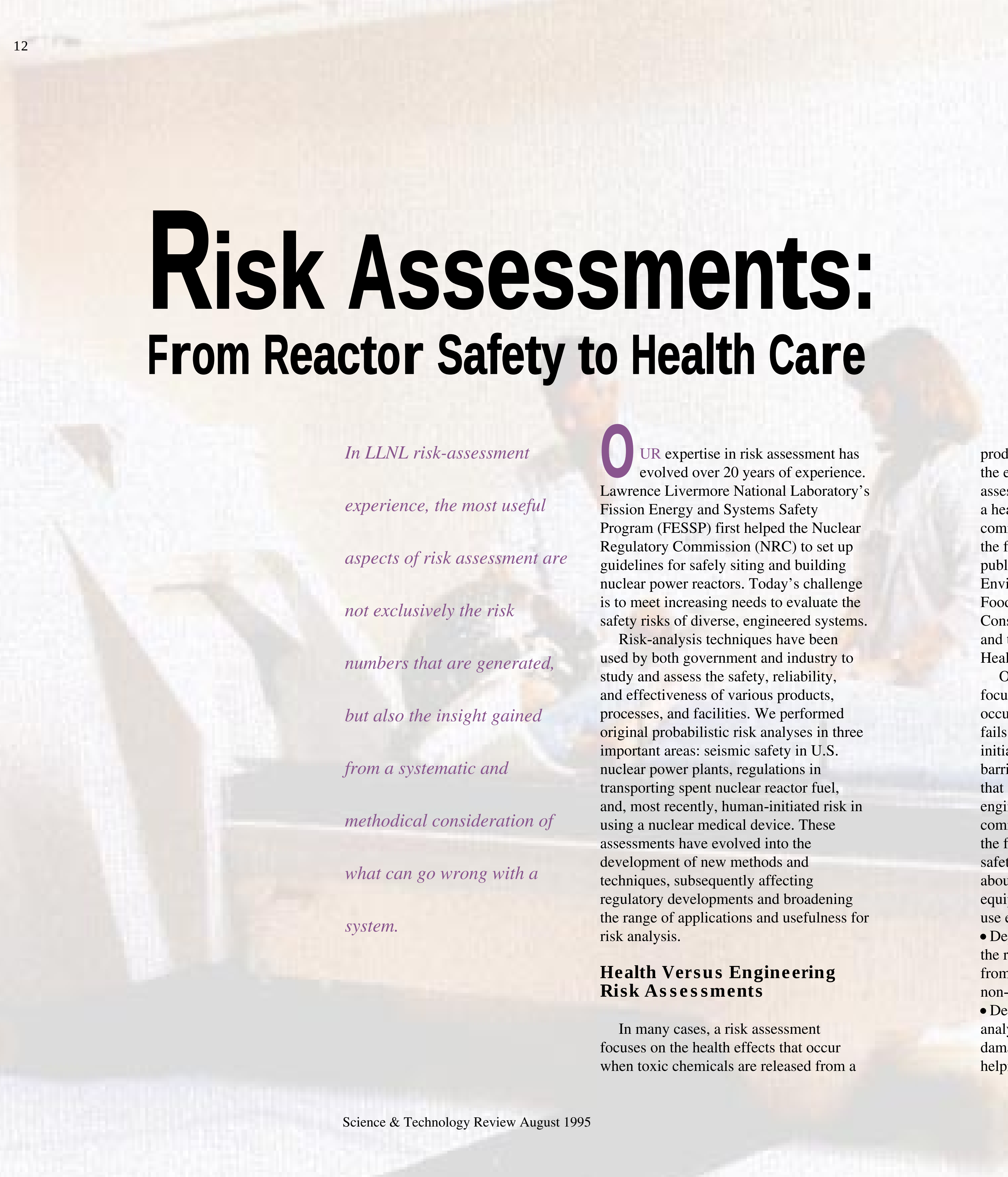


Risk Assessments:

From Reactor Safety to Health Care

In LLNL risk-assessment experience, the most useful aspects of risk assessment are not exclusively the risk numbers that are generated, but also the insight gained from a systematic and methodical consideration of what can go wrong with a system.

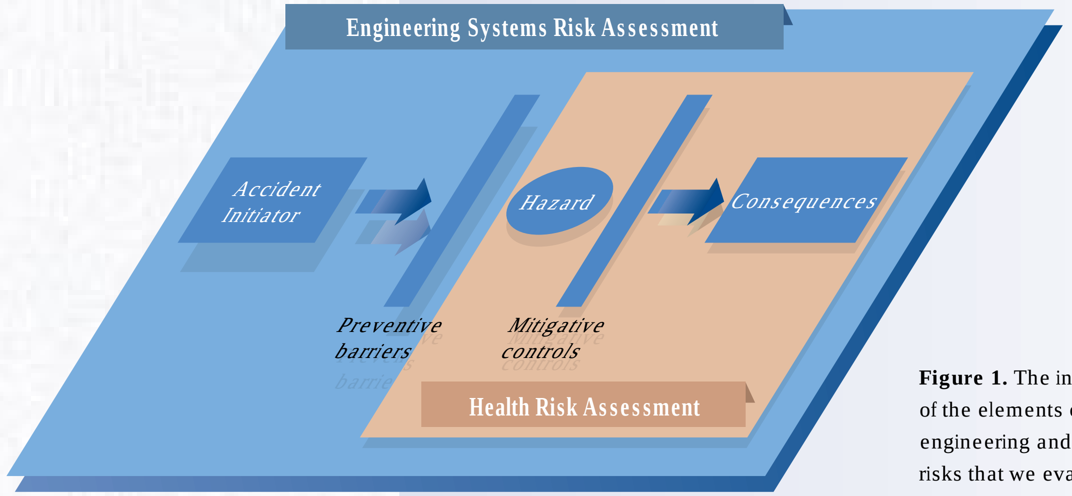


Figure 1. The interplay of the elements of engineering and health risks that we evaluate.

OUR expertise in risk assessment has evolved over 20 years of experience. Lawrence Livermore National Laboratory's Fission Energy and Systems Safety Program (FESSP) first helped the Nuclear Regulatory Commission (NRC) to set up guidelines for safely siting and building nuclear power reactors. Today's challenge is to meet increasing needs to evaluate the safety risks of diverse, engineered systems.

Risk-analysis techniques have been used by both government and industry to study and assess the safety, reliability, and effectiveness of various products, processes, and facilities. We performed original probabilistic risk analyses in three important areas: seismic safety in U.S. nuclear power plants, regulations in transporting spent nuclear reactor fuel, and, most recently, human-initiated risk in using a nuclear medical device. These assessments have evolved into the development of new methods and techniques, subsequently affecting regulatory developments and broadening the range of applications and usefulness for risk analysis.

Health Versus Engineering Risk Assessments

In many cases, a risk assessment focuses on the health effects that occur when toxic chemicals are released from a product, process, or facility and enter the environment. This type of risk assessment is often referred to as a health risk assessment and is commonly undertaken by agencies of the federal government that deal with public health and safety, e.g., the Environmental Protection Agency, the Food and Drug Administration, the Consumer Product Safety Commission, and the Occupational Safety and Health Administration.

Other times, a risk assessment focuses on the health effects that can occur when an "engineered" system fails, because of a natural or human-initiated event or when the protective barrier between the environment and that system fails (Figure 1). Known as engineering risk assessments, they are commonly carried out by agencies of the federal government that make safety, health, or design decisions about risk-posing facilities or equipment. Examples of agencies that use engineering risk assessments are

- Department of Energy, in evaluating the radiological and chemical risks from various types of nuclear and non-nuclear facilities.
- Department of the Interior, in analyzing dam safety, assessing damage from ecological disasters, and helping to predict natural hazards, such as earthquakes, floods, or volcanoes. Much of this risk assessment work is directed toward improving the probability distributions that describe the recurrence of these natural hazards and their possible intensity.
- Federal Aviation Administration, in analyzing potential collision scenarios, such as the simultaneous approach of two aircraft on closely spaced, parallel runways in inclement weather.
- National Aeronautics and Space Administration, in assessing the possibility of shuttle accidents that might result in the release of radioactive material from radioactive power sources.
- Nuclear Regulatory Commission, in analyzing risks of low-level radioactive waste disposal, evaluating performance of high-level waste repositories, and evaluating risks associated with nuclear power plant accidents.

The Assessment Process

Although the process used to assess risks from engineered systems varies with each user and application, it usually retains five common elements (Figure 2):

- A description of the system's hardware components, operating environment, and staff operators.
- A hazard identification analysis to determine the events or conditions that might lead to accidents or failures.
- An analysis to estimate the frequency of events that must occur before health impacts could occur.
- An analysis to determine the health effects, i.e., the consequences of these events to workers and the public.
- A procedure to quantify assessed risks, including the uncertainties inherent in any risk evaluation.

In 1983, the National Academy of Sciences published a document that standardized the process for health risk assessment. The book, *Risk Assessment in the Federal Government: Managing the Process,*[1] is also known informally as the "Red Book."

The Red Book breaks the risk assessment process into four basic elements:

- A hazards identification analysis to determine whether a particular chemical is or is not causally linked to a particular health effect.
- An exposure assessment to determine the extent of human exposure before or after the application of regulatory controls.
- A dose-response assessment to determine the relation between the magnitude of exposure to a chemical

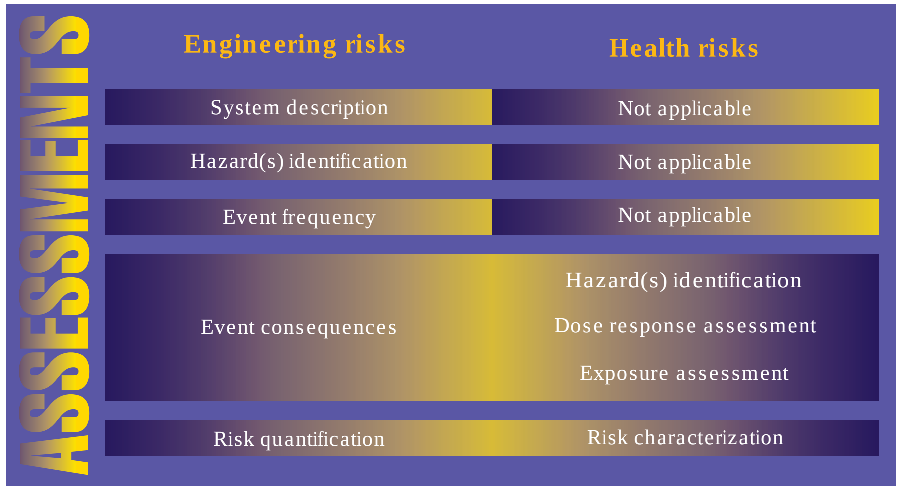


Figure 2. Some components of engineering systems risk assessments overlap those for health risk assessments.

and the probability of occurrence of the health effect in question.

- A risk characterization procedure to describe the nature and magnitude of human risk, including any attendant uncertainty.

If we compare these health risk assessment elements to the five basic elements of engineering risk assessment, we find both similarities and differences between the two processes. In an engineering risk assessment, the event consequence step contains the first three steps described in the Red Book (Figure 2). In NRC studies that analyze the impact from a release of radioactive material, this consequence would be the dispersion of material in the environment; the uptake of the material via inhalation, ingestion, or other exposure pathways; and the response of various body organs to such exposures. The results would lead to an estimate of the probability of cancer incidence or fatality, given that the radioactive release had occurred.

Perhaps the most significant difference between the two processes is the treatment of event frequencies. In an engineering risk assessment, the analyst considers both the frequency of an event (e.g., a large earthquake occurring near a nuclear power plant) and the probabilities of different failures within the engineered system. Different combinations of failures can lead to health threats of different severity. For example, an earthquake could produce a variety of damage in a nuclear power plant, including no damage at all. These damage states could, in turn, lead to a variety of potential radioactive releases, or no release at all. Thus, a single initial event can lead to a variety of possible health effects, each with its own probability.

On the other hand, in a health risk assessment, the analyst deals primarily with situations involving chronic releases to the environment with a release probability of 1, that is, the assumption that such a release will absolutely occur. This type of assessment would propose to restrict or eliminate the material's presence rather than mitigate with engineering controls or boundaries.

The differences between engineered-system risk assessment and health risk assessment thus have a significant impact on risk-management strategies. Although eliminating hazards is an effective strategy, it is not always practical in an industrialized economy. Engineering risk assessment supports the management of risk through design, maintenance, and administrative controls. Reducing the possibility that accident initiators and hazards can cause consequences—through effective and reliable engineered barriers and mitigative controls—provides a means of managing risks in industrial activity while protecting the environment, safety, and health of the public.

Another important difference between the two processes has to do with consequence measures, or endpoints, of risk assessment. Health risk assessment is specific to exposures from toxic chemicals and the associated dose response; hence, the ultimate endpoint can be cancer fatality. In engineering risk assessment, the endpoint varies. Common endpoints include worker health and safety, loss of a facility or piece of equipment (for example, the crash of an airplane and the associated, implicit health effects), immediate loss of life (one of the results of a large earthquake), or long-term loss of life from cancer (one of the results of a nuclear power plant accident). In addition to these consequences, engineering risk assessment can have other nonhealth-related endpoints. For example, the endpoint of a Department of the Interior risk assessment study on dam failure involved the economic impact that failure would have on the surrounding community.

Our Focus: Engineering Risk Assessment

Depending on its application, an engineering risk-assessment study can fall into one of five classes: it can be a conceptual design evaluation, a detailed design study, a facility operations study, a management support study, or a policy and standards development study. Table 1 offers examples of the applications or activities appropriate to each class. Conceptual design evaluations and detailed design studies tend to focus on equipment or one facility at a time; facility operations, management support, and policy standards and development studies can focus on a single facility or on multiple facilities and activities.

The FESSP specializes in integrating advanced analytic methods with an understanding of nuclear technologies, economics, and policy-making. Over the last 20 years, we have performed a number of original risk-assessment studies to support regulatory developments at the NRC. We concentrate on safety issues relating to engineered systems that either use or contain nuclear material, as shown in the following four cases:

- An analysis to develop seismic criteria for the siting and design of nuclear power plants.
- A risk analysis of reactor coolant piping systems to establish new piping design objectives and increase nuclear power plant safety.
- A study of risks involved in the transport of spent reactor fuel to determine the level of safety provided during transport and the adequacy of existing transport regulations for such material.
- The development of an approach to identify human-initiated risks in the use of nuclear medical devices such as the Gamma Knife.[2]

Depending on the nature of the problem, the detailed methods used in each study vary in that they may include any or all of the basic elements of the engineering risk-assessment process. However, each study is similar in that it constitutes a rational and systematic approach to obtaining information that can be used to increase safety, formulate policy, develop standards, omit costly duplications, or implement regulatory guidelines.

Our evolving experience base thus provides the government with recommendations of risk-based regulations and prioritizations for resource allocations. It shows where regulatory reform can help the

Table 1. Classification of engineering risk assessment by application or activity.

Type of engineering risk assessment	Application or activity
Conceptual design evaluations	• Determine the viability of a particular site for a particular facility. • Analyze and compare competing technologies or processes. • Evaluate the risks of emerging technologies.
Detailed design studies	• Identify risk-dominant scenarios to provide guidance for refinements in the design of a system or facility. • Analyze and compare the reliability or availability of system/component options. • Provide specifications to design components, systems, or structures that will have high reliability and protection against severe natural phenomena. • Analyze and improve a facility's training programs, operator–equipment interfaces, and operating procedures. • Determine optimum safety limits, equipment outage times, and testing frequencies to minimize risk. • Analyze acceptable risk to document the importance of risk-based design features and systems interactions data.
Facility operations studies	• Carry out a risk-based analysis of operating events. • Design and implement risk-based trends and patterns. • Improve system availability. • Enhance component inspection, testing, monitoring, and maintenance based on component failure analysis. • Evaluate and prioritize safety issues. • Evaluate, select, and schedule modification. • Assess continued operations. • Enhance safety, emergency, and accident management information and training.
Management support studies	• Provide risk-based perspectives for decision-making. • Provide information for allocating resources (staff, budgets) and identifying research needs. • Measure safety performance. • Perform risk-based quality assurance and audits.
Policy/standards development studies	• Assess and develop rules, standards, and safety criteria. • Develop safety measures, goals, and criteria. • Assure coordination and consistency of safety goals and criteria.

government—and the country—work better and safer for less.

Case 1: Seismic Criteria for Siting Nuclear Power Plants

Since the early 1970s, the Laboratory has worked with the NRC to establish seismic criteria for regulating the siting of nuclear power plants. Most of these criteria are deterministic in that they are based on the determined size and location of the most credible seismic event, not on its frequency of occurrence or the possible consequences. In areas where very large earthquakes have occurred (such as New Madrid, Missouri, or Charleston, South Carolina) or cannot be excluded from occurring, even if the likelihood of occurrence is very small, the application of siting regulations based on these criteria could lead to very conservative design criteria and prohibitive costs.

To help the NRC evaluate the effect of such siting regulations, we proposed to assess the seismic hazard by using a probabilistic methodology—that is, we weighted all the possible earthquakes that could affect a site by their likelihood of occurrence. By coupling this methodology with a newly developed systems analysis concept, we systematically analyzed the series of causative events and the behavior of all structures, systems, and components in the plant. We then identified the failure modes and quantified their consequences. The total risk was obtained by considering the entire spectrum of earthquakes and all possible modes of failure and integrating their calculated consequences (Figure 3).

Sponsored by the NRC, this first U.S. seismic probabilistic risk assessment for nuclear power plants from 1978 to 1985 cost $18 million. The same methodology was then used by the nuclear industry to assess 35 nuclear power plant sites. The majority of seismic probabilistic risk-assessment knowledge existing in the technical community today was gained through this massive exercise.

Our methodology is now widely used by the NRC and other public utilities to evaluate and compare, on a relative scale, the risks associated with existing nuclear power plants. In many cases, its use has led to retrofitting, reinforcement, and redesign of components or systems to achieve comparable levels of risk across the entire population of plants.

Currently, we are helping the NRC to overhaul the seismic siting criteria for new nuclear power plants. Our experience base has been used to help develop proposed risk-based regulations now under public review. Previous regulations were based on methodologies that rely on single deterministic models. Often such models pit one group of experts against another group, creating time delays and thus protracting the plant licensing process. The proposed changes to regulations are based on a methodology that provides a framework for assessing all information and makes maximum use of existing data and factors from all possible modeling and scientific alternatives. As such, the changes should help streamline the plant licensing process.

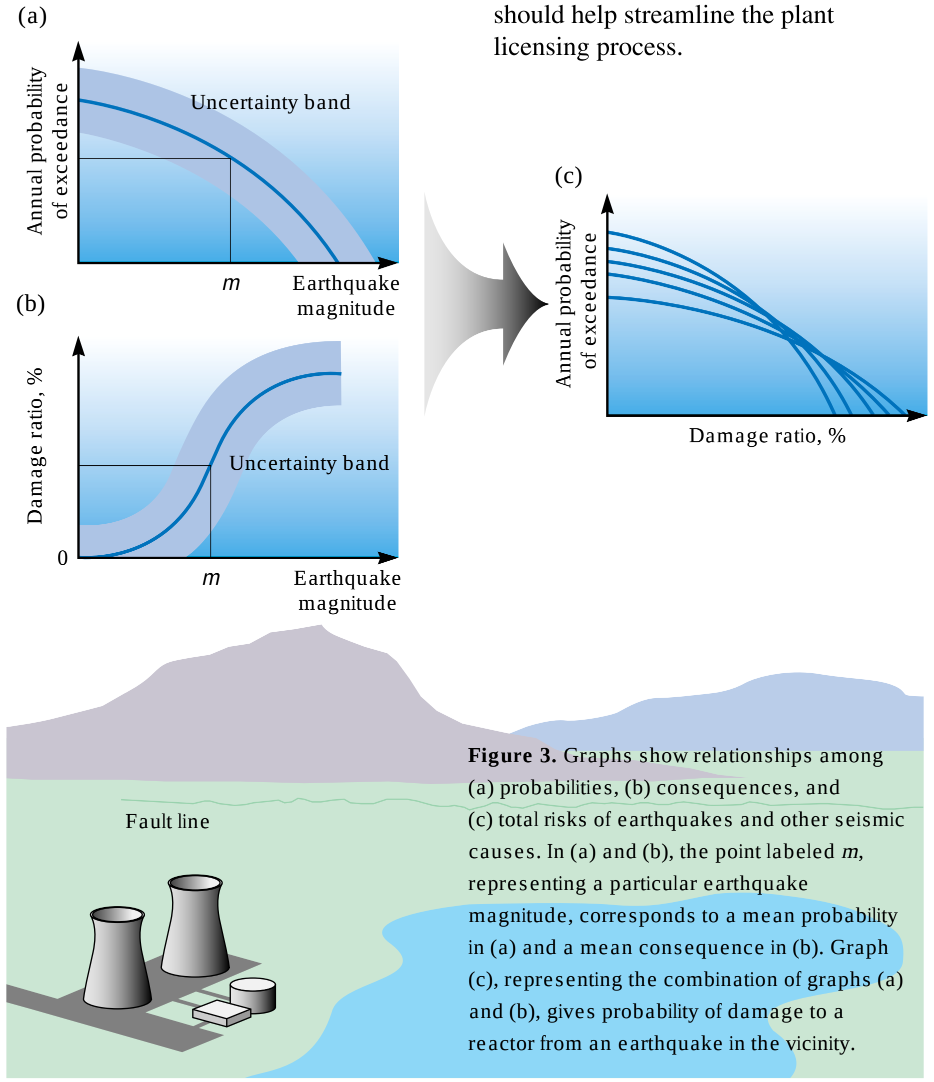


Figure 3. Graphs show relationships among (a) probabilities, (b) consequences, and (c) total risks of earthquakes and other seismic causes. In (a) and (b), the point labeled *m*, representing a particular earthquake magnitude, corresponds to a mean probability in (a) and a mean consequence in (b). Graph (c), representing the combination of graphs (a) and (b), gives probability of damage to a reactor from an earthquake in the vicinity.

Case 2: Safety of Reactor Coolant Piping

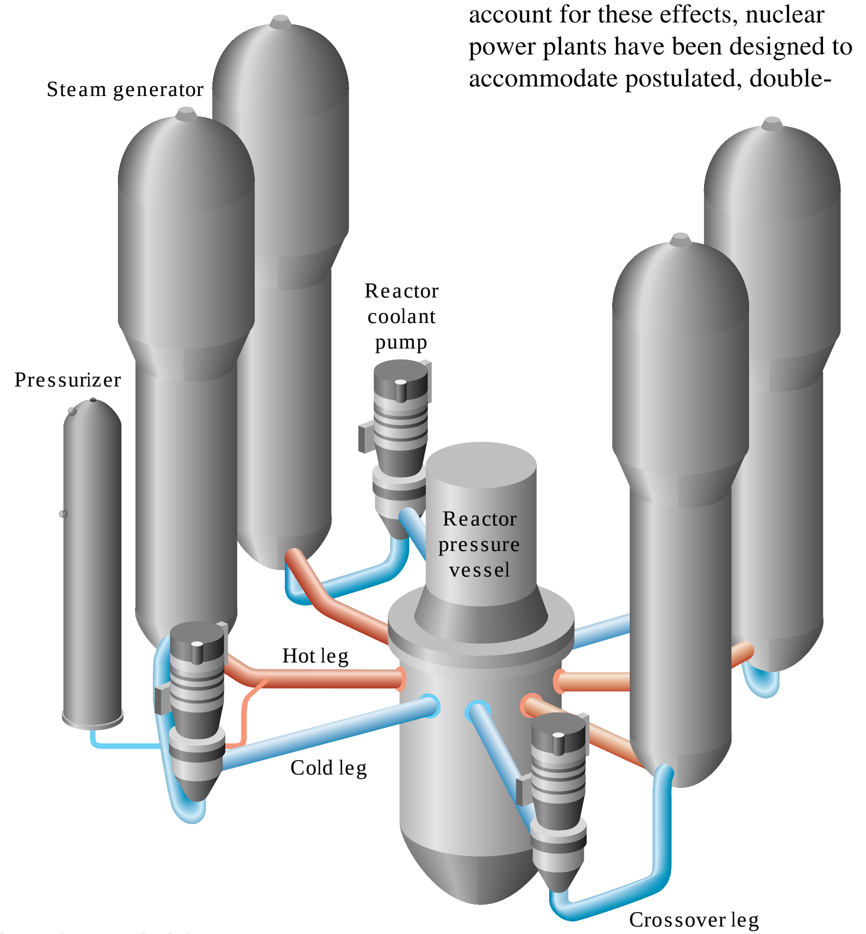
This safety assessment was one of the first Laboratory studies in which risk-assessment techniques resulted in regulatory change. It is also a classic example of a substitution risk, that is, substituting a change in risk for a savings in dollars.

The *Code of Federal Regulations*[3] requires that structures, systems, and components important to the safety of nuclear power plants be designed to withstand the effects of naturally occurring hazards as well as the effects of normal and accident conditions. Design criteria require that safety-related structures, systems, and components of nuclear power plants be designed to withstand the effects of a large loss-of-coolant accident. To account for these effects, nuclear power plants have been designed to accommodate postulated, double-ended, "guillotine" breaks in their high-energy piping systems, particularly the massive ones about a meter in diameter that circulate primary reactor coolant (see Figure 4a).

The difficulty—and cost—of designing a nuclear power plant for postulated pipe breaks was exacerbated by a related requirement that the hydrodynamic loads be combined with the vibratory loads that result from a "safe shutdown earthquake," the maximum design-basis earthquake for a nuclear power plant. In effect, this requirement presumed that an earthquake could cause pipe breaks in all high-energy piping systems. This requirement was also problematic because the design objectives for safe piping systems under normal conditions contradicted those for safe piping systems under earthquake conditions.

During normal operation, piping systems must be flexible enough to expand to relieve the thermal stresses that can drive cracks through their walls and cause leaks or breaks. However, during a large earthquake (which is most likely a once-in-a-plant-lifetime occurrence), stiff piping is needed to assure that seismically induced breaks

(a) A reactor coolant piping system



(b) Failure probability

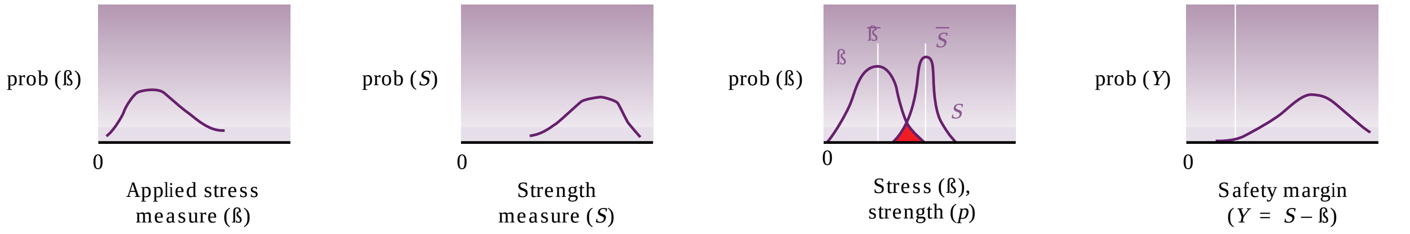


Figure 4. (a) LLNL developed standards and proposed regulations concerning the high-energy piping systems that circulate primary reactor coolant. (b) Probabilistic approach for assessing component adequacy for postulated load conditions in piping. In this approach, failure is possible only in the region shaded red.

do not occur. Designers have met these cross purposes by using “pipe snubbers,” elaborate mechanical and/or hydraulic devices that allow pipes to move during normal operation but anchor them rigidly when they are subjected to rapid (i.e., seismic) loads. Pipe snubbers not only require periodic testing and maintenance—in areas of high radiation and difficult access—but have proved unreliable. Many have been found to lose their earthquake-resisting function; others have been found to restrict normal thermal expansion and seriously increase pipe stresses. (In the latter mode, then, these safety devices can actually increase the likelihood of pipe failure.)

For years, nuclear plant designers have contended that the likelihood of seismically induced breaks is low enough to be considered negligible. They believed that protective measures such as pipe whip restraints and jet impingement barriers may actually decrease the reliability of piping systems. In the early 1980s, the nuclear industry sought to exempt itself from the NRC piping safety regulations by doing extensive research in deterministic fracture mechanics so that it could argue the merits of a “leak-before-break” concept. That is, because of the very tough materials used in nuclear piping, even large cracks through walls would remain stable and not result in a double-ended guillotine break. The NRC sought additional technical information to respond to the exemption request.

The FESSP engineers, in an independent confirmatory research effort funded by the NRC Office of Nuclear Regulatory Research, developed and applied risk-assessment techniques (Figure 4b) to estimate the likelihood of a double-ended guillotine break in the coolant loop piping of a pressurized water reactor (PWR). This effort consisted of the “Flexible vs Rigid Piping Program,” “Piping Reliability Program,” and “Load Combination Program” carried out between 1981 and 1985 at a cost of $3.5 million.

The results of this analysis indicated that the probability of this kind of break in a PWR’s coolant loop piping is low enough under all plant conditions, including earthquakes, to justify eliminating it as a basis for plant design. Our analysis also showed that the probability of a pipe break being caused by an earthquake is significantly less, by a factor of 10 to 100, than the probability of a pipe break being caused by thermal stress. The results of a companion probabilistic analysis of stiff versus flexible piping supported the opinion that inadvertent stiffness (resulting, for example, from failed pipe snubbers) can indeed reduce nuclear power plant safety.

On the basis of these technical results, we recommended that the NRC eliminate the double-ended guillotine break requirement in the reactor coolant loop of PWR designs. After an exhaustive peer review of the results by technical experts, the provisions of General Design Criterion 4 were modified by excluding from the design basis any dynamic effects associated with loss-of-coolant accidents. Our technical analyses made it possible to apply the new exclusion rule to the main reactor coolant loop piping in all U.S. PWR plants.

The rule change also indicated the removal of pipe snubbers—a decision that had two major effects. First, it reduced the amount of time that maintenance and inspection personnel had to spend in high radiation areas, thus reducing their exposure to radiation. Second, the nuclear power industry no longer had to design, fabricate, install, and maintain the costly snubber equipment. Industry spokespersons say that the rule change has resulted in savings of tens of millions of dollars for each nuclear power plant.

Case 3: Assessments for Transporting Spent Nuclear Fuel

Tens of thousands of spent nuclear fuel assemblies from U.S. nuclear power plants are currently being stored at the plants. In the near future, these spent fuel assemblies will be placed in a federal repository for permanent storage.

From 1985 to 1987, we performed a transportation model study for the NRC to determine the level of safety provided when spent reactor fuel is transported to a nuclear waste repository. During transport, the protective casks carrying the fuel could be exposed to highway or railway accidents. Our task was to evaluate and document what might happen to the casks under severe conditions and to assess how effectively the current federal transport regulations would protect the public.

This assessment represented a departure in risk-assessment techniques from reactor safety studies. The nuclear power plant probabilistic risk assessment addresses stationary facilities, with system functions and potential faults fairly well understood. In this assessment, a first in transportation regulations, we studied scenarios having nuclear material moving through populations, with various potential highway and rail accidents.

Spent fuel shipments, now occurring at a very low rate, are regulated by both the Department of Transportation (DOT) and the NRC. The NRC evaluates and certifies the design of the shipping casks used to transport spent fuel, and DOT regulates vehicles and drivers. Current NRC regulations require that shipping casks meet certain performance standards. For example, under normal operating conditions and hypothetical accident conditions, a cask must limit releases of radioactive material and minimize external radiation levels, and it must assure that the spent fuel will remain subcritical (not undergo a self-sustaining nuclear chain reaction).

The study evaluated the possible mechanical and/or thermal forces generated by actual truck and railroad accidents. The magnitudes of forces from actual accidents were compared with forces attributed to the hypothetical accident conditions defined in the NRC and DOT regulations (Figure 5). The frequency of accidents that can produce defined levels of thermal or mechanical force was also developed. With this information, the study results showed that for certain broad classes of accidents, spent fuel casks provide essentially complete protection against radiological hazards. For extremely severe accidents imposing forces on the cask greater than those implied by the hypothetical accident conditions, we made calculations of the likelihood and magnitude of any radiological hazard.

The study also contained an evaluation of the radiological risk from accidents during transport. Risk represents the summation of the products of the magnitude and likelihood of all accident outcomes. The purpose for making the risk calculations was to compare the resulting values with those previously used by the NRC in judging the adequacy of its regulations. We confirmed the adequacy of existing regulations. Our methods subsequently have become the basis for other transportation risk studies required by DOE/Defense Programs and DOE/Office of Civilian Radioactive Waste Management.

Case 4: Identifying Risks of Using Nuclear Medical Devices

Our experience with analyzing risks of radiation-emitting systems has led to performing other radiation-based analyses. In one of these cases, involving a medical application, we found it necessary to develop new techniques to evaluate the potential risks of a relatively new device for which operators have limited operating experience and processes have substantial human-factor considerations.

As part of its public health and safety charge, the NRC is responsible for regulating radiation from nuclear byproduct material. Current NRC regulations address procedures for conventional cobalt-60 teletherapy devices, but do not necessarily address appropriate or comparable procedures for the Gamma Knife (Figure 6), a commercially available external-beam radiation device. It is used to locate and surgically treat inaccessible lesions in the brain while sparing healthy tissue along some 200 radiation entry paths.

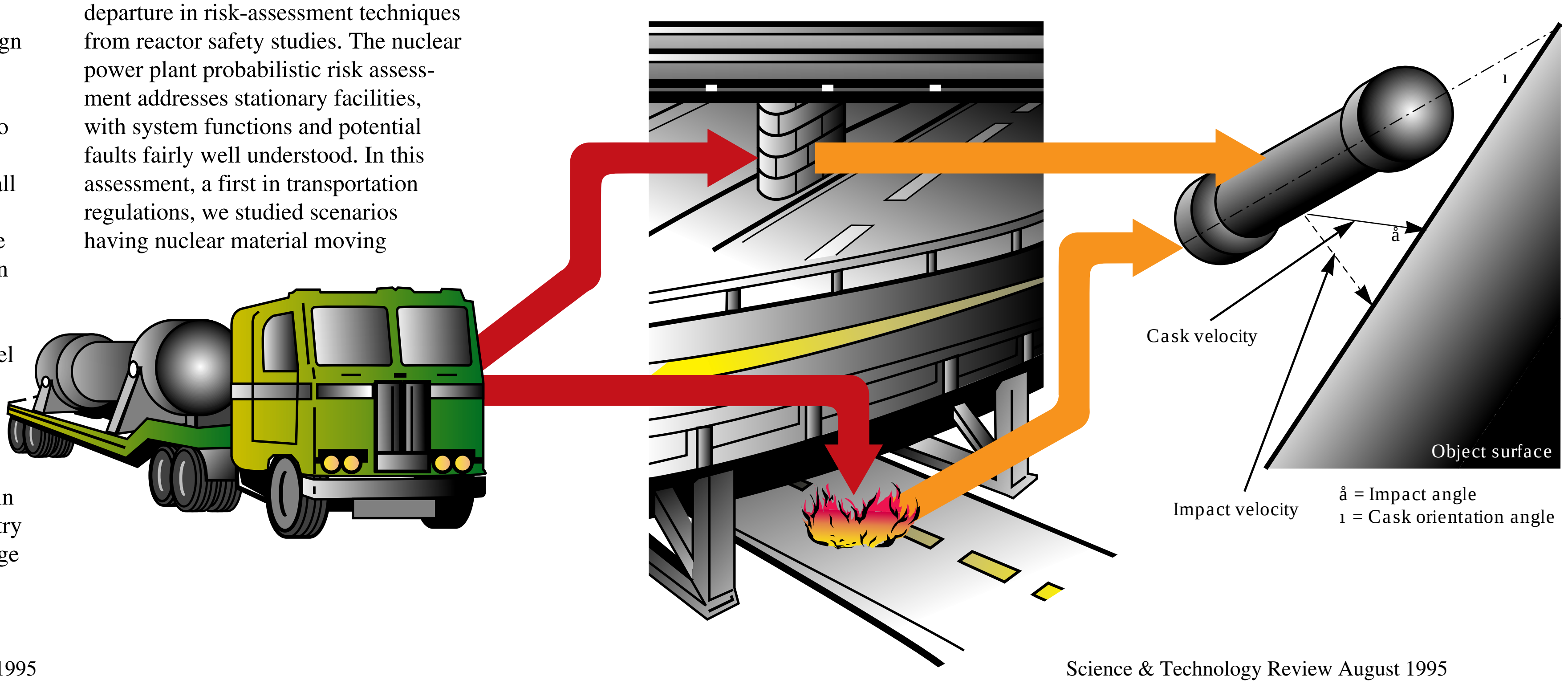


Figure 5. Comparisons were made of forces from actual transportation accidents and hypothetical conditions for a risk assessment of transporting spent nuclear fuel. Damage to the cask depends on the velocity of the cask and its orientation when it impacts a hard surface.

Reports received by the NRC pointed to some cases of misadministration in conventional teletherapy that have resulted from equipment malfunctions or human errors in treatment planning, dose calculations, and measurements. It was reasonable to project that comparable events may occur with the Gamma Knife.

The NRC therefore asked us to perform a preliminary risk analysis of the use of the Gamma Knife. Our review of cases of misadministrations and abnormal occurrences for conventional teletherapy indicated that the assessment of the risks of such an external beam therapy system should be balanced between equipment failures and human mistakes, if not skewed toward the human errors.

The Gamma Knife is used to deliver gamma radiation from cobalt-60 to precisely defined, intracranial targets. Its relatively simple hardware system requires significant human control, but because the instrument is relatively new, very little operating failure data exists for it. Most operational information resides in the, as yet, limited and little-documented experience base of the manufacturer and operators. FESSP was asked to identify the high-risk, human-initiated actions and failure modes that are most likely to occur and to evaluate their relative importance.

To do that, we adopted an approach that relied on empirical evidence, observations, and expert experience. In this approach, an analysis of the Gamma Knife treatment tasks provided a systematic framework that could adequately account for and describe activities and equipment that could lead to undesirable events or consequences. We relied on experts' estimates of likelihood, consequence, and risk for the primary tasks, and compared them by means of relative risk rankings and risk profiles. These estimates aided the identification of the highest-risk or critical tasks, without requiring an absolute quantification of risk for each task.

We believe the approach may be best used to identify weaknesses in processes and to support the development of positive performance measures, rather than to predict the numerical risk associated with poor performance. Perhaps most effective in nuclear medical applications that are not highly structured, the approach could serve to produce reliable processes and procedures to prevent misadministrations that result from mistakes. We have yet to apply these principles and techniques elsewhere, but we expect them to be applicable where human-initiated actions are important. The lesson learned is that informative assessments can be made from a relative risk analysis; the approach is also inexpensive and practical.

When to Perform Risk Assessments

Risk assessment is an excellent risk-analysis tool in that it allows us to

- Systematically examine a broad set of design and operational features.
- Integrate the influence of system interactions and human–system interactions.
- Explicitly consider uncertainties in estimates.
- Consider and analyze competing risks—those of one system versus another, or of one set of modifications versus another.
- Measure the relative importance of systems, components, and other engineered elements to risk.
- Quantify the overall level of risk for a system.
- Identify relative risks versus cost tradeoffs in design and operational modifications.

However, risk assessment also has its limitations. It may sometimes exclude or not adequately quantify potentially important risk factors, such as very-low-frequency accident initiators, various failures derived from a common event, physical processes resulting from several low-frequency failures, or long-term health effects from potentially toxic materials. Furthermore, because a risk assessment often deals with low-frequency but high-consequence accident risks, there is considerable potential for its results to be misunderstood.

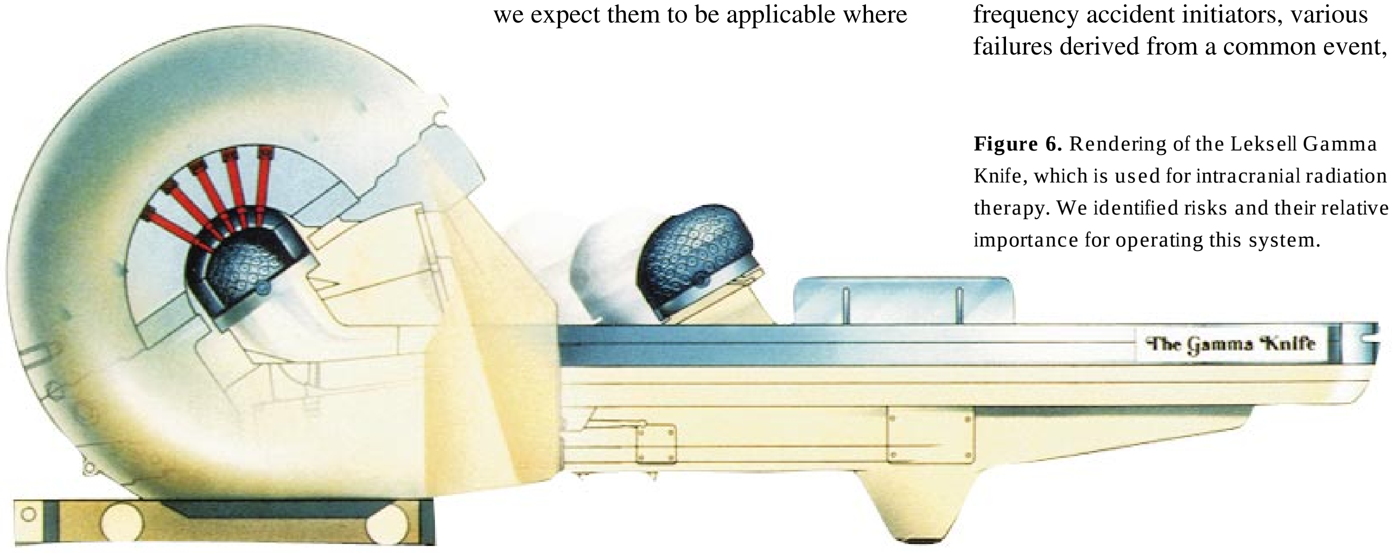


Figure 6. Rendering of the Leksell Gamma Knife, which is used for intracranial radiation therapy. We identified risks and their relative importance for operating this system.

In our experience, the most useful aspects of risk assessment are not exclusively the risk numbers that are generated; they are also the insight gained by a systematic and methodical consideration of what can go wrong with a system. A procedural analysis helps us to understand the likely vulnerabilities of the system, the threats they pose, and the measures that could be applied to mitigate or prevent them.

Risk assessment is a particularly powerful tool when there is only a limited set of alternatives for risk evaluation. "Real-world" managers, too, often have only limited resources to improve safety. Ultimately, the "best" choice will depend on the context of the manager's problem, as illustrated by our piping safety study.

We have found that it is important to do sensitivity, or "what-if," analyses to determine the relative importance of input to a risk assessment. Varied input allows us to (1) distinguish risks from variations in assumptions, modeling, or data; (2) identify where a lack of information is crucial; (3) determine which factors contribute the most to risk; and (4) investigate potential preventive or mitigative solutions that combine various risk-reduction measures. Because evaluations of alternatives or sensitivity analyses do not require absolute risk values, we can use relative risk estimates or risk rankings to compare risks. Relative risk estimates are adequate to compare alternative approaches to the same problem or to achieve comparable levels of risk across a population of similar systems. Thus, meaningful insights can be obtained by a risk assessment without depending on the accuracy of an "actual risk" value—such values are notoriously difficult to ascertain.

Uncertainty is a very important part of any risk assessment, particularly when there is an attempt to accurately quantify an actual risk. Uncertainty studies should be performed to evaluate the dependence of the assessment results on uncertainty values. Sources of uncertainty occur in models, methods, and data. Given the uncertainties inherent in any risk assessment, expert analysts may disagree over risk characterization values. Sometimes consensus is obtained by defaulting to the most conservative estimates. Such practices tend to "ratchet-up" prescriptive risk standards.

Because a risk analysis receives so much scrutiny, the risk assessment must be documented and understood. It is also extremely important to have the assessment reviewed by independent agents both internal and external to the organization performing the assessment.

Finally, the results of a risk assessment are only one of many inputs to a decision. Other factors—which may have nothing to do with technical risk per se—include cost considerations, compliance with rules and regulations, mission objectives, business operations, and public perceptions. The relationships among these factors can be complex, and the relative value of each is context dependent. Integrating these factors into the decision-making process is essential.

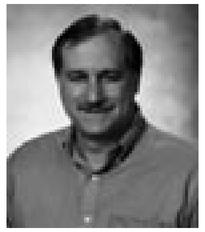
Key Words: engineering risk assessment; Fission Energy Systems Safety Program (FESSP), Nuclear Regulatory Commission (NRC); probabilistic, risk, risk assessment,

References

1. National Research Council, *Risk Assessment in the Federal Government: Managing the Process,* National Academy Press, Washington, DC (1983). This guideline has recently been augmented by a new National Research Council study, *Science and Judgment in Risk Assessment,* National Academy Press, Washington, DC (1994).
2. Registered trademark of Elekta Instruments, Inc.
3. *Code of Federal Regulations,* Title 10, Part 50.

For further information contact Edwin Jones (510) 422-8259 (jones37@llnl.gov).

About the Engineer



ED JONES came to the Laboratory in 1991, when he joined the Fission Energy and Systems Safety Program. Since 1993, he has been the Deputy Associate Program Leader for Risk Assessment, System Engineering, and Human Performance. He has written ten papers on risk assessment since arriving in Livermore.

Jones received his B.S. degree in Engineering and Physics in 1975 from the University of California, Berkeley. He did graduate work in engineering and physics at Stanford University from 1975 to 1978 and doctoral research in physics from 1979 to 1981 at the University of Oxford. Before coming to LLNL, Jones worked at Eyring Research Institute from 1983 to 1987 and at BDM International, Inc., from 1987 to 1990; he was president of Jones and Associates from 1990 to 1991.