requirements for "areas for evacuation assistance" first appear in the 1991 edition of the Uniform Building Code. The Code provision requires areas of refuge be provided in the exit routes for people who may need assistance in exiting the building during an emergency. The purpose is to provide an area to protect people from fire and smoke until the firefighters arrive. The code does not require these areas to be hardened to resist a terrorist attack.

Stair towers and emergency exits should be designed to remain smoke free during a fire. One method of providing smoke-free exits would be to pressurize the stairwells. The bombing of the World Trade Center demonstrated the need for providing smoke-free emergency exits.

5.5.4 Exterior Facade

Architectural elements attached to the exterior of the structure, such as glass curtain wall, are required to be designed for structural strength of the unit and ductility of it's connection to the structure. The purpose is to minimize the falling of these elements from the building in the event of a severe windstorm or an earthquake. Hazards are created from the failure of these exterior elements. Their connections to the structural frame

must accommodate the movement of the building frame. Some people blamed the Hancock Tower glass failure on the excessive building movement and the glass inability to accommodate the movement. Studies later determined that the glass failure was attributed to the construction of the glass panels and not a result of the building movement. But anytime a failure mode results in glass shards raining down on the streets below, the system and its components warrant an intensive investigation to insure its reliability and safety.

5.5.5 Foundation Excavation

As stated earlier in this report the foundation excavation for the Hancock Tower damaged adjacent streets and adjacent historic masonry buildings. The resulting damage cost the John Hancock Mutual Life Insurance Company millions of dollars. Specific information regarding the depth of excavation and its proximity to adjacent structures is not known.

The engineers had to be aware of the soil's conditions at the site and were probability were aware that some of the adjacent buildings were supported by relatively shallow timber pile foundations. The water table may have been lowered so as to construct the basement levels. A geotechnical firm would have been on the design team for a project of this size.

The design team consisting of the structural engineer, geotechnical engineer, and the architect would have considered the risk of locating a new building, requiring a deep excavation, adjacent to existing buildings. Different foundations systems would have been considered. The architect would want to locate the utility spaces and mechanical spaces in the lower levels, below the street entry level. The basement in as large as the Hancock Tower may consist of several levels containing parking, mechanical rooms, connections to subway trains.

One option may have been to eliminate or reduce the depth of the basement by locating some of the underground functions up in the upper floors. But if the basement could not be revised, the engineer would want to select the foundation system that minimizes the risks to the surrounding structures. Driven steel piles were used to support the mat foundation for the Hancock Tower. The vibrations from the pile driving operation may have contributed to the problems encountered. A better choice may have been augercast piles, which are not driven into place. Safety is a great concern when a deep excavation is placed close to busy downtown streets and structures. The excavation system would need to be carefully studied and the design verified before construction started.

5.5.6 Ethics

There is nothing in any of the literature to indicate any unethical behavior of any of the parties involved. The designers realized they had a problem and developed ideas to remedy the problems.

5.6. Recommendations for Future Projects

As engineers we should convince the public and local building department of the value of independent peer project review of structural designs, because structural failures is one of the most disastrous consequences of human error. The loss of life, injuries suffered, and the cost of property damage is severe enough to warrant the design professional to change the process.

However, as in the case of the Hancock Tower case, the mood following the discovery of a structural problem is not conducive to a dispassionate study of the actual causes.

A few Building Departments require the owner to pay for a review of the structural design by an independent structural engineer as part of the permit process. The building owner is usually not happy to pay for what he see as an additional cost. My personal experience has been that these reviews are nothing more than the reviewer filling out a standard check list, rather than a review of the assumptions, methods, and procedures made by the designer.

A four-point program to restore concern for structural safety in current design practices was recently submitted to ASCE "Practice Periodical on Structural Design and Construction". The third point of the proposed program was for Building Code provisions requiring independent peer review of the structural design, drawings and specifications submitted with the application for a building permit. These code provisions would require the owner to select a review engineer from a list approved by the building department to review the structural design to determine it's compliance with the relevant provisions of the building code. The scope of the review would be custom tailored to each project. The review would at a minimum check the design criteria, verify the foundation design against the geotechnical report, verify that the design is consistent with accepted practice, and perform calculations on representative members. Some engineers are reluctant to embrace these reviews because they feel insulted or threatened when a building department reviewer requests a copy of the structural calculations.

Designers of projects that intend to push the envelope should do research and study any pertinent technical publications to determine if the proposed system or design has a tested track record. Lastly engineers are human and humans make mistakes, but if problems do arise, engineers should always act ethically even if it means losing a client.

5.7. References

Jacob Feld (deceased) and Kenneth L. Carper, Construction Failure

Matthys Levy and Mario Salvadori, Why Buildings Fall Down

Walter McQuade, Why All Those Buildings are Collapsing

6. St. Francis Dam — A Reliability, Safety, and Security Failure: Surety Issues in Action

prepared and presented by Steven Maberry

6.1 Full Faith and Liability

St. Francis Dam—Conceived, Born, & Failed

Spanning the midnight hour between March 12 and March 13, 1928, St.

Francis Dam, a grand achievement of the Los Angeles Bureau of Water Works and Supply, broke. It spilled 12 billion gallons of water, combined it with more than 500,000 cubic yards of landslide soil, and headed down the San Francisquito canyon. Five and a half hours later, it reached the ocean, leaving more than 300 dead, over 100 missing (presumed dead). Strewn in its path were shocked and stumbling

homeless, weeping survivors, and a broken engineering career.

It was not a slow failure. In a rush, cold waters, churning soil, and the full faith and liability of the Los Angeles water bureau destroyed everything in its path by first scouring a water line along the walls 110 feet above the canyon floor. This mass traveled at speeds as high as 18 miles per hour, a sedate rate for a vehicle or smaller phenomenon, but an incredible clip for 50 million tons of indifferent material.

The St. Francis Dam collapse gave California the opportunity to design procedures that preceded other states by decades. Here, we review the calamity for issues specifically classified as "surety." These issues include reliability under normal environments, safety in abnormal environments, and security when there is a malevolent threat.

6.1.1 Background

The St. Francis Dam tragedy began several million years ago. During the Paleocene epoch, a paleo mega-landslide choked off the San Francisquito canyon. This land slide formed a natural dam that blocked the stream and filled the valley with a lake. Sediment from this lake formed a broad flat plain behind the paleo dam.

In geological time, the waters rose and breached the land slide dam. The natural lake emptied down the path toward the sea and left behind an attractive sediment plain. This fine plain drained toward a narrow gap in the canyon walls.

Laying against the east side of the canyon wall, and forming the east edge, were the remains of the massive Paleocene land slide. This landslide material, laminated mica schist, sloped inward toward the canyon floor. Opposite, on the west side of the canyon wall, rested sespe sandstone.

The trap was set. Bated with a broad, high capacity plain that drained toward a narrow channel in the canyon walls, the location beckoned to an engineer. Build here, it said. Build a reservoir here to protect the thirsty city from the capriciousness of the San Andreas fault and to protect them from the maliciousness of the Owens Valley opposition . . . Build here.

William Mulholland heard that call. Years before St. Francis began to take shape, Mulholland noted the broad valley and the narrow canyon drainage, a good place to build a dam.

6.1.2 Construction

The Los Angeles Bureau of Water Works and Supply began building St. Francis Dam in April 1924. Twice, after construction started, they increased the capacity of the reservoir. First, they first added a small ancillary dam extending from the west abutment. This increased the height of the reservoir water by ten feet. They made this change July 1924, when they were only three months into construction. Then again, one year later during July 1925, they increased the capacity by adding 10 feet to the dam's height.

The Bureau completed St. Francis Dam in May 1926. They diverted water from the Owens aqueduct into the reservoir several months before completing construction. One year after substantial completion, during May 1927, the reservoir reached a level three feet below the crest of the dam.

During the months of filling in 1926 and 1927, several transverse cracks

appeared in the dam. The sespe sandstone formation on the west side also drew attention because of its propensity to swell and leak. Spring runoff ceased in May 1927, and the reservoir level began to recede.

Early percolation tests in the sespe sandstone on St. Francis's west side suggested that it was a good formation for their future dam. It is true that the water level in the perc test pit did not fall appreciably. The testers did not realize, however, that the sespe formation was actually "melting" from the sides, swelling, and filling the hole- - masking the loss of water through seepage.

After construction, it was this west abutment in the sespe formation that drew all the attention. Water came through the sespe formation and through an exposed fault line where the sespe met the mica schist. They filled cracks in the dam and installed conduits to drain off flows. They watched the flows for signs of piping.

In 1928, the spring runoff began arriving in January. Again, water from the Owens aqueduct flowed into the reservoir. The water level behind St. Francis passed the previous year's high watermark. It reached maximum capacity on March 7, 1928.

6.1.3 Failure[1]

As the west side sespe sandstone absorbed water and swelled, it heaved against its end of the dam. Meanwhile, the east side also absorbed water, but there, the effects were different.

Laminated mica on the east side contained or laid on shale, clay or other materials in layers that absorbed the water. These hydrophilic layers expanded, and lubricated the laminations. Water drawn (by capillary action) into the soil above the water line increased the gravity load on these weakened areas. The land began to slide, slowly, toward the dam's east abutment.

Now, caught between the swelling sespe on the west and the sliding mica schist on the east, huge lateral forces pressed against the slightly curved dam. This incipient landslide and the swelling sespe were "thereby progressively distorting the distribution of stresses within the structure (and negating most of the dam's conventional loading assumptions)."[2]

Those loading assumptions were based on gravity dam behavior. In a gravity dam, the dam resists the pressure of the water behind it with its weight acting on a lever formed by the dam's base with the downstream toe as the fulcrum. As noted earlier, they increased the capacity of the reservoir twice after construction had begun. The increase was a total of 20 vertical feet.

A gravity dam depends upon its weight and the width of its base to resist the overturning forces of the dammed water behind it. Increasing the capacity of this type of dam by merely extending the height of the crest or the reservoir is anathema. The increased load and increased leverage from the pressure of the water acting against the upstream face increases the needed moment (leverage) along the base of the dam. There is evidence in the construction pictures that the buried base of the

---

[1] *This description of the failure is a reasonable interpretation of the existing evidence-- after the event. It relies heavily on Rogers's conclusions in his work (See references). However, it does not follow Rogers's work exactly. Any errors in interpretation are my own, and not the fault of Rogers.*

[2] *Rogers, page 53.*

dam was not even as wide as the design drawings showed.

Post failure analysis suggests that the dam was inadequate for this mode of failure. The outcome was that the gentle arch of the dam carried part of the overload into the abutment soils on the west and east. Some dams do carry loads like this; they are arch dams. St. Francis was not designed as an arch dam, but its inadequate function as a gravity dam turned the gentle curve into a source of structural resistance.

So, St. Francis Dam had gently swelling sespe sandstone pressing against its west end, and an incipient landslide pressing against its east end. Inadequate base/weight further compromised its behavior and carried forces along the arch into flawed side formations. As if that wasn't enough, uplift forces from the water seeping into the rock formations around the base lightened the assumed acting weight of the concrete dam. "Many engineers were just beginning to appreciate the destabilizing effects of uplift pressures in the late 1920's, when the dam failed."[3] Although there was stinging criticism about this aspect after the failure, the St. Francis designers had, at least, the newness of engineering understanding of this detail as an excuse.

On March 12, 1928, St. Francis dam sat against these flawed formations, improperly using them as braces against overturning forces, and struggling against the water seeping into its deep foundations trying to lift it from its seat. The lateral forces pressing from the west and east bowed the dam upward and formed two sets of cracks along each abutment. These cracks were interpreted as shrinkage cracks rather than as tension cracks formed by the side pressures trying to fold the dam upward and inward toward the curvature axis. Water soaking into the foundations applied increasing uplift pressure.

This day, March 12, Tony Harnischfeger, the dam tender, called William Mulholland with concerns about the water flows from the western (sespe sandstone) foundations at the downstream base of the dam. Mulholland and his trusted associate, Harvey Van Norman, inspected the offending area. Tony was right to be concerned, but tracing the flow to its source revealed that the water, surfacing from underneath the dam, ran clear. Clear water meant no erosion; no erosion, no piping. Since the foundation was not piping, the leak was an expected effect of the dam and would not lead to further degradation of the foundation. The two engineers also noted some cracks (and water flows) in the concrete dam itself. Massive dams always have cracks. They had been chasing and monitoring several cracks along both abutments. These cracks and the foundation leaks were just more of the same problems they had already experienced. This kind of stuff was more a public relations, or perception problem, than any real threat-- so long as it didn't start piping. Or so they thought.

Later, some time before midnight, Tony and Leona Johnson, his common law wife, awoke to strange things. There was a noise, like some distant high-pressure nozzle spewing out caustic water, and an unnatural mist/fog turning the canyon into a surreal landscape designed by a nightmare.

Tony and Leona, now wide awake and dressing to investigate the strange things, must have wondered if maybe

---

[3] *Rogers, page 30.*

the engineers had erred. They left their home, downstream from the dam, and started toward St. Francis to see what was causing this noise and the eerie mist. Unknown to them, the incipient landslide was more insistent and pressed harder against the dam. Lateral pressures grew. St. Francis deflected, and the tension crack on its east side opened just enough to allow full pressure orifice flow. It roared, filling the canyon with that unnatural mist.

Geology and concrete shift to fit changing conditions. Support structures and load paths reorganize--somewhere upstream, support vanishes. The incipient landslide becomes full fledged. In and above the reservoir, the mica schist gives way. It drops like a curtain into the lake. Landslide soil billows in the water and riots around the reservoir. It slams against the dam, nudges the top toward the downstream side, and sloshes back. With the loss of upstream support and the riotous shoving of the dam, the east foundation cannot take anymore. It joins the riot, plunges down and sweeps away the eastern quarter of the dam.[4]

At 11:57:30 p.m., a Southern California Edison Lancaster power line failed, as if it were cut. It ran along the eastern abutment of St. Francis Dam. Tony's body was never found, neither was his son's. Leona's body was fully clothed and upstream from her home, between it and the dam.

As water/soil flows began progressing toward a discharge rate of 1.7 million cubic feet per second. The flood scoured a deep hole underneath and to the east of the central dam section. This central concrete block teetered on the edge of the hole and twisted with the rushing water. The tension cracks between the center and the west abutment gave way, and this central block tilted toward the hole. Eastern sections of the block sheared off and plummeted into the rushing scour hole. However, in all this violence, the reservoir made a new path. It attacked the jumble of released blocks around the west tension cracks, swept them up in its awesome flow, and carried them away.

The flow tapered. Powerful forces abated at the dam; instead, they accompanied the massive flow on its journey to the sea. The central block of concrete remained standing. The scour hole filled as quickly as it formed. The reservoir was empty.

Downstream from St. Francis, a wall of water scoured the canyon. It marked the sides with a waterline as much as 110 feet above the canyon floor. Confined in the canyon, it traveled 1.5 miles in five minutes, 18 miles per hour. It encountered Powerhouse Number Two and wiped out 120 employees and dependants of the Bureau of Power and Light. It continued to where the San Francisquito met the Santa Clara River.

Slowed now to a little more than 12 miles per hour, this gush of water, soil, and debris, turned right, spread out, and plowed the next ten miles into a bare ruin. Its height had now dropped, but it was still over 50 feet. Seventeen miles from the dam, the St. Francis flood collided with an Edison construction camp. At one hour and fifteen minutes after midnight, this

---

[4] There is little debate that the fundamental cause of the St. Francis dam failure was a massive, and sudden, foundation failure. However, as the detail in this description gets finer, the possibility of error gets greater.

night goblin passed over the tent camp. It left in its wake the dead, the injured, and the frightened. Some survived; 84 of the 150 were left dead.

After the Edison camp, it spread out, began to slow below 12 mph and merely damaged its path so that ". . . two-thirds of the valley was waste."[5] From the town of Fillmore to the sea, in this last 25 miles, the widening valley absorbed and cushioned the wall of water, but it resulted in extensive damage anyway, all the way to the sea. It traveled this last bit between five and 12 mph. "[T]he evacuees would number in the thousands."[6]

Nearly fifty-four miles from St. Francis Dam and five hours, 27.5 minutes, from the time of the failure, the reservoir that once stood behind St Francis dam emptied into the ocean. It carried debris, soil, and some of the dead in a discharge flume for miles. It averaged 9.8 miles per hour from beginning to end.

6.1.4 St. Francis Dam and Surety

The St. Francis Dam failure provides an opportunity to look back at serious civil disaster without recriminations that might become implied in more recent disasters, where the victims and responsible parties might still be suffering. The obvious issue is reliability.

Under normal conditions the dam failed. The flood carried away lives, property and reputations. How did the structure become so unreliable? Los Angeles Bureau designer/builders constructed 19 dams before St. Francis, and by that they earned an appropriate reputation as authorities in large dam construction. Some, but not all, of the lack of reliability can be blamed on a lagging state-of-the art in gravity dam design and in geotechnical information. There were, however, issues of design that fell well within the engineering understanding of the time.

Beyond the issue of reliability, there was little thought given to processes in the abnormal environment of a failure. As time has unfocused the accusations with fading memories, one can study how thinking about "what if" conditions of low probability (a dam failure is a low probability) would have cost essentially nothing and saved dozens, maybe hundreds, of lives.

Finally, the operators of St. Francis Dam had evidence that it could be a target. Serious adversaries from Owens Valley had proven their capabilities by several assaults on the system, sometimes characterized as a near state of civil war. Today we would call their acts "terrorism." Owens Valley residents had serious grievances with the Los Angeles Bureau of Water Works and Supply. It was their water that the city transported away to fuel urban growth. These people proved that their capabilities were great enough to be a serious threat. Security at St. Francis Dam, however, was completely reactive; security responded only to reported assaults, without the benefit of forethought or security components.

---

[5] *Outland, page 134.*
[6] *Outland, page 99.*

6.2 Reliability

6.2.1 Definition

Turning to standard English references, the following definitions for reliability[7] are unsatisfactory:

reliability (n)

1: the quality or state of being reliable

reliable (adj.)

1: suitable or fit to be relied on: dependable

rely

1: to be dependent <the system on which we *rely* for water>

2: to have confidence based on experience
<someone you can *rely* on>

From this, a definition for reliability, when applied to infrastructure, is *the quality or state of being suitable for us to be dependent upon.*

A dictionary of computer terms defines reliability as the following:

1: the degree to which a computer, a device, or a software application can perform with a minimum of errors.[8]

While neither of these definitions is objectionable, the best definition for reliability applied to a dam is:

> Reliability is the *probability* that a system will perform its *intended function* adequately for a specified period of *time* under *stated conditions.*[9]

The useful detail about this definition is that it provides several opportunities to assign appropriate designated standards. These are *probability, intended function time,* and *stated conditions.*

With civil structures, we do not talk about "a minimum or errors," as in the definition applicable to computers. Instead, the goal is a *very high* "probability that a system will perform . . ." The public expects civil structures to perform at near 100% reliability[10] under expected (normal) conditions. The only debate available is the definition of normal conditions. Normal conditions include use for the intended function, for an acceptable time (design life), and some standards of conditions.

6.2.2 Los Angeles Water System Reliability

The intended function of the St. Francis Dam was, ironically, to increase the reliability of the water supply system to Los Angeles. San Francisquito Creek was not originally part of the water supply rights to the reservoir behind the St. Francis Dam. Although Los Angeles began seeking water rights out of the creek, they did not possess them when the dam failed. The reservoir served as storage for

---

[7] *Definitions from Merriam-Webster's Collegiate Dictionary, Tenth Edition. 1993-4.*

[8] *Definition from the 21st Century Dictionary of Computer Terms from the Philip Lief Group, Inc. 1995.*

[9] *The final definition here was the working definition, quoted for use in a civil engineering graduate course at the University of New Mexico, Spring 1997. Course Instructors: Rudy Matalucci and Dennis Miyoshi. Origin of quote unknown.*

[10] *". . . The expected reliability of most civil engineering systems will be in the range of 0.95 to 0.99." From Reliability-Based Design in Civil Engineering, 1987. Author and publisher not known. Source is notes from UNM graduate course.*

Owens Valley water brought in by an aqueduct.

The aqueduct carrying water from Owens Valley to the city crossed the San Andreas fault at the Elizabeth Tunnel. After an earthquake, repairs to this tunnel "could take more than a year."[11] William Mulholland recognized that the city was vulnerable to water supply loss. The Bureau of Water Works and Supply needed more storage, and it needed it close to the city where the supply would be less vulnerable to earthquake disruption. Additionally, in 1924, Owens Valley residents took "the law into their own hands, settlers began a campaign of sabotage against the Los Angeles Aqueduct that would keep the valley in an intermittent state of siege for three years."[12] The distance of the water source (Owens Valley) from the water users (Los Angeles) made the supply vulnerable. The San Andreas fault made this vulnerability a near certainty. Considerations of sabotage from Owens Valley residents also played a small part in evaluating the required reliability of the water source.

The reservoir behind St. Francis Dam was the solution to that reliability problem. The bureau turned Owens Valley aqueduct water into this reservoir to provide reliable storage for Los Angeles water.

6.2.3 St. Francis Dam's Reliability

Within the reliability definition that includes probability, intended function, time, and stated conditions, St. Francis Dam was unreliable. The original intended function was changed twice during construction when they decided to raise the water level. This statement of intended function should have stimulated a feedback loop that recognized required design changes necessary to meet the newly defined function. The dam lasted only five days (from March 7 to March 12) at maximum pool level. The conditions on March 12, 1928, were not abnormal. Because it is after the fact, we know that the probability of failure was 100%. Inquiries into the probability of failure, armed with the progress of knowledge about dam behavior since the failure, would also lead one to an unacceptable conclusion (even without hindsight).

Some things were unknown, or poorly circulated, that excuse some design deficiencies. Uplift forces fall into this category. However, a similarly designed dam, the Mulholland Dam, included the improper understanding of uplift forces and continued to function.[13] The raising of the reservoir elevations without design review is puzzling. More extensive consultation with geological experts *may* have prevented a horrible tragedy.

6.2.4 William Mulholland

William Mulholland ran a massive effort that transformed a struggling burg into a powerful metropolis. He believed in the effort. He became, for many, the symbol of that massive effort. It made him a hero to Angelinos and a villain to others who saw it as water theft.

Mulholland chose the site for St. Francis Dam, and he was the head of

---

[11] *Rogers, page 19.*
[12] *Outland, page 23.*

[13] *Armed with new understanding, the Los Angeles Bureau of Water Works and Supply undertook a retrofit of Mulholland Dam in 1932. Because it was a similar design, Bill Mulholland ordered the lowering of the reservoir in this dam after St Francis failed. Mulholland Dam (later Hollywood Dam) shared the same uplift problems, but not the foundation problems.*

the bureau that designed and built the dam. However, St. Francis "was only one part of a whole. The only part which failed. The rest has held. The whole system has held. Because it has integrity."[14] This speaks volumes for the competency of the people involved in building this system.

Mulholland did not design the dam (it was designed by his engineering office), a detail neatly overlooked by those willing to focus blame on him. He also did not directly oversee the construction process (that was Stanley Dunham). He did, however, design the system that produced the design and construction for the St. Francis Dam. Here lies, perhaps, a weakness that contributed to failure. William Mulholland was 67 when design began for St. Francis. He was 68 when construction began, 71 when it was completed.

"Bill Mulholland was, simply put, a giant of his time."[15] He was an Irish immigrant, arriving in the United States as a journeyman sailor at the age of 18. In 1877, he reached California. In California, he went to work for a Los Angeles private water company. He was 22. Mulholland became interested in technical aspects and decided to become an engineer. At the age of 30, in 1886, he became chief engineer of the Los Angeles water supply system.

In those years, university education was not a requirement for entering engineering. Apprenticeship traditions were far stronger. "Much of Mulholland's success was drawn from his habit of reading the leading technical literature while working with some of the best water resource engineers of the era."[16] William Mulholland then became, in his turn, one of the best water resource engineers of his era.

"Perhaps more than anything else, Mulholland enjoyed a reputation as a person who could get big things done. He possessed a charismatic persona unusual for an engineer, and his workingman viewpoint made him a champion of construction workers and water and power employees . . . . The personification of a field general, he surrounded himself with talent. The young engineers he hired, people such as Harvey Van Norman, Edward Bayley, Charles Lee and Ralph Proctor, were men not unlike himself: hardworking, to a large degree self-educated, and possessing a willingness to work in the field under difficult conditions."[17,18]

These men, and others, called Bill Mulholland "the Chief," and they meant it like a royal title. Mulholland's exceptional competence cast its great shadow over the work of the bureau. The Chief's willingness and ability to dominate the undertakings gave the other talented and not-so-talented

---

[14] Mulholland, page 134. She was quoting Richard Callison (personal conversation), a young Los Angeles Water and Power engineer—1989. There is an additional point of fact. The Upper and Lower Van Norman Dams, important parts of the system, also failed, but during an earthquake. They were partial failures, but the reservoir in the lower was only half full (the preceding winter was dry). Had the upper failed more fully, it would have cascaded to the lower. If that had happened, or if the lower had been full, the event may have challenged the St Francis failure.

[15] Rogers, page 3.

[16] Rogers, page 4.

[17] Rogers, page 5.

[18] These self-educated engineers who worked for Mulholland left independent marks on the profession themselves. For example: "The fundamentals of compaction of cohesive soils are relatively new. R.R. Proctor in the early 1930s was building dams for the old Bureau of Water Works and Supply in Los Angeles, and he developed the principles of compaction . . . In his honor, the standard laboratory compaction test which he developed is commonly called the Proctor test."

engineers relief from responsibility for their own judgments.

6.2.5 Succession of Institutional Responsibility

In 1911, when the bureau built the aqueduct across the same mica schist formation that would later destroy the St. Francis Dam, Mulholland recognized its geological significance.[19] Where was this insight when excavation advanced on the east embankment?

When he proposed the Owens–Los Angeles aqueduct, a precedent-setting massive undertaking, he convened a peer review board of outside consultants (in 1906). The absence of outside geological or engineering consultants on the St. Francis Dam is striking.

A peer review board might have contained someone who was more concerned with the recent knowledge about uplift forces. Several, with the benefit of hindsight after the failure, were quite critical of this aspect. A review board could have dredged up concern about the sespe formation. It was weak and slacked under emersion. Maybe somebody would have even noticed the paleo-mega landslide when they returned to check out site concerns. Mulholland himself might have reviewed his earlier cares from when he constructed the aqueduct in 1911. A year after the St. Francis Dam catastrophe, a peer review board prevented a dam disaster when a member of that review board recognized a similar paleo slide in San Gabriel Canyon.[20]

One often sees it. The cult of personalities on the political scale is a matter of recorded history. Alexander the Great, Julius Caesar, Mao Zedong, and Fidel Castro are just a few. Sometimes we fail to recognize that it also happens when a very competent person controls an institution that is less than a nation or national army.

Privately held companies recognize the problem so clearly that at least one business association, the Association of General Contractors, consciously addresses this problem with management succession conferences for their membership. Private businesses are notoriously vulnerable at this stage, where one competent generation must succeed another. No transferral of authority (and power) was underway at the Bureau of Water Works and Supply when the St. Francis Dam faded; this was true although its leader for the past four decades was 72.

6.2.6 Peer Review

Perhaps the very success of the bureau was cause for its leadership to overtrust its own capabilities. This behavior may then have worsened the possibility of a tragic event by holding

---

[19] This conclusion, about Mulholland's insight into the mica schist, comes from Rogers who quotes a Mulholland report on page 22 in his work. His source for the quotation is Outland, page 37. About the east canyon wall of San Francisquito canyon, Mulholland wrote: "As the face of the canyon . . . is exceedingly rough, and the dip and strike of the slate such as to threaten slips, in case side-hill excavation were made, this portion of the line was also placed well back under the mountain and will be constructed from adits run in from the canyons . . ."

[20] Interestingly, the peer review member who recognized the paleo-slide, geology professor George Louderback, served on the first inquiry into the St. Francis failure. That board concluded that the failure was due to piping through the fault line on the west embankment where the sespe formation met the mica schist (not likely, piping failures are progressive— slow by nature, and much more material was absent from the east canyon wall after the failure than from the west). Louderback missed the mega-landslide formation in San Francisquito Canyon.

up as an example of success to younger engineers this rugged individualist competency.

The competency of the individual at the top, and probably of the talented engineers with whom he surrounded himself, may have ensured that even a peer review panel could have missed the weaknesses of the dam site. However, the chances of this oversight would have been greatly reduced. The past success and the leading work that this team completed gave them the right to believe they were the best.

The evidence that the base of the dam as constructed or as designed was not wide enough for gravity dam behavior, even without the uplift pressures, is troubling. A review process would have either caught this or caused more careful internal review before it was submitted to an outside body.

An outside review of the site and design might have caught the weaknesses (like it did at San Gabriel Canyon). Even if a review panel *had missed* the danger, the participation of the panel would have increased the probability that the dam followed or exceeded the known physical science standards of the day. If such a process *had* still managed to lead to the St. Francis Dam design, it would have been little comfort to the victims, but it would have been great comfort to William Mulholland and his people.

6.2.7 Reliability Revisited

By any standard, today's or the standards of 1928, St. Francis Dam was unreliable. The foundation was unreliable; the design was unreliable.

Considering the capabilities of the team of engineers who were directly and indirectly responsible for the dam, there is some arrogance in drawing this conclusion almost 70 years later. The very competence of the team was one source of the reliability failure.

As the leadership aged,[21] continuing with the way they were was more comfortable than starting the necessary adjustment. They ignored the changes that were occurring to their leader and to themselves. A smooth transferral of responsibility was required, but they ignored it.

Maybe as part of this confidence in the infallible Chief or in themselves, they also felt no impulse to seek outside consultants. A formal review board, like that convened for the original aqueduct, would have served very well to increase the probability of success. Worst case, this board would have reduced some suffering of the responsible individuals, including Mulholland. Best case, the whole thing might never have happened.

6.3 Safety

6.3.1 Definition

In the general meaning of the term, safety is implied under an umbrella of reliability. If something is reliable, it is safe. Here, though, we would like to separate the definition of safety from that of reliability. Reliability anticipates completing an intended function under *stated conditions*. Those stated conditions would be a *normal* environment.

---

[21] *"The unremitting strain and worry of the water war between Los Angeles and Owens Valley, along with his customary hands-on management of the city's department of water and his exertions on behalf of the Boulder Dam project, had taken their toll on the aging man. His extraordinary vigor had long allowed him to maintain a pace arduous for a man of any age, but intimations of mortality had begun to encroach." Mulholland, page 118.*

What we would like to separate out is a definition of safety that is about behavior during some low-probability *abnormal* environment. Engineering does this often. Generally accepted procedures in engineering practice anticipate the possibility of some kind of abnormal condition[22] and then endeavor to limit the harm or injury.

Application of this practice, designing for abnormal environments, results in a safer structure or system beyond the issue of reliability. Under this definition, a safe design continues to function in some abnormal environment to a degree that protects the public, even if the structure itself is sacrificed. This safe design might include procedures *and* physical components.

6.3.2 St. Francis Dam and Safety

If we separate safety this way from reliability, we find that, under this definition, the St.Francis Dam lacked safety. The issue here is the absence of engineering thought given to the abnormal environment of a dam failure. No one gave thoughts to procedures or response that would mitigate harm and injury if this, or any dam, in the Los Angeles system, should fail.

Mulholland and Van Norman both arrived at St. Francis Dam "within two hours after it went out . . ."[23] Two hours after it went out, the Edison construction camp had been dead for 42 minutes. The Edison camp was 17 miles from the St. Francis Dam site. Mulholland and Van Norman lived in Los Angeles, some 40-plus miles from the dam.

The timeline suggests here that the two engineers received notification from someone within the system who could even more easily have notified the Edison camp. The flood took an hour and eighteen minutes to reach that camp. The camp had a night security officer and was connected to telephone service. With minutes involved in the emergency, we can understand how a temporary construction camp set up downstream might fail to be remembered by whoever notified the Chief.

"Why was an immediate warning not flashed to the Santa Clara Valley? The plausible answers are the dispatchers did not realize the terrible urgency of the crisis, and even if they did they were not familiar enough with the terrain to know the path the flood waters would take."[24]

6.3.3 Emergency Procedures

The key here would have been to give thought to the improbable (but possible) abnormal environment of a dam break. If the bureau had asked the question, "What if a dam breaks . . .?" and answered it with an

---

[22] Examples of this "abnormal environment" thinking abound in engineering. The most well known is probably the design efforts to protect building occupants during the abnormal environment of an earthquake, previously considered an unavoidable "act of God." There is also the careful design of reinforced concrete so that the a reinforced concrete component failure is ductile rather than brittle IF it happens to be loaded beyond its "normal" design strength.

[23] Mulholland, page 137. Catherine Mulholland is quoting the Chief's testimony. There is some debate as to when Mulholland and Van Norman were actually notified. Outland questions this testimony because of the distances and travel time involved. Catherine Mulholland misses the significance of this debate when she concludes that Van Norman and her grandfather were notified earlier than 1:09 a.m. and points out that the chauffeur was Mulholland's live-in son. No matter what the interpretation, the Edison camp died unnotified.

[24] Outland, page 96.

appropriate response, hundreds of lives could have been saved.[25]

Further downstream, local sheriff and police departments begin responding as the warning finally out-raced the flood. Here, even with the warning, many had to risk their lives to carry word to others. Telephone operators stayed at their telephone exchange locations, calling households to awaken them and warn them to evacuate. Several locations for these telephone operators were themselves vulnerable.

Coordination of effort was nonexistent. The successful evacuation of thousands worked because neighbors worked for and with each other and because that night, little heroes were active everywhere.

The Bureau of Water Works and Supply had no emergency plan. Had they participated in what we can call here "surety thinking," they would have produced and promoted a system of handling dam break emergencies.[26] Their own people, the dam tender and family, and those at Powerhouse Number Two would not have been helped. They were only five minutes downstream. Everyone else from the Edison camp to the sea would have been greatly helped.

The responsible party, the Bureau of Water Works and Supply, was unprepared and unable to mitigate the ruin its dam had caused until after the emergency was ended. Then in the deliberate way of large institutions, it undertook the massive compensations and needed repairs. Had this institution dared to think about such an abnormal occurrence before it happened, it could have saved many lives.

6.3.4 Safety Plans

"Studies in the U.S. have shown that where early warning systems and evacuation plans are in place, the fatalities caused by dam bursts are on average reduced by a factor of more than 100. However, such plans have been made for only a handful of the world's dams, mostly in the U.S., Canada and Australia. The first step in an emergency plan should be to draw up and make public a detailed 'inundation map' of areas at risk if a dam should burst. Yet, according to David Ingle Smith of the Australian National University in Canberra, of the few countries that have produced adequate inundation maps some regard them as so confidential that they do not allow even the emergency services to see them."[27]

California became the first state to mandate a review of proposed dam projects by a board of outside consultants retained by the state engineer. In the following decades, other states followed, but it did not become complete in the U.S. until the failure of Teton in 1976 (Idaho) prompted federal legislation. With the arrival of these boards came better thinking on surety issues around dams. Part of the Teton-inspired legislation finally included requirements for emergency notification and action.

---

[25] *"The average worldwide risk of any dam failing in a given year is on the order of 1 in 10,000." McCully, page 117. This "worldwide risk" includes third world countries, but probably does not include China. China has been very secretive about their dam failures.*

[26] *The author owes Charles Johnson a word of thanks for comments made during a brief telephone conversation. It was those few words that started me thinking about how "surety" thinking would have saved lives.*

[27] *McCully, page 122.*

As noted, such actions are rare in the world; the impulse to protect the information springs from not inviting accusations of liability. California also developed, after St. Francis, an efficient system to settle the claims. The system sprang from awareness of a predatory impulse from some who would take advantage of the confusion and guilt. The potential for this was also abetted by opportunistic members of the legal system. The Los Angeles compensation procedures that followed the collapse provided timely response and seemed to have satisfied most of those involved. If a claims adjustment system were made and underscored by permanent national legislation, liability might not be so hard to admit.

Nevertheless, even without tort reform of this type, someone who understands the real impact of a dam failure would act to consider the safety issue here seriously. They would not keep the plan from those who may need it within minutes of a collapse. For future generations of dam operators and engineers, the story of the St. Francis Dam failure can make acute the importance of safety after a dam failure.

6.4 Security

6.4.1 Definition

We have defined reliability in relation to a *normal* environment. For safety, we produced a definition of function in an *abnormal* environment. Then, security must operate in what we should call a *malevolent* environment.

The goal of security, it follows, is to increase the probability of reliable or safe function under conscious, thinking threats. While direct threats to safety and reliability are serious, they generally come from processes that do not adjust their behavior. Once understood, these natural threats will not change their behavior perversely to overcome the defenses designed into the system. The security threat is most dangerous in this area. Security adversaries are thinking and proactive. They may escalate the conflict or respond to the designer's counter measures with counter-counter measures.

6.4.2 St. Francis Dam and Terrorism

Malevolent threats to our society are not something new and unique to our period of history. Terrorism and terrorists are not a recent invention; they are the result of the nature of human conflict. Throughout the history of any society, including the U.S., significant conflicts among people often led to acts that we would today call terrorism. We have merely developed new words for the behavior.

In the 1920s, the Los Angeles Bureau of Water Works and Supply had reason to take seriously a malevolent threat to their system. The settlers of Owens Valley viewed the diversion of their water as a personal threat to their wealth and way of life. This view of the Los Angeles water works led to acts of violence.

Their actions included "captured headgates, seizure of Los Angeles representatives by masked men, forcible rides out of the valley under armed escort, illegal stopping and searching of automobiles, and wholesale dynamiting of the aqueduct . . ."[28] The dynamiting included placing a heavy charge along the aqueduct (May 27, 1927) that ripped out 450 feet of pipe. For the following months of June and July, the

[28] *Outland, page 23.*

St. Francis Dam supplied the Los Angeles water system until the dynamited damage could be repaired.

"One day during the heat of the Owens Valley tension, an anonymous phone call was received in the office of the Los Angeles sheriff reporting that a carload of men were on their way from Inyo County with the intention of dynamiting St. Francis Dam . . ."[29] This incident came to nothing, but the threat was real.

This "terrorist" activity began in 1924, the same year that the Los Angeles Bureau of Water Works and Supply began St. Francis Dam construction. As the conflict escalated, the bureau had no qualms about making significant performance design changes (they raised the water level twice). They made no design considerations for security, nor did they act after the conflict escalated.

6.4.3 The Adversary

Had there been a formal procedure, like that used by security consultants today, the most significant entry into an adversary analysis chart would have been an entry for the Owens Valley opponents.

	Owens Valley (Terrorist or Criminal)
Theft	Low Probability
Sabotage	Very High Probability
Ideological	Not
Economic	High Motivation Source
Personal	Some Motivation
Number	Tens (potential for hundreds if escalated)
Weapons	Dynamite, Firearms, Tools
Equipment and Tools	General Construction, Farm
Transportation	Automobile, Small Truck
Technical Experience	Reasonably High (but not experts)
Insider Assistance	Some Possibility

The Owens Valley settlers had no interest in the Los Angeles water system, except that it be *gone*. Sabotage was both a rational action to make the system more expensive and an irrational angry strike at the hated system. Their motivations were economic (in the west, water is wealth) and personal. The water in their valley struck very close to the notions they had for developing their own lives and families. There were significant numbers, and a real possibility of hundreds of opponents if the violent acts became legitimized to the average citizen's thinking.

This adversary was also well armed and reasonably well equipped for the era. Their technical experience, from settling a remote area, was adequate to pose a threat to any structure unless opposed by expert response. This expert response was absent.

6.4.4 Consequences

Owens Valley considered Los Angeles their opponent. They would not have knowingly imposed destruction on the

[29] *Outland, page 48.*

occupants of the Santa Clara River Valley.

Initially, some believed the St. Francis collapse was the result of malicious dynamiting. In the light of past dynamiting acts and the seriousness of the tension, this conclusion was reasonable. It was further supported by one researcher concluding that the dead fish strewn along the flood path had to be the result of explosive concussion.

A few clung to the explanation because it absolved Los Angeles of guilt; however, an alternative explanation of the fish deaths and the records of seismographs disproved dynamiting as a possibility. The fish were killed by the high sediment loads in the water forced into their gills and gullets. Solid experience existed, from earlier construction activity, that the seismographs in the area would have recorded a blast at St. Francis. No such blast was recorded.

An inadvertent, overly destructive, blast could have caused the same disaster. Knowing that the foundations of the dam were unreliable, we can easily imagine a dynamiting act by Owens Valley that could have worked in concert with the existing flaws and resulted in the same event. The blame would have been different, but the devastation would have been the same. The intent of these hypothetical dynamiters could have been to cause a slow failure that eliminated the dam as a backup source of water for the next aqueduct destruction. The associated powerhouses could also have been targets to irritate and cost their enemies.

The consequences of complete and sudden failure in the actual scenario were quite high, the worst civil disaster in the US during the twentieth century.[30] They would have been just as high if the cause were malevolent action. After a successful "bleeding" of the dam until it was unsafe to back up, any aqueduct failures would then have been more effective. The City of Los Angeles would have suffered significant water shortages.

The people of Owens Valley viewed the conflict in terms of water theft. Therefore, they would be more likely to attack the water works than to attack the powerhouses. Edison powerhouses were also well populated with workers and their families, further lowering the probability of a successful attack. They could more easily have attacked the power lines, but these would be easier to repair than other targets. However, attacks on the powerhouses would have caused power inconveniences (low consequences). St. Francis was primarily a water supply dam. The power was an ancillary benefit.

A table analysis (similar to those used by security consultants) would have looked like:

High Consequences	Intentional Sudden Dynamiting	Inadvertent Sudden Dynamiting	
Medium Consequences			"Bleeding" attacks on the dam
Low Consequences	Powerhouse attacks		
	Low Probability	Medium Probability	High Probability

6.4.5 Physical Protection System

There were no barriers, no warning systems, and no formal effort to improve communication to the sheriff's department. A public road ran very

---

[30] *The South Fork Dam collapse, also known as the Johnstown flood, killed 2,209 people. It was in 1889.*

close to the east edge of the dam, giving ready access to any adversary. The owners depended entirely on the county sheriff's department for all their security.

St. Francis Dam did not collapse from an act of terrorism. If it had, the anger directed at the perpetrators would have been greater than that which was aimed at Los Angeles and its water bureau. Such a breach of security would have absolved Los Angeles of liability, even if the contributions from an unreliable foundation had been recognized.

Jurisprudence having evolved since then to include a "deep pockets" concept, such absolution would not be possible today. A failure to analyze security needs and act on the results of that analysis would expose an owner to liability just as if they were as responsible as Los Angeles actually was in 1928.

The St. Francis Dam had a dam tender. In light of the active threat they experienced, it would not have been unreasonable to use the detection system of the day: a security officer, at least until the hostilities ended. (The Edison Construction camp had a night security officer.) Direct communication and a communication plan to the sheriff's department would have improved security and aided the earlier discussed matter of safety.

Those items—a night security officer, communications, and a coordinated plan with the sheriff—would have provided the 1928 technological roles of detection and response. A complete physical protection system includes detection, barriers, and response. The county sheriff was a long way off. The dam needed some kind of delay to allow adequate response. It is unlikely that the security officer could serve as adequate response against the anticipated adversary.

Any thought given to the security of St. Francis would have considered moving the public road. Fencing and concrete barriers have become ubiquitous today.

Today, that hostile environment would call for electronic monitoring, significant barriers, and a commitment from public or private response teams. St. Francis Dam was near the center of a recognizable and significant threat. It did not happen, but today, liability and responsibility in that malevolent environment would call for pro-active security thought and involvement.

6.4.6 Dams and Threats

There is no water war in the U.S. today that would include such capable, planned assaults as occurred in those years. However, this author knows of one attempted dam dynamiting in New Mexico. It was a laughably inept attempt and maybe only half-hearted.[31] However, part of the idea of providing surety is to ask the question, "What if . . .?"

As part of the mandated periodic review of the reliability and safety of dams, a security analysis would provide some further insight. Not all dams would merit security measures, some might merit minimal measures, but there might be those in which this is a real concern.

A knowledgeable adversary could do more damage than any recent U.S.

---

[31] *The attempt noted here was motivated by ideological anger at the continued existence of a dam in the neighborhood. Alcohol was involved. The act probably posed a greater threat to the perpetrator than to the dam.*

terrorist attacks have. An effective assault on a dam with a vulnerable population downstream would magnify the power of any explosives that the assailant uses. "With the exception of nuclear power plants, no man-made structure has a greater potential for killing a large number of people than a dam."[32]

Like St. Francis, the security needs of a dam might change with time. When the troubles with Owens Valley residents settled, the threat to St. Francis also would have dissipated. Since this changing environment prevails, periodic review with the reliability and safety issues is important.

6.5 Requiem for St. Francis Dam

St. Francis Dam will never rest in peace. Those interested in infrastructure will always find that we can learn more from its collapse.

6.5.1 Reliability

A smooth management transition and a system of peer review would have done much to improve St. Francis Dam's performance probability. Not all structures are significant enough to merit extensive review processes. The review, cost, and commitment must match the project. A large dam merits the maximum process.

The process starts with an internal house review. In a house review, a peer who was not a part of the design group would ask questions about the design approach and the information on the dam. These questions would be the least threatening in the review process and should serve to provide in-house quality control.

Outside consultants appropriate to the project become very important. St. Francis may have survived. To survive, the outside review group would have had to identify what the designers missed, the paleo-mega landslide geology. Mulholland recognized its significance in 1911. If the in-house review missed it, the outside review might not have. Even if all the reviews had also failed, the water bureau would have had some relief from guilt.

Then the construction process also failed. There should have been a system that recognized significant design changes, sent them to design teams, and prompted a timely review, including a return to the outside consultants.

6.5.2 Safety

A communication plan would have saved lives. Complete emergency response plans that include inundation maps, evacuation plans, and coordination with emergency services would have reduced stress on all concerned. We cannot hold 1920s Los Angeles to 1990s standards, but we can use St. Francis as a tale that motivates responsible parties today.

6.5.3 Security

St. Francis is an interesting exercise in the liability changes around security issues. From 1924 until it collapsed, the threat was clear. Yet no one would have then considered Los Angeles responsible for the attack if it had been caused by dynamiting. Contrast that with today. Victims of assault in hotels sue the hotel owner based on some theory of inadequate security. The recent bombing of the federal building

---

[32] *McCully, page 115. He is quoting Joseph Ellam, Pennsylvania State Director of Dam Safety, 1987.*

in Oklahoma City has prompted suits based on the federal government's theoretical ability to have foreseen the assault.

Owners of public infrastructures must now consider security issues. These considerations extend beyond protection of just the asset, but also to a responsibility to protect the public and employees from being caught in the cross fire.

6.5.4 Requiem for Willliam Mulholland

In studying this disaster, I identified heavily with "the Chief." The records did not count Mulholland as among the victims, but he was one of them.

Because so many people who were victims of this tragedy had no hand in making the tragedy, lamenting what it did to William Mulholland has been difficult. Even his granddaughter, Catherine Mulholland, had difficulty in openly weeping for her grandfather in her written work about this tragedy. This engineer chose the site and ran the bureau that built and operated the site. However, he did not design the dam nor did he directly oversee the construction of St. Francis Dam. Nevertheless, the city blamed him, and the survivors blamed him. Did he blame himself? Some say he did, others say that he always looked for some "reason" beyond their control for the failure.

William Mulholland was 72 years old when St. Francis Dam shattered the lives of so many. He was near the end of a long career that had made him the hero of Los Angeles. St. Francis Dam crowned this engineer's rough and able life with a tragedy that destroyed the reputation of all the work that he had accomplished before March 1928.

"Please, God," he said when he first heard the failure reported by telephone just after midnight. "Don't let people be killed."[33] They were, and he wept on the witness stand. He once hoped that it had been the work of Owen's Valley saboteurs. Finally, he told them all, victim and citizens, "Don't blame anyone else, you just fasten it on me. If there was an error in human judgment, I was the human."[34]

And they did. They blamed William Mulholland. Without further fanfare, St. Francis Dam buried the memory of all the good he had done for Los Angeles and the urban development of California.

William Mulholland died July 22,1935.

References

Gillis, Kevin, Producer. *Compton's Interactive World Atlas.* Softkey Multimedia, Inc., Orem, Utah: 1997. (For useful general information about landslides.)

*Hoffman, Abraham. *Charles F. Outland, Local Historian.* Historical Society of Southern California. Los Angeles, California: 1995.

Holts, Robert and Kovacs, William. *An Introduction to Geotechnical Engineering.* Prentice Hall, New Jersey. 1981.

*Johnson, Charles. *Following the Flood. A Photographic Study of the St. Francis Dam Disaster.* Historical Society of Southern California. Los Angeles, California: 1995.

Johnson, Charles. Personal telephone conversations. March and May, 1997.

McCully, Patrick. *Silenced Rivers, the Ecology and Politics of Large Dams.*

---

[33] *Mulholland, page 126.*

[34] *Outland, page 211. Outland's source was the Los Angeles Coroner's Inquest, Book 26902.*

Zed Books. London and New Jersey: 1996.

*Mulholland, Catherine. *William Mulholland and the St. Francis Dam.* Historical Society of Southern California. Los Angeles, California: 1995.

Outland, Charles. *Man-Made Disaster, the Story of St. Francis Dam.* The Arthur H. Clark Company. Glendale, California 1963.

*Rogers, David. *A Man, a Dam and a Disaster: Mulholland and the St. Francis Dam.* Historical Society of Southern California. Los Angeles, California: 1995.

These four works are bundled together. The resulting publication is *The St. Francis Dam Disaster Revisited.* Historical Society of Southern California. Los Angeles, California: 1995