SAND99-1358J

Commentary: Risk Management and Reliability Design for Buildings

Regina L. Hunter, Dennis L. Berry, and Robert M. Cranwell

Sandia National Laboratories, Albuquerque, NM 87185

TF 9711-634

INTRODUCTION

Risk and reliability are complementary concepts: risk assessment tries to predict and mitigate the occurrence of unexpected events, and reliability processes try to improve expected performance. Risk management and reliability design are in common use in the nuclear-power industry, in waste management and environmental restoration, and in manufacturing; however, these tools have been little used in architecture-engineering and construction projects.

For years, the airline and nuclear industries have used formal risk assessment tools to improve designs and operational safety margins. Many aspects of environmental cleanup and nuclear waste management use risk assessment techniques for guiding technology selection and for selecting project goals (1). The Departments of Energy and Defense have applied risk management techniques to ensure both conventional and nuclear-weapon safety and reliability over a wide range of operational conditions. Several government agencies and industries are attempting to use formal risk-management tools to analyze risks and to guide decision making (e.g., the U.S. Environmental Protection Agency [2] and the U.S. Nuclear Regulatory Commission [3]). Risk management and assessment methods have been developed for fire protection, floods, earthquakes, and other threats to structures and systems. Manufacturing industries, including micro-electronics, petrochemicals, and pharmaceuticals, have applied formal risk and reliability assessment techniques to ensure product quality and public health and safety (4). In the light of these precedents, it seems appropriate to develop new tools that use formal risk-management techniques for buildings and other structures.

Reliability of buildings and other structures has been approached in the past primarily through the application of the Uniform Building Code (5), other applicable codes and standards, and good engineering judgment. Architects and engineers for the most part know through a combination of training, experience, and intuition how to construct buildings that don't immediately fail or wear out. On the other hand, the formal reliability techniques that are routinely applied in many other industries are not commonly used in the construction industry. Seismic reliability, for which there is a large body of literature, is one important exception to this comment. Design-for-reliability concepts could be applied to structures to guide the steps taken during design, construction, maintenance, and remodeling to increase architectural reliability.

RISK MANAGEMENT

The Challenges

Risk assessment seeks to determine risk; risk management seeks to reduce or mitigate risks that have been identified. Formal risk assessment and management methods have not been applied to such structures as domed stadiums, large high-rise buildings, major transportation systems, and so forth, for several reasons. In the United States, construction practices have largely been governed by a complex and thorough experience-based set of rules and guidelines called the Uniform Building Code (5). These prescriptive codes have evolved over the years to use the best demonstrated available technology for engineering and construction. They are supported by independent testing and by many years of satisfactory performance. In general, buildings keep standing and bridges don't collapse. Where there are uncertainties, safety margins and more robust design and construction practices ensure that things work. Quality control processes guarantee that buildings and other structures are designed, built, and maintained in accordance with best engineering practice. Within the design envelope, there is high confidence that structures will perform safely and reliably. In general, there is little incentive to perform any analysis not required by "The Code." As a final risk-management tool, the owners of buildings and other structures can purchase insurance to reduce their liability for unforeseen or highly unlikely occurrences that could threaten human health, safety, and security.

The combination of excellent building codes, good engineering practice, and an insurance safety net leads to considerable inertia within the engineering and construction industry, which does not routinely use risk methods in current practice. The expense, uncertainty, and difficulty of recouping the cost of the analyses through reduced construction or insurance cost also weigh against the use of risk-assessment approaches.

New Perceptions

The impediments to the use of formal risk management for buildings largely continue to outweigh the incentives. However, a number of factors are emerging that are likely to change this situation. One of these involves society's perception of risk. People want to feel as safe and secure in public places as they do in their homes, but they are beginning to recognize that their work place or public gathering place may be subjected to conditions that go beyond the design basis for the structure. Terrorist attacks, whether through explosion or the release of toxic chemicals or biological agents, usually are not analyzed or accommodated for in design. Earthquakes can exceed, although with low probability, the design capabilities of structures, and certain design features, such as large glass panels or beams suspended with a single point of failure, can pose significant hazards to safety under some conditions. In light of this, it is increasingly recognized that the civil engineering aspects of buildings and structures must be viewed in light of the comfort, safety, and security systems of buildings. The interdependency and interrelationships between civil structural features and building systems becomes more important as the range and variety of hazards increase. For some time fire has been analyzed and addressed in holistic fashion by considering the protection of building structural integrity while coordinating fire protection system design and operation with that of heating, ventilating, and air conditioning systems and security systems. However, for other hazards, such as terrorism, earthquake, high wind, and external blasts, a holistic assessment of structures and systems is rarely performed, although the logical parallel to fire is obvious. An analysis of the risks arising from terrorism particularly calls for a detailed examination of potential single-point failures, although single-point failures can arise from a number of more common causes as well.

A final development that could enhance the likelihood that formal risk management could be used for buildings and structures is that risk assessment tools (models, computer programs, databases) are becoming more routinely available, more computationally powerful, and easier to use. With these tools, decision makers in government or industry could weigh the relative risks of various design or lease options for existing buildings or structures. They could choose an optimum balance for dealing with a variety of hazards or threats and could trade off various retrofit options for addressing new threats as they emerge.

When Risk Management is Appropriate

A number of factors might go into an informed decision about when formal risk management would be appropriate for structures: cost, construction time, number of people affected in the case of an accident, number of units in existence, availability of insurance, perception of risk, and the richness of engineering experience and actuarial data (i.e., abundant statistics on causes and rates of loss). A single-family house is a typical building for which formal risk assessment would rarely be appropriate. Single-family houses generally share a number of characteristics that make them poor candidates for risk assessment. As structures go, houses tend to be inexpensive, costing on the order of $100,000 per unit (6). Construction time typically varies from a few weeks to a few months. The number of people in a house at any one time, and therefore the number likely to be at risk, is small, on the order of three or four. Because of the very large number of houses, about 100 million units in the United States (6), actuarial data on typical hazards are plentiful. In much of the United States, new construction is governed by the Uniform Building Code, for example, which is based on a wealth of data, practice, and engineering experience. Insurance that will cover not only the original purchase cost of any property loss, but even the replacement cost of such property, is readily available. Finally, most people perceive that they are "safe at home" and are likely to be unreceptive to the idea that risk assessment is necessary.

A nuclear power plant, in contrast, is typical of structures for which formal risk assessment is not only appropriate, but routine. In addition to the regulatory requirement that formal probabilistic risk assessment (PRA) be performed, other factors increase the usefulness of PRA in this case. Nuclear power plants are extremely expensive to build, costing on the order of $3 billion to $5 billion. Construction typically takes 4 to 10 years. Several hundred people are present at the site around the clock, and in the case of an accident that releases radioactivity, hundreds of thousands to millions of people could be affected. Worldwide, only about 400 commercial power reactors exist, and many of these are built to unique designs, particularly in the United States. Actuarial data are thus essentially nonexistent. Stringent regulations are based primarily on engineering judgment rather than on experience. The owner's liability for hazards arising from nuclear accidents is limited by the Price-Anderson Act. Nuclear power plants tend to be perceived as dangerous neighbors for which all possible precautions, including risk assessment, should be taken.

A high-rise office building is an example of the kinds of high-occupancy structures for which formal risk assessment might or might not be appropriate, depending on the specific details of location, cost, and so on. Other structures in this category include stadiums, shopping centers, dams and reservoirs, and transportation assets like tunnels, bridges, or transportation terminals, where failures would affect large numbers of people. These types of structures and infrastructures are intermediate between single-family dwellings and nuclear power plants for all the factors mentioned above. Within this group of structures, some are appropriate candidates for formal risk assessment and some are not. How should we make this decision?

In addition to the factors enumerated above, several others must be examined to determine the appropriateness of formal risk assessment for this intermediate group of structures: number of persons potentially affected, collateral effects, symbolic value, perceived risk, attractiveness as a terrorist target, and vulnerability to single-point failures. Some structures occasionally house a very large number of people, such as a large commercial building, shopping center, or athletic stadium. Only a fortunate turn of fate prevented hundreds or even thousands of people from being present, and possibly injured, in commercial buildings damaged by the Northridge earthquake of January 1994, which occurred very early in the morning (7). Even if the structure itself does not house a large number of people, damage to the structure could affect a large number of people; for example, damage to a power plant or a transmission line can cause widespread collateral power outages. A structure may have symbolic value that would make a large monetary investment in risk assessment seem reasonable. Major damage to the Lincoln Memorial or the Statue of Liberty, through gradual failure of the foundations for example, would represent an incalculable loss to the people of the United States, even though their dollar value is not enormous. The perceived risk associated with the building may be very high, depending on recent headlines or some specialized use such as housing violent criminals. The possibility that a building may be an attractive target for terrorists because of some high-visibility government use or symbolic factor must also be considered. Finally, the vulnerability of the entire structure to the effects of failure at a single point should be assessed during the design phase.

As a result of this closer look at the structure, we may decide that an ordinary high-rise office building housing a few hundred people working for a number of low-profile businesses does not merit a full-blown risk analysis, because customary application of the Uniform Building Code and good engineering judgment are adequate. In contrast, a large federal building housing high-profile agencies and a foreign embassy in a major metropolitan center may well deserve formal risk assessment. The risk assessment would examine the number of persons at risk, missions of the tenant agencies, and nature of the contents and property, for example, to determine whether changes in building design or construction or increased security are warranted.

In performing the risk assessment, the analyst first identifies and prioritizes the consequences of concern and the hazards likely to affect the structure. Both the probability that a hazard will occur and the damage that the hazard will inflict if it does occur go into an assessment of the risk. At nuclear facilities, for example, the analyst weighs the probability of occurrence of an earthquake that is larger than the design-basis earthquake against the environmental damage that would occur as a result of such an earthquake. The resulting analysis and ranking of the risks provides support for an assessment of possible alternative design, construction, or upgrading options. The results of the risk assessment could produce information leading to a variety of decisions. If construction has not begun, design modifications to mitigate projected risks could be implemented, often at minimal cost. For existing structures, risk-based decisions might drive remodeling, repair, demolition, or relocation of the occupants to another building. Risk analysis would also allow informed tradeoffs between security and ease of access or between comfort and safety.

Tools

Once the decision is made to perform a formal risk assessment for a building, the analyst must select appropriate tools, usually a combination of expert scientific and engineering judgment and computer codes, to use in doing the work. At this time, few risk-assessment tools have been designed specifically for buildings, although many existing tools and methods for the analysis of fire (8), seismic loading (9), structural loading (10), blast (11), and so on would be more-or-less directly applicable to this specialized area. In addition, more generalized decision-support tools could be used (12). One of the authors (Hunter) is currently leading an effort ot design and build a screening-level tool specifically for the risk analysis of buildings of interest to the U.S. General Services Administration. Finally, general techniques for risk management are widely known, and these could be applied to buildings by most risk analysts without modification.

DESIGN FOR RELIABILITY

"Design for reliability" means building reliability into the design of a system rather than incorporating it after development has begun or is finished. Reliability should be considered as a design parameter early in the life cycle of a product, preferably while product requirements are being defined or during feasibility analysis. Designing in reliability does not mean that reliability issues can subsequently be ignored. Reliability evaluation and continuous improvement should take place throughout the life cycle of a system.

Advantages

The early life cycle phases typically represent the smallest portion of the total life-cycle costs borne by the supplier of a system, yet they generally present the most cost-effective opportunity to improve system reliability. As a design moves toward completion, design details become increasingly fixed, and the cost in time and dollars to correct reliability problems increases. Figure 1 shows that typically toward the end of the design and development phase of the life cycle, only about 15% of the life-cycle costs are consumed, but about 95% of the total life-cycle costs have been determined. Design and development determine the materials and components to be used in production, for example, which in turn determine production costs and greatly influence product performance. Changes made to improve reliability after design and development have little effect on overall life cycle costs, but they can be very expensive in terms of costly design changes, retrofits, service call, warranty claims, and customer goodwill. This is not meant to imply that reliability improvements for systems already in production or in operation should be ignored. Reliability improvement activities should continue throughout the life of the structure. Although reliability improvements made early in the life cycle can increase initial costs to the builder, they generally result in lower support costs for the manufacturer and lower operational costs for the consumer.

A second aspect of designing for reliability is "designing for maintainability." One method of enhancing reliability is to enhance the reparability or maintainability of a system. This is particularly important for buildings or systems where life extension is considered, or where upgrades or improvements are important. The replacement cost of the existing infrastructure of the United States would be astronomical, so it is important to design structures for ease of repair, maintenance, or upgrading. Figure 2 illustrates the importance of building in constructability, reliability, and low cost at the earliest possible stages of design. The influence of the design on performance of a structure is far out of proportion to the cost of the design itself.

System-Level Focus

Field reliability data on complex systems indicate that the primary causes of failures are not component failures, but rather are system-level deficiencies in design, manufacturing, or requirements definition (14). Data indicate that part failures account for only about 15% of system failures; 85% are due to system-level problems associated with design and manufacturing. As a result, reliability assessments based primarily on component reliability do not adequately represent system-level reliability. The National Research Council's Evaluation of NASA's safety analysis of the Challenger accident included criticisms of their lack of an emphasis on systems analysis, their failure to adopt established probabilistic risk assessment methods, and their lack of uncertainty analysis (15).

A system-level reliability focus is a top-down approach that starts early in system design. Prediction and analysis are used at every stage of design to identify problems in meeting system requirements and to correct these problems as early as possible.

A system-level focus applies optimization techniques to determine such things as optimal target reliabilities for design and upgrades for structures. Such approaches have been proposed for formulating cost-effective risk-based criteria for the design and upgrading of structures with special reference to earthquake protection. (Target reliabilities [or acceptable risks] for damage control and human safety are determined on the basis of minimum expected life-cycle cost, from which risk-consistent criteria for design or upgrading are developed.) A systems approach also recognizes that most reliability problems involve decision making under uncertainty. Decisions are evaluated in terms of their effects on system reliability. Although it is clear that the reliability of a system is known with certainty only after it has been used until it is worn out and its failure history has been faithfully recorded, design for reliability is a cost-effective step toward increasing the time period of reliable performance.

Designing Reliable Structures

What does it mean for a structure to be reliable? Our society tends to associate "reliability" with products whose life spans are relatively limited: automobiles, appliances, electronic equipment, industrial machinery, and so on. Buildings and other structures, in contrast, typically have life spans measured in decades. We define a reliable structure to be one that can continue to serve its original function (or a closely related function) for at least the design lifetime without a significant increase in maintenance and repair costs. Thus a reliable building is one in which (1) failures of major structural components (such as the foundation) do not occur; (2) maintenance schedules for major non-structural components (such as the roof finishing materials or facade) are determined by component lifetimes, not by secondary effects of other structural failures; (3) heating, cooling, and ventilation continue to function efficiently without increasing energy usage, (4) electrical and plumbing systems can be maintained and repaired easily and inexpensively; and (5) renovation and modernization do not require major structural modifications. Reliable structures may cost more to build, but they typically cost less to maintain. In an unreliable building, on the other hand, the foundations shift, causing the walls to crack and the roof to sag; energy usage increases; maintenance and repair costs are high; and renovation and modernization are not cost effective.

How might reliability concepts be applied to the design and construction of buildings, bridges, transportation systems, dams, and other structures? The initial steps of the process are clear. First, long-term structural reliability must be included as a design parameter along with other basic considerations such as function, size, and location. Second, the design phase must include a systems analysis. The systems analysis should be a holistic examination of both component reliability and the interactions of components. It should consider the construction processes to be used and the environment the structure must function in after construction is complete. The systems analysis should result in an allocation of construction resources in such a way that overall reliability is enhanced. For example, components that directly or indirectly support the function of several other components could be singled out for higher-grade construction materials, while components that do not support multiple functions or are likely to be replaced for cosmetic reasons could be candidates for cost savings. The systems analysis should also consider ease of maintenance and repair. Components with moving parts (e.g., heating systems) or with short lifetimes due to high usage (e.g., elevators) should be designed in such a way that they are readily accessible for maintenance and repair without removing walls or furnishings or inconveniencing occupants. Finally, the possibility that major new systems (e.g., fiber optics) may have to be installed at a later time should be considered and the design be made flexible enough to accommodate such upgrades.

The results of the systems analysis should be used in a comprehensive reexamination of the design to ensure that appropriate emphasis has been give to lifetime reliability of the structure. At this point the design can be optimized to achieve a proper allocation of reliability and cost. Uncertainty and sensitivity analysis allow the designer to make informed decisions about the potential impacts of inadequate data.

CONCLUSION

Where there is a significant actuarial basis for decision making (e.g., the occurrence of fires in single-family dwellings), there is little incentive for formal risk management. Formal risk assessments are most useful in those cases where the value of the structure is high, many people may be affected, the societal perception of risk is high, consequences of a mishap would be severe, and the actuarial uncertainty is large. For these cases, there is little opportunity to obtain the necessary experiential data to make informed decisions, and the consequences in terms of money, lives, and societal confidence are severe enough to warrant a formal risk assessment.

Other important factors include the symbolic value of the structure and vulnerability to single point failures.

It is unlikely that formal risk management and assessment practices will or should replace the proven institutions of building codes and engineering practices. Nevertheless, formal risk assessment can provide valuable insights into the hazards threatening high-value and high-risk (perceived or actual) buildings and structures, which can in turn be translated into improved public health, safety, and security. The key is to choose and apply the right assessment tool to match the structure in question.

Design-for-reliability concepts can be applied to buildings, bridges, transportation systems, dams, and other structures. The use of these concepts could have the dual benefits of lowering life-cycle costs by reducing the necessity for maintenance and repair and of enhancing the safety and security of the structure's users.

Acknowledgement — Sandia National Laboratories is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-ACO4-94AL85000.

REFERENCES

1. U.S. Environmental Protection Agency, 1985. "Environmental Standards for the Management and Disposal of Spent Fuel, High-Level and Transuranic Radioactive Wastes, Final Rule." 40 CRR Part 191. Federal Register. Vol. 50. Pp. 38066-38089.

2. Conference on the Risk Assessment Paradigm After Ten Years: Policy and Practice Then, Now, and in the Future, 1993. EPA/600/R-93/039. Washington, DC: Office of Research and Development, U.S. Environmental Protections Agency.

3. "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement," 1995. Federal Register. Vol. 60. P. 42622.

4. Guidelines for Equipment Reliability. SETEC91-025. Albuquerque, NM: Sandia National Laboratories.

5. International Conference of Building Officials, 1997 Uniform Building Code, International Conference of Building Officials, Whittier, CA, 1997.

6. Bureau of the Census, 1996. Statistical Abstract of the United States 1996. Washington, DC: U.S Department of Commerce. Table 1195, p. 722.

7. Aurelius, E., Executive Editor, 1994. "The January 17, 1994 Northridge, CA Earthquake." San Francisco, CA: EQE International.

8. Tieszan, S. R.; Nicolette, V. F.; Gritzo, L. A.; Holen, J. K.; Murray, D.; Moya, J. L. Vortical Structures in Pool Fires: Observation, Speculation, and Simulation. SAND96-2607.

Albuquerque, NM: Sandia National Laboratories; 1996.

9. Lambright, J. A., Bohn, M. P.; Daniel, S. R.; Johnson, J. J.; Ravindra, M. K.; Hashimoto, P. O.; Mraz, M. J.; Tong, W.H.; Brosseau, D. A.. Analysis of Core Damage Frequency: Peach Bottom, Unit 2 External Events. SAND86-2084. Albuquerque, NM: Sandia National Laboratories; 1990.

10. Moya, J. L.; Skocypec, R. D.; Thomas, R. K. Development and Experimental Validation of Computational Methods to Simulate Abnormal Thermal and Structural Environments. SAND93-2215C. Surety Technology Symposium, September 27-October 1, 1993, Chelyabinsk, Russia. 1993. Available on request from Technical Library; Albuquerque, NM: Sandia National Laboratories.

11. Kennedy, R. P.; Blejwas, T. E.; Bennett, D. E. Capacity of Nuclear Power Plant Structures to Resist Blast Loadings. SAND83-1250. Albuquerque, NM: Sandia National Laboratories; 1983.

12. Webb, E. K. Sandia's Environmental Decision-Making Support Program: Providing an Efficient, Consistent, Comprehensive Decision-Making Framework. SAND94-0410. Albuquerque, NM: Sandia National Laboratories; 1994.

Arsenault, J. E., Roberts, J. A., eds., Reliability and Maintainability of Electronic Systems, Potomac, MD: Computer Science Press; 1980.

14. "Ask RAC." RAC Journal 3(4):10, Rome, NY: Reliability Analysis Center; 1995.

15. Marshall, E. Academy Panel Faults NASA's Safety Analysis. Science 239:1233. March 11, 1988.