PROBABILISTIC RISK ASSESSMENT

DEFINITION OF RISK

Risk is a measure of the potential loss occurred from natural or human activities. Potential losses are the adverse consequences of such activities in the form of loss of human life, adverse health effects, loss of property, and damage to the natural environment. Risk analysis is the process of characterizing, managing, and informing others about existence, nature, magnitude, prevalence, contributing factors, and uncertainties of the potential losses. In engineering systems, the loss may be external to the system and caused by the system to one or more recipients (e.g., human, organization, economic assets, and environment). Also the loss may be internal to the system and only damaging the system itself. For example, in a nuclear power plant, the loss can be damage to the plant caused by partial melting of the reactor core, or it can be release of radioactivity into the environment by the power plant. From an engineering point of view, the risk is associated with exposure of the recipients to hazards, and can be expressed as a combination of the probability or frequency that the hazard will occur and the consequences of that hazard. Consequences to be considered include injury or loss of life, reconstruction costs, loss of economic activity, and environmental losses. In engineering systems, risk analysis is performed to measure the amount of potential loss and more importantly the elements of the system that most contribute to such losses. This analysis can be performed either explicitly or implicitly. When explicitly addressed, targets should be set in terms of the acceptable risk levels. However, usually the engineer does not make the decision about risk acceptance of systems. Decisions are made by risk managers, policy makers, and politicians who are influenced by the prevailing economic environment, press, public opinion, interest groups, and so on. This aspect also underlines the importance of risk communication between the various parties and stakeholders involved.

CATEGORIES OF RISK

Risk can be categorized on the basis of the causes of risk or the nature of loss (consequences) or both. Risk, as mentioned, is the potential for loss. Such a loss can be ultimately measured in economic terms, and thus, risk can be viewed as a potential economic loss. However, a more appropriate categorization is based on five broad categories that account for potential losses. These risk categories are Health, Safety, Security, Financial, and Environmental.

Health risk analysis involves estimating potential diseases and losses of life affecting humans, animals, and plants.

Safety risk analysis involves estimating potential harms caused by accidents occurring from natural events (climatic conditions, earthquakes, brush fires, etc.) or human-made products, technologies and systems (i.e., aircraft crashes, chemical plant explosions, nuclear plant accidents, technology obsolescence or failure).

Security risk analysis involves estimating access and harm caused by war, terrorism, riot, crime (vandalism, theft, etc.), and misappropriation of information (national security information, intellectual property, etc.).

Financial risk analysis involves estimating potential individual, institutional, and societal monetary losses such as currency fluctuations, interest rates, share market, project losses, bankruptcy, market loss, misappropriation of funds, and property damage.

Environmental risk analysis involves estimating losses from noise, contamination, and pollution in ecosystem (water, land, air, and atmosphere) and in space (space debris).

Also, interrelations exist among these categories. For example, environmental risks may lead to financial risks.

APPLICATIONS OF RISK ANALYSIS

A traditional approach to risk analysis has been to design and/or to regulate engineering systems conservatively to avoid risk (i.e., through overdesign). These systems include, for example, the philosophy of defense-in-depth in the nuclear industry, which includes multiple safety barriers, large safety margins, quality control, and frequent inspections. Experience and research has shown that this philosophy, although reasonably assures safety, often leads to expensive systems, products, and technologies that the society and market would not be able to afford. Furthermore, studies have also shown that, although some designs and regulations based on the conservative approaches seem to reduce the risk of complex engineering systems and products, this may come at an exorbitant cost and still does not guarantee safety. Recognizing these problems, industries and regulatory agencies have been steadily relying on formal risk analysis techniques to evaluate contributors to risk and to improve safety of engineering systems more formally. For example, the U.S. Nuclear Regulatory Commission has been a pioneer in using risk-informed techniques in devising or augmenting its regulations derived from conservative defense-in-depth methods with risk analysis results. The nuclear industry and more recently transportation (land and air), space, and food safety industries promote a greater use of risk analysis in their operations and policy decision making. Risk analysis can be used in all stages of design, development, construction, and operation of engineering systems.

PROBABILISTIC APPROACH TO RISK

Probabilistic risk assessment (PRA) is a systematic quantitative procedure for investigating how complex systems are built and operated. The PRAs model how human, software, and hardware elements of the system interact with each other. Also, they assess the most significant contributors to the risks of the system and determine the value of the risk. PRA involves estimation of the degree or probability of loss. A formal definition proposed by Kaplan and Garrick (1) provides a simple and useful description of the elements of risk assessment that involves addressing three basic questions:

1. What can go wrong that could lead to exposure of hazards?
2. How likely is this to happen?
3. If it happens, what consequences are expected?

The PRA procedure involves quantitative application of the above triplets in which probabilities (or frequencies) of scenarios of events leading to exposure of hazards are estimated and the corresponding magnitude of health, safety, environmental, and economic consequences for each scenario is predicted. The risk value (i.e., expected loss) of each scenario is often measured as the product of the scenario frequency and its consequences. The main result of the PRA is not the actual value of the risk computed (the so-called bottom-line number); rather it is the determination of the system elements that substantially contribute to the risks of that system, uncertainties associated with such estimates, and the effectiveness of various risk reduction strategies available. That is, the primary value of a PRA is to highlight the system design and operational deficiencies and to optimize resources that can be invested on improving the design and operation of the system.

In the remainder of this article, the formal steps in conducting a PRA will be discussed.

STEPS IN CONDUCTING A PRA

The following subsections provide a discussion of the essential components of PRA as well as the steps that must be performed in a PRA analysis.

The NASA PRA Guide (2) describes the components of the PRA as shown in Fig. 1. Each component of PRA will be discussed in more detail in the following section.

Objectives and Methodology

Preparing for a PRA begins with a review of the objectives of the analysis. Among the many objectives that are possible the most common ones include design improvement, risk acceptability, decision support, regulatory and oversight support, and operations and life management. Once the objectives are clarified, an inventory of possible techniques for the desired analyses should be developed. The available techniques range from required computer codes to system experts and analytical experts. This, in essence, provides a road map for the analysis. The resources required for each analytical method should be evaluated, and the most effective option should be selected. The basis for the selection should be documented, and the selection process should be reviewed to ensure that the objectives of the analysis will be adequately met. See Modarres (3) and Kumamoto and Henley (4) for the inventory of methodological approaches to PRA.

Familiarization and Information Assembly

A general knowledge of the physical layout of the overall system (e.g., facility, design, process, aircraft, or spacecraft), administrative controls, maintenance and test procedures, as well as barriers and subsystems, whose job is to protect, prevent, or mitigate hazard exposure conditions, is necessary to begin the PRA. All subsystems, structures, locations, and activities expected to play a role in the initiation, propagation, or arrest of a hazard exposure condition must be understood in sufficient detail to construct the models necessary to capture all possible scenarios. A detailed inspection of the overall system must be performed in the areas expected to be of interest and importance to the analysis. The following items should be performed in this step:

1. Major critical barriers, structures, emergency safety systems, and human interventions should be identified.
2. Physical interactions among all major subsystems (or parts of the system) should be identified and explicitly described. The result should be summarized in a dependency matrix.
3. Past major failures and abnormal events that have been observed in the facility should be noted and studied. Such information would help ensure inclusion of important applicable scenarios.
4. Consistent documentation is critical to ensure the quality of the PRA. Therefore, a good filing system must be created at the outset and maintained throughout the study.

Identification of Initiating Events

This task involves identifying those events (abnormal events or conditions) that could, if not correctly and timely responded to, result in hazard exposure. The first step involves identifying sources of hazard and barriers around these hazards. The next step involves identifying events that can lead to a direct threat to the integrity of the barriers.

A system may have one or more operational modes that produce its output. In each operational mode, specific functions are performed. Each function is directly realized by one or more systems by making certain actions and behaviors. These systems, in turn, are composed of more basic units (e.g., subsystems, components, and hardware) that accomplish the objective of the system. As long as a system is operating within its design parameter tolerances, little chance exists of challenging the system boundaries in such a way that hazards will escape those boundaries. These operational modes are called normal operation modes.

During normal operation mode, loss of certain functions or systems will cause the process to enter an off-normal (transient) state transition. Once in this transition, two possibilities exist. First, the state of the system could be such that no other function is required to maintain the process in a safe condition (safe refers to a mode where the chance of exposing hazards beyond the system boundaries is negligible.) The second possibility is a state wherein other functions (and thus systems) are required to prevent exposing hazards beyond the system boundaries. For this second possibility, the loss of the function or the system is considered an initiating event. As such an event is related to the normally operating equipment, it is called an operational initiating event.

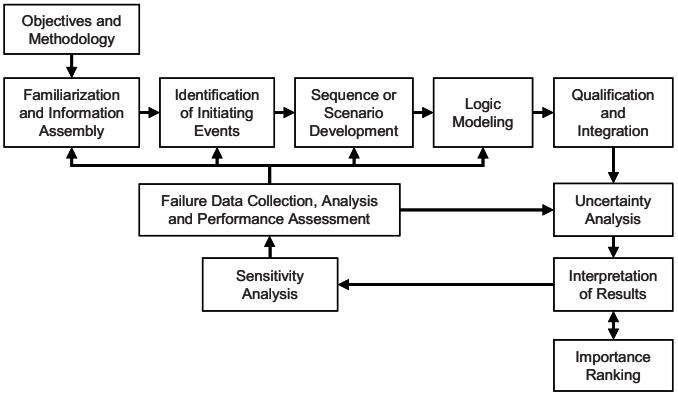

Figure 1. Components of the overall PRA process (2).

One method for determining the operational initiating events begins with first drawing a functional block diagram of the system. From the functional block diagram, a hierarchical relationship is produced, with the process objective being successful completion of the desired system. Each function can then be decomposed into its subsystems and components and can be combined in a logical manner to represent operations needed for the success of that function.

Potential initiating events are events that results in failures of particular functions, subsystems, or components, the occurrence of which causes the overall system to fail. These potential initiating events are "grouped" such that members of a group require similar subsystem responses to cope with the initiating event. These groupings are the operational initiator categories.

An alternative to the use of functional hierarchy for identifying initiating events is the use of failure mode and event analysis (FMEA) [see Stamatis (5)]. The difference between these two methods is noticeable; namely, the functional hierarchies are deductively and systematically constructed, whereas FMEA is an inductive and experiential technique. The use of FMEA for identifying initiating events consists of identifying failure events (modes of failures of equipment, software, and human) whose effect is a threat to the integrity and availability of the hazard barriers of the system. In both of the above methods, one can always supplement the set of initiating events with generic initiating events (if known). For example, see Sattison et al. (6) for these initiating events for nuclear reactors and the NASA Guide (2) for space vehicles.

To simplify the process, after identifying all initiating events, it is necessary to combine those initiating events that pose the same threat to hazard barriers and require the same mitigating functions of the process to prevent hazard exposure.

The following inductive procedures should be followed when grouping initiating events:

1. Combine the initiating events that directly break all hazard barriers.
2. Combine the initiating events that break the same hazard barriers (not necessarily all the barriers).
3. Combine the initiating events that require the same group of mitigating human or automatic actions after their occurrence.
4. Combine the initiating events that simultaneously disable the normal operation as well as some available mitigating human, software, or automatic actions.

Events that cause off-normal operation of the overall system and require other systems to operate so as to maintain hazards within their desired boundaries, but are not directly related to a hazard mitigation, protection, or prevention function, are non-operational initiating events. Non-operational initiating events are identified with the same methods used to identify operational events. One class of such events of interest is those that are primarily external to the overall system or facility. These so-called "external events" will be discussed later in more detail in this article. The following procedures should be followed in this step of the PRA:

1. Select a method for identifying specific operational and non-operational initiating events. Two representative methods are functional hierarchy and FMEA. If a generic list of initiating events is available, it can be used as a supplement.
2. Using the method selected, identify a set of initiating events.
3. Group the initiating events having the same effect on the system; for example, those requiring the same mitigating functions to prevent hazard exposure are grouped together.

Sequence or Scenario Development

The goal of scenario development is to derive a complete set of scenarios that encompasses all potential exposure propagation paths that can lead to loss of containment or confinement of the hazards, after the occurrence of an initiating event. To describe the cause-and-effect relationship between initiating events and subsequent event progression, it is necessary to identify those functions (e.g., safety functions) that must be maintained to prevent loss of hazard barriers. The scenarios that describe the functional re-

sponse of the process to the initiating events are frequently displayed by event trees. The event tree development techniques are discussed in References 2–4.

Event trees order and depict (in an approximately chronologic manner) the success or failure of key mitigating actions (e.g., human actions or mitigative hardware actions) that are required to act in response to an initiating event. In PRA, two types of event trees can be developed: functional and systemic. The functional event tree uses mitigating functions as its heading. The main purpose of the functional tree is to better understand the scenario of events at an abstract level, after the occurrence of an initiating event. The functional tree also guides the PRA analyst in the development of a more detailed systemic event tree. The systemic event tree reflects the scenarios of specific events (specific human actions, protective or mitigative subsystem operations, or failures) that lead to a hazard exposure. That is, the functional event tree can be further decomposed to show failure of specific hardware, software, or human actions that perform the functions described in the functional event tree. Therefore, a systemic event tree fully delineates the overall system response to an initiating event and serves as the main tool for continued analyses in the PRA. For detailed discussion on specific tools and techniques used for this purpose, see Modarres (7). The following procedures should be followed in this step of the PRA:

1. Identify the mitigating functions for each initiating event (or group of events).
2. Identify the corresponding human actions, systems, or hardware operations associated with each function, along with their necessary conditions for success.
3. Develop a functional event tree for each initiating event (or group of events).
4. Develop a systemic event tree for each initiating event, delineating the success conditions, initiating event progression phenomena, and designing the end effect of each scenario.

For specific examples of scenario development, see References 2–4.

Logic Modeling

Event trees commonly involve branch points at which a given subsystem (or event) either works (or happens) or does not work (or does not happen). Sometimes, failure of these subsystems (or events) is rare, and an adequate record of observed failure events may not be given to provide a historical basis for estimating frequency of their failure. In such cases, other logic-based analysis methods such as fault trees or master logic diagrams may be used, depending on the accuracy desired. The most common method used in PRA to calculate the probability of subsystem failure is fault tree analysis. This analysis involves developing a logic model in which the subsystem is broken down into its basic components or segments for which adequate data exist. For more details about how a fault tree can be developed to represent the event headings of an event tree, see Modarres et al. (8). The following procedures should be followed as a part of developing the fault tree:

1. Develop a fault tree for each event in the event tree heading for which actual historical failure data does not exist.
2. Explicitly model dependencies of a subsystem on other subsystems and intercomponent dependencies (e.g., common cause failures). For common cause failures, see Mosleh et al. (9).
3. Include all potential reasonable and probabilistically quantifiable causes of failure, such as hardware, software, test and maintenance, and human errors, in the fault tree.

Failure Data Collection, Analysis, and Performance Assessment

A critical building block in assessing the reliability and availability of complex systems is the data on the performance of its barriers to contain hazards. In particular, the best resources for predicting future availability are past field experiences and tests. Hardware, software, and human reliability data are inputs to assess performance of hazard barriers, and the validity of the results depends highly on the quality of the input information. It must be recognized; however, that historical data have predictive value only to the extent that the conditions under which the data were generated remain applicable. Collection of the various failure data consists fundamentally of the following steps: collecting generic data, assessing generic data, statistically evaluating facility- or overall system-specific data, and developing failure probability distributions using test and/or facility-specific and system-specific data. Three types of events identified during the risk scenario definition and system modeling must be quantified for the event trees and fault trees to estimate the frequency of occurrence of sequences: initiating events, component failures, and human error.

The quantification of initiating events and hazard barriers and components failure probabilities involves two separate activities. First, the probabilistic failure model for each barrier or component failure event must be established; then the parameters of the model must be estimated. Typically the necessary data include time of failures, repair times, test frequencies, test downtimes, and common-cause failure events. Additional uncertainties associated with such data must also be characterized. Kapour and Lamberson (10), Modarres et al. (8), and Nelson (11) discuss available methods for analyzing data to obtain the probability of failure or the probability of occurrence of equipment failure. Also, Crow (12) and Ascher and Feingold (13) discuss analysis of data relevant to repairable systems. Finally, Mosleh et al. (9) discusses analysis of data for dependent failures, Poucet (14) reviews human reliability issues, and Smidts (15) examines software reliability models. Establishment of the database to be used will generally involve collection of some facility-specific or system-specific data combined with the use of generic performance data when specific data are absent or sparse. For example, References 16–18 describe generic data for electrical, elec-

tronic, and mechanical equipment.

To attain the very low levels of risk, the systems and hardware that comprise the barriers to hazard exposure must have very high levels of performance. This high performance is typically achieved through the use of well-designed systems with adequate margin of safety considering uncertainties, redundancy, and/or diversity in hardware, which provides multiple success paths. The problem then becomes one of ensuring the independence of the paths, because always some degree of coupling occurs between agents of failures such as those activated by failure mechanisms, either through the operating environment (events external to the system) or through functional and spatial dependencies. Treatment of dependencies should be carefully included in both event tree and fault tree development in the PRA. As the reliability of individual subsystems increases from redundancy, the contribution from dependent failures becomes more important; in certain cases, dependent failures may dominate the value of overall reliability. The following steps should be followed in the dependent failure analysis:

1. Identify the hardware, software, and human elements that are similar and could cause dependent or common cause failures. For example, similar pumps, motor-operated valves, air-operated valves, human actions, software routine, diesel generators, and batteries are major components in process plants and are considered important sources of common cause failures.
2. Items that are potentially susceptible to common cause failure should be explicitly incorporated into the corresponding fault trees and event trees of the PRA where applicable.
3. Functional dependencies should be identified and explicitly modeled in the fault trees and event trees.

Including the effects of dependent failures in the reliability models used in the PRA is a difficult process and requires some sophisticated, fully integrated models be developed and used to account for unique failure combinations that lead to failure of subsystems and ultimately exposure of hazards. The treatment of dependent failures is not a single step performed during the PRA; it must be considered throughout the analysis (e.g., in event trees, fault trees, and human reliability analyses).

The following procedures should be followed as part of the data analysis task:

1. Determine generic values of material strength or endurance, load or damage agents, failure times, failure occurrence rate, and failures on demand for each item (hardware, human action, or software) identified in the PRA models. These values can be obtained either from facility-specific or system-specific experiences, from generic sources of data, or both.
2. Gather data on hazard barrier tests, repair, and maintenance data primarily from experience, if available. Otherwise use generic performance data.
3. Assess the frequency of initiating events and other probability of failure events from experience, expert judgment, or generic sources.
4. Determine the dependent or common cause failure probability for similar items, primarily from generic values. However, when significant specific data are available, they should be primarily used.

Quantification and Integration

Fault trees and event trees are integrated to determine the frequencies of scenarios and associated uncertainties in the calculation of the final risk values. Normally, the quantification will use a Boolean reduction process to arrive at a Boolean representation for each scenario. Starting with fault tree models for the various systems or event headings in the event trees, and using probabilistic estimates for each event modeled in the event trees and fault trees, the probability of each event tree heading (often representing failure of a hazard barrier) is calculated (if the heading is independent of other headings). The fault trees for the main subsystems, support units (e.g., lubricating and cooling units and power units) are merged where needed, and the equivalent Boolean expression representing each event in the event tree model is calculated. The Boolean expressions are reduced to arrive at the smallest combination of basic failures events (the so-called minimal cut sets) that lead to exposure of the hazards. These minimal cut sets for each of the main subsystems (barriers), which are often identified as headings on the event trees, are also obtained. The minimal cut sets for the event tree event headings are then appropriately combined to determine the cut sets for the event-tree scenarios. If possible, all minimal cut sets must be generated and retained during this process; unfortunately in complex systems and facilities, this leads to an unmanageably large collection of terms and a combinatorial outburst. Therefore, the collection of cut sets is often truncated (i.e., probabilistically small and insignificant cut sets are discarded based on the number of terms in a cut set or on the probability of the cut set.) This truncation is usually a practical necessity because of the overwhelming number of cut sets that can result from the combination of a large number of failures, even though the probability of any of these combinations may be vanishingly small. The truncation process does not disturb the effort to determine the dominant scenarios because we are discarding scenarios that are extremely unlikely.

Even though the individual cut sets discarded may be several orders of magnitude less probable than the average of those retained, the large number of them discarded may sum to a significant part of the risk. The actual risk might thus be larger than what the PRA results indicate. This possibility can be discussed as part of the modeling uncertainty characterization. Detailed examination of a few PRA studies of very complex systems, for example, nuclear power plants, shows that cut-set truncation will not introduce any significant error in the total risk assessment results [see Dezfuli and Modarres (19)].

Other methods for evaluating scenarios also exist that directly estimate the frequency of scenario without specifying cut sets. This process is often performed in highly

dynamic systems whose configuration changes as a function of time leading to dynamic event tree and fault trees. For more discussion on these systems see Chang et al. (20), the NASA Procedures PRA Guide (2), and Dugan et al. (21). Employing advanced computer programming concepts, one may directly simulate the operation of parts to mimic the real system for reliability and risk analysis [see Azarkhail and Modarres (22)]. The following procedures should be followed as part of the quantification and integration step in the PRA:

1. Merge corresponding fault trees associated with each failure or success event modeled in the event tree scenarios (i.e., combine them in a Boolean form). Develop a reduced Boolean function for each scenario (i.e., truncated minimal cut sets).
2. Calculate the total frequency of each sequence, using the frequency of initiating events, the probability of barrier failure including contributions from test and maintenance frequency (outage), common cause failure probability, and human error probability.
3. Use the minimal cut sets of each sequence for the quantification process. If needed, simplify the process by truncating based on the cut sets or probability.
4. Calculate the total frequency of each scenario.
5. Calculate the total frequency of all scenarios of all event trees.

Uncertainty Analysis

Uncertainties are part of any assessment, modeling, and estimation. In engineering calculations, we routinely ignored the estimation of uncertainties associated with failure models and parameters, because the uncertainties are very small and more often analyses are performed conservatively (e.g., by using high safety factor and design margin). As PRAs are primarily used for decision making and management of risk, it is critical to incorporate uncertainties in all facets of the PRA. Also, risk management decisions that consider PRA results must consider estimated uncertainties. In PRAs, uncertainties are primarily shown in the form of probability distributions. For example, the probability of failure of a subsystem (e.g., a hazard barrier) may be represented by a probability distribution showing the range and likelihood of risk values.

The process involves characterization of the uncertainties associated with frequency of initiating events, probability of failure of subsystems (or barriers), probability of all event tree headings, strength or endurance of barriers, applied load or incurred damage by the barriers, amount of hazard exposures, consequences of exposures to hazards, and sustained total amount of losses. Other sources of uncertainties are in the models used. For example, the fault tree and event tree models; stress-strength and damage-endurance models used to estimate failure or capability of some barriers; probabilistic failure models of hardware, software, and human; correlation between amount of hazard exposure and the consequence; exposure models and pathways; and models to treat inter- and intrabarrier failure dependencies. Another important source of uncertainty is the incompleteness of the risk models and other failure models used in the PRAs. For example, the level of detail used in decomposing subsystems using fault tree models, scope of the PRA, and lack of consideration of certain scenarios in the event tree just because they are not known or experienced before.

Once uncertainties associated with hazard barriers have been estimated and assigned to models and parameters, they must be "propagated" through the PRA model to find the uncertainties associated with the results of the PRA, primarily with the bottom-line risk calculations and with the list of risk significant elements of the system. Propagation is performed using one of several techniques, but the most popular method used is Monte Carlo simulation. The results are then shown and plotted in the form of probability distributions. Steps in uncertainty analysis are as follows:

1. Identify models and parameters that are uncertain and the method of uncertainty estimation to be used for each.
2. Describe the scope of the PRA and significance and contribution of elements that are not modeled or considered.
3. Estimate and assign probability distributions depicting model and parameter uncertainties in the PRA.
4. Propagate uncertainties associated with the hazard barrier models and parameters to find the uncertainty associated with the risk value.
5. Present the uncertainties associated with risks and contributors to risk in an easy way to understand and visually straightforward to grasp.

Sensitivity Analysis

Sensitivity analysis is the method of determining the significance of choice of a model or its parameters, assumptions for including or not including a barrier, phenomena or hazard, performance of specific barriers, intensity of hazards, and significance of any highly uncertain input parameter or variable to the final risk value calculated. The process of sensitivity analysis is straightforward. The effects of the input variables and assumptions in the PRA are measured by modifying them by several folds, factors, or even one or more order of magnitudes one at a time, and they measure relative changes observed in the PRA's risk results. Those models, variables, and assumptions whose change leads to the highest change in the final risk values are determined as "sensitive." In such a case, revised assumptions, models, additional failure data, and more mechanisms of failure may be needed to reduce the uncertainties associated with sensitive elements of the PRA.

Sensitivity analysis helps focus resources and attentions to those elements of the PRA that need better attention and characterization. A good sensitivity analysis strengthens the quality and validity of the PRA results. Usually elements of the PRA that could exhibit multiple impacts on the final results, such as certain phenomena (e.g., pitting corrosion, fatigue cracking, and common cause failure) and uncertain assumptions, are usually good can-

didates for sensitivity analysis. The steps involved in the sensitivity analysis are as follows:

1. Identify the elements of the PRA (including assumptions, failure probabilities, models, and parameters) that analysts believe might be sensitive to the final risk results.
2. Change the contribution or value of each sensitive item in either direction by several factors in the range of 2–100. Note that certain changes in the assumptions may require multiple changes of the input variables. For example, a change in failure rate of similar equipments requires changing of the failure rates of all these equipments in the PRA model.
3. Calculate the impact of the changes in step 2 one-at-a-time and list the elements that are most sensitive.
4. Based on the results in step 3 propose additional data, any changes in the assumptions, use of alternative models, and modification of the scope of the PRA analysis.

Risk Ranking and Importance Analysis

Ranking the elements of the system with respect to their risk or safety significance is one of the most important outcomes of a PRA. Ranking is simply arranging the elements of the system based on their increasing or decreasing contribution to the final risk values. Importance measures rank hazard barrier, subsystems, or more basic elements of them usually based on their contribution to the total risk of the system. The ranking process should be performed with much care. In particular, during the interpretation of the results, because formal importance measures are context dependent and their meaning varies depending on the intended application of the risk results, the choice of the ranking method is important.

Several unique importance measures exist in PRAs. For example, Fussell-Vesely (23), risk reduction worth (RRW), and risk achievement worth (RAW) (8) are identified as appropriate measures for use in PRAs, and all are representative of the level of contribution of various elements of the system as modeled in the PRA and enter in the calculation of the total risk of the system. For example, the Birnbaum (24) importance measure represents changes in total risk of the system as a function of changes in the basic event probability of one component at a time. If simultaneous changes in the basic event probabilities are being considered, a more complex representation would be needed.

Another important set of importance measures focuses on ranking the elements of the system with the most contribution to the total uncertainty of the risk results obtained from PRAs. This process is called "uncertainty ranking" and is different than component, subsystem and barrier ranking. In this importance ranking, the analyst is only interested to know which of the system elements drive the final risk uncertainties, so that resources can be focused on reducing important uncertainties.

For additional discussions on the risk ranking methods and their implications in failure and success domains, see Azarkhail and Modarres (25). Applications of importance measures may be categorized into the following areas:

1. (Re)Design: To support decisions of the system design or redesign by adding or removing elements (barriers, subsystems, human interactions, etc.)
2. Test and Maintenance: To address questions related to the plant performance by changing the test and maintenance strategy for a given design.
3. Configuration and Control: To measure the significance or the effect of failure of a component on risk or safety or temporarily taking a component out of service.
4. Reduce uncertainties in the input variables of the PRAs.

The following processes are the major steps of importance ranking:

1. Determine the purpose of the ranking, and select the appropriate ranking importance measure that has consistent interpretation for the use of the ranked results.
2. Perform risk ranking and uncertainty ranking, as needed.
3. Identify the most critical and important elements of the system with respect to the total risk values and total uncertainty associated with the calculated risk values.

Interpretation of Results

When the risk values are calculated, they must be interpreted to determine whether any revisions are necessary to refine the results and the conclusions. Two main elements are involved in the interpretation process. The first is to understand whether the final values and details of the scenarios are logically and quantitatively meaningful. This step verifies the adequacy of the PRA model and the scope of analysis. The second is to characterize the role of each element of the system in the final results. This step highlights additional analyses data and information gathering that would be considered necessary.

The interpretation process heavily relies on the details of the analysis to see whether the scenarios are logically meaningful (for example, by examining the minimal cut sets of the scenarios), whether certain assumptions are significant and greatly control the risk results (using the sensitivity analysis results), and whether the absolute risk values are consistent with any historical data or expert opinion available. Based on the results of the interpretation the details of the PRA logic, its assumptions, and its scope may be modified to update the results into more realistic and dependable values.

The ranking and sensitivity analysis results may also be used to identify areas where gathering more information and performing better analysis (for example, by using more accurate models) is warranted. The primary aim of the process is to reduce uncertainties in the risk results.

The interpretation step is a continuous process with receiving information from the quantification, sensitivity, uncertainty, and importance analysis activities of the PRA. The process continues until the final results can be best

interpreted and used in the subsequent risk management steps.

The basic steps of the PRA results interpretation are as follows:

1. Determine the accuracy of the logic models and scenario structures, assumptions, and scope of the PRA.
2. Identify system elements for which better information would be needed to reduce uncertainties in failure probabilities and models used to calculate performance.
3. Revise the PRA, and reinterpret the results until attaining stable and accurate results.

BIBLIOGRAPHY

1. Kaplan, S.; Garrick, J. On the Quantitative Definition of Risk. *Risk Analysis* 1981, **1**, pp 11–28.
2. Stamatelatos, M., et al., *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, Version 1.1; National Aeronautics and Space Administration: Washington DC, 2002.
3. Modarres, M. *What Every Engineer Should Know About Reliability and Risk Analysis*; Marcel Dekker: New York, 1993.
4. Kumamoto, H.; Henley, E. J. *Probabilistic Risk Assessment for Engineers and Scientists*; IEEE Press: New York, 1996.
5. Stamatis, D. H. *Failure Mode and Effect Analysis: FMEA from Theory to Execution*, 2nd ed.; ASQ Quality Press: Wisconsin, 2003.
6. Sattison, M. B., et al. *Analysis of Core Damage Frequency: Zion, Unit 1 Internal Events*;NUREG/CR-4550, 7, Rev. 1, 1990.
7. Modarres, M. *Risk Analysis in Engineering, Techniques, Tools and Trends*; CRC Press: Boca Raton, FL, 2006.
8. Modarres, M.; Kaminskiy, M.; Krivtsov, V. *Reliability Engineering and Risk Analysis, A Practical Guide*; Marcel Dekker: New York, 1999.
9. Mosleh, A., et al. *Procedure for Treating Common Cause Failures in Safety and Reliability Studies*; U.S. Nuclear Regulatory Commission,NUREG/CR-4780,vols.**I and II**; Washington, DC, 1988.
10. Kapur, K. C.; Lamberson, L. R. *Reliability in Engineering Design*; Wiley: New York, 1977.
11. Nelson, W. *Accelerated Testing: Statistical Models, Test Plans and Data Analyses*; Wiley: New York, 1990.
12. Crow, L. H. Evaluating the Reliability of Repairable Systems; *Proc. Annu. Reliability Maintainability Symp.*; IEEE, 1990.
13. Ascher, H.; Feingold, H. *Repairable Systems Reliability: Modeling and Inference, Misconception and Their Causes*; Marcel Dekker: New York, 1984.
14. Poucet, A. Survey of methods used to assess human reliability in the human factors reliability benchmark exercise. *Reliability Eng. Syst. Safety* 1988, **22**, pp 257–268.
15. Smidts, C. Software Reliability.In *The Electronics Handbook*;Whitaker, J. C., Ed.; CRC Press and IEEE Press: Boca Raton, FL, 1996.
16. Guidelines for Process Equipment Data, New York: Center for Chemical Process Safety; American Institute of Chemical Engineers (AICHE), 1989.
17. Military handbook, Reliability Prediction of Electronic Equipment (MIL-HDBK-217F). Department of Defense, 1995.
18. Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations (IEEE Std. 500); IEEE Standards: New York, 1984.
19. Dezfuli, H.; Modarres, M. A Truncation Methodology for Evaluation of Large Fault Trees. *IEEE Trans. Reliability* 1984, **R-33**,pp 325–328.
20. Chang, Y. H.; Mosleh, A.; Dang, V. Dynamic Probabilistic Risk Assessment: Framework, Tool, and Application; *Society for Risk Analysis Annual Meeting*; Baltimore, MD, 2003.
21. Dugan, J.; Bavuso, S.; Boyd, M. Dynamic Fault Tree Models for Fault Tolerant Computer Systems. *IEEE Trans. Reliability* 1993, **40**,p 363.
22. Azarkhail, M.; Modarres, M. An Intelligent-Agent-Oriented Approach to Risk Analysis of Complex Dynamic Systems with Applications in Planetary Missions; *Proc. of the Eighth International Conference on Probabilistic Safety Assessment and Management*; ASME: New Orleans, LA, May 2006.
23. Fussell, J. How to Hand Calculate System Reliability and Safety Characteristics. *IEEE Trans. Reliability* 1975, **R-24**.
24. Birnbaum, Z. W. *On the Importance of Different Components in a Multicomponent System*.In *Multivariate Analysis II*;Krishnaiah, P. R., Ed.; Academic Press: New York, 1969.
25. Azarkhail, M.; Modarres, M., A Study of Implications of Using Importance Measures in Risk-Informed Decisions; *PSAM-7; ESREL 04 Joint Conference*; Berlin, Germany, June 2004.

MOHAMMED MODARRES
University of Maryland