

**Department of Energy**

Washington, DC 20585

January 23, 2006

2006 JAN 26 11:08  
MAIL ROOM

The Honorable A.J. Eggenberger  
Chairman  
Defense Nuclear Facilities Safety Board  
625 Indiana Avenue, NW, Suite 700  
Washington, D.C. 20004

Dear Mr. Chairman:

Your letter of November 23, 2005 to Secretary Bodman, requested a report from the Department of Energy (DOE) "providing the details of a more aggressive plan for developing and implementing an appropriate DOE-level policy, along with the necessary implementing guidance, to ensure the appropriate use of risk assessment methodologies at defense nuclear facilities." You noted a concern that in the absence of DOE policy and guidance on the use of risk assessment, "individual program elements and field entities continue to apply various approaches on an ad hoc basis." On behalf of Secretary Bodman, I am pleased to respond to your request for a plan to develop DOE policy and guidance on the use of risk assessment methodologies.

Attached is a revised draft Department of Energy Risk Assessment Policy. You provided comments on a previous draft and this revision responds to your comments and other input. Also attached is a draft Risk Management Planning and Execution Guidance document (draft DOE G 421.1-2). This draft guidance provides DOE expectations on appropriate processes to plan and execute risk assessment methodologies for nuclear applications.

This guidance document is based on the review of other risk assessment methodologies and techniques used in other government agencies and industries as tools to aid safety decision-making. References to some of these other methodologies are provided in this document. We recognize, however, that DOE hazards and work environments are unique and evolving, and safety decisions inherently involve some assumption of risk. To properly assess and use risk-insights, we agree that DOE should provide a more formalized and disciplined structure and process for risk assessment and management so that important safety decisions are credible and defensible.

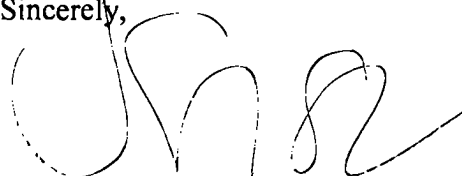
The Office of Nuclear and Facility Safety Policy developed the attached draft policy and guidance. I requested that it lead a DOE-wide effort to finalize this policy and guidance. A team will be formed to (a) further review DOE applications of risk assessment tools, (b) collaborate with other government agencies, particularly the Nuclear Regulatory Commission and the National Aeronautical Space Agency, on processes, (c) evaluate



industries standards for probabilistic risk assessments, (d) involve risk assessment experts in our National Laboratories, and (e) involve appropriate working groups from the Energy Facility Contractors Group (EFCOG).

I believe that the draft policy and guidance documents are good starting points for this collaborative effort. DOE will form a review team and hold the first planning meeting within 45 days. Your staff will be invited to this meeting. This meeting will occur after the EFCOG Safety Basis Workshop in Albuquerque on February 14 and 15, 2006. This Workshop will provide more details on expected actions, schedules and responsibilities that are necessary for the review team. We will provide those details to you after the first team meeting. I expect the next version of the policy and guidance documents within 6 months based on the broader team input. The final policy and guidance documents should be available for DOE-wide review within 12 months. This effort will be coordinated with your staff and periodic meetings and briefings will be provided.

Sincerely,

A handwritten signature in black ink, appearing to read 'J. Shaw', written over a faint, dotted outline of the signature.

John Spitaleri Shaw  
Assistant Secretary for Environment,  
Safety and Health

Attachments:

Cc:

C. Sell, S-2  
L. Brooks, NA-1  
D. Garman, ESE-1  
J. Rispoli, EM-1  
S. Johnson, NE-1  
M. Whitaker, DR-1

SEPARATION

PAGE

**U. S. Department of Energy**  
Washington, D.C.

**POLICY**

**DRAFT**  
**DOE P XXXX**

Approved: XX-XX-06

**SUBJECT: DEPARTMENT OF ENERGY RISK ASSESSMENT POLICY**

---

## **PURPOSE**

The U.S. Department of Energy (DOE) must conduct its nuclear activities in a manner that adequately protects the public, its workers and the environment. Ensuring adequate protection requires developing and implementing a basis for safe and effective operations. Establishing a proper safety basis for operations requires informed decisions by approving DOE officials that are based on credible, complete and reliable information and analysis.

DOE nuclear activities are not without some risk to workers, members of the public, the environment, or property. DOE considers the magnitude and nature of that risk in its decisions. DOE and its contractors analyze risks to provide the decision-maker with the best available information and knowledge to judge the acceptability of the risk. These analyses provide information and insights so that fully-informed and sound decisions are made.

Given the complexity and diversity of DOE's hazardous activities, a graded approach to risk assessment is appropriate. Safety decisions are supported by both qualitative and quantitative risk insights. In some instances, the traditional deterministic approach to analyzing hazards and determining the necessary controls to prevent or mitigate those hazards can be enhanced by additional risk insights.

## **POLICY**

It is DOE policy to use risk-informed approaches to support critical safety decisions when value can be added to the decision process by an assessment of the risk of operations under postulated accident scenarios. Traditional deterministic safety assessment methods prescribed in DOE directives and standards are adequate to support many operational decisions. In highly hazardous and complex operations, a risk assessment can enhance the deterministic approach by (1) prioritizing safety challenges and required controls on the basis of risk significance, (2) explicitly identifying and

quantifying uncertainties in analyses, and (3) testing the sensitivity of the results to key assumptions.

All risk assessments must be done in a disciplined and formal manner to assure the quality and credibility of the results support fully-informed and optimal decisions. If risk assessments are conducted and results are used, the results must be documented and be consistent with existing DOE rules, directives and standards.

The following are DOE expectations regarding a disciplined and consistent approach to risk assessments. These expectations will be supplemented by additional DOE guidance in the DOE Directives System.

**Planning Risk Assessments:**

- Define the purpose of the assessment – i.e., what is the goal; what is expected achievement
- Justify the use of a risk assessment technique to achieve the purpose
- Describe the methodology – i.e., what analyses will be done and how
- Describe how analysis inputs will be generated or derived
- Describe the models to be used
- Describe how the results will be used
- Describe how uncertainties will be handled and how they affect the interpretation and use of the results

**Reviewing Risk Assessments (by a peer group):**

- Was the risk assessment plan followed?
- Were the analysis inputs and assumptions justified and appropriate?
- What conclusions can be drawn from the analysis?
- What affect do the uncertainties have on the conclusions?

Risk assessments can be costly. DOE expects that risk insights can improve safety decisions and operations. Managing risk results in better use of scarce and valuable resources. We expect that the planning process will determine whether a risk assessment will improve the decision-making process to fit the available information, the associated uncertainties, and the complexity of the operations.

As part of the disciplined and formal approach to risk assessments, it is also DOE policy to share the lessons learned. A formalized process will be developed to review risk-informed decisions and share the insights and techniques across the complex, including to interested parties and affected stakeholders as appropriate. These insights may also be used to improve DOE rules, directives and standards to better institutionalize the methods and techniques.

**RESPONSIBILITIES**

Program Secretarial Officers, including the Administrator of the National Nuclear Security Administration, and associated field and site office managers are responsible for implementing this policy.

The Office of Environment, Safety and Health is the Office of Primary Interest for developing and maintaining this policy, including associated DOE rules, directives and standards.

DOE roles and responsibilities regarding this policy will be established in the DOE Safety Management Functions, Responsibilities and Authorities Manual (FRAM), DOE M 411.1-1.

**BY ORDER OF THE SECRETARY OF ENERGY:**

SEPARATION

PAGE

DOE G 421.1-2

Approved: xxxxx  
Review Date: 12-31-07

# RISK MANAGEMENT PLANNING AND EXECUTION GUIDANCE



**DRAFT January 06**

**U.S. DEPARTMENT OF ENERGY  
OFFICE OF ENVIRONMENT, SAFETY AND  
HEALTH**

**DISTRIBUTION:  
All Departmental Elements**

**INITIATED BY:  
Office of  
Environment,  
Safety and Health**



# Risk Methodology Planning and Execution Guidance

## Chapter I: Introduction

Analyses in support of management of risk at Department of Energy (DOE or Department) nuclear facilities are based largely on deterministic analyses in the evaluation of hazards and the selection of safety controls. DOE's regulatory requirements and defined acceptable methodologies for assuring the safety of its Hazard Category 1, 2, and 3 nuclear facilities are embodied in 10 CFR 830, Nuclear Safety Management. Subpart B of 10 CFR Part 830 requires the development of a safety basis for each nuclear facility that includes a Documented Safety Analysis (DSA) and Technical Safety Requirements (TSR). The DSA provides a systematic identification of hazards associated with the facility. Normal, abnormal, and accident conditions, including consideration of the need for analysis of beyond design basis accidents, that might contribute to the generation of uncontrolled release of radioactive and other hazardous materials are evaluated. Further, the DSA identifies the hazard controls necessary to ensure adequate protection of workers, the public, and the environment; and establishes the safety management programs, including a criticality safety program when criticality hazards exist, necessary to ensure safe operations. The Department's expectations, requirements, and guidance are embodied throughout the Directives system, including safe harbor approaches for DSAs in 10 CFR 830, Subpart B and Implementation Guides for DSAs and TSRs (DOE G 421.1-1 and DOE G 423.1-1, respectively).

To complement or aid decision making in the development of safety bases or the identification of appropriate safety systems, structures or components for new or existing facilities, DOE and its contractors often use risk assessment techniques. Examples of these include:

- Development of accident scenario event trees, including estimates of branch probabilities, to give an overall perspective of hazard controls and their effectiveness in preventing or mitigating the accident scenario. This includes decision making regarding selection of controls and their safety classification (as Safety Class (SC), Safety Significant (SS), or defense-in-depth.
- Development of frequency estimates associated with failure mechanisms to justify dismissing potential hazards from further consideration based on being "beyond extremely unlikely."
- Use of expert elicitation for estimation of values of parameters for accident analyses when empirical data are not available, uncertainties are large and significant, more than one conceptual model can explain or be consistent with available data, or technical judgments are needed to assess whether assumptions and calculations are appropriately conservative.
- Development of full level 1, 2, and 3 probabilistic risk assessments (PRAs) for various purposes, including programmatic decision making.

## **Chapter II DOE Applications of Risk Assessment Methodologies or Techniques**

Probabilistic risk assessment (PRA) is a comprehensive, structured, and logical analysis methodology to identify and assess risks in complex technological systems. PRA is generally used for low-probability, high-consequence events for which limited statistical data exist. PRA, as discussed in this document, is not limited to such events. Its application, meaning a structured and disciplined method at analyzing risk, is targeted at risk environments that may involve the compromise of safety, including the potential adverse impacts to people or property that may be found in DOE missions, programs or projects.

Risk analysis techniques when executed in a disciplined way can provide useful insights to technical issues. DOE elements and contractors have employed risk techniques in several areas. These include a range from development of "risk-based end states" for cleanup activities, to a proposed line oversight/contractor assurance system, to PRAs for nuclear weapons systems. These are very individualized applications of risk analysis, with varying degrees of formality, and with differing objectives.

A common misconception is that a PRA is not possible or useful when few data are available. In fact, this is precisely the situation when a PRA is most useful. The comprehensive and systematic nature of the assessment associated with a PRA is directly applicable to systems with the largest uncertainties. No PRA would be needed if all information required to ensure mission safety is known with certainty. Although a PRA is useful in all program/project life cycle phases, the type of information that is required and the types of scenarios modeled vary. This is illustrated in the following discussion of a typical program/project life cycle consisting of four phases: design, operation, upgrade, and decommissioning. This discussion demonstrates that, in all these phases, the assessment of comparative or relative risk, rather than its absolute value, will be most useful.

### **a. PRA in Design**

Design generally seeks to optimize programs, missions, and/or systems to meet required objectives and functionality within technical, schedule, regulatory, and cost constraints. A good design effort generally develops technologically feasible configurations that meet required objectives and seeks options that best satisfy schedule and regulatory constraints while minimizing costs. PRAs are used to identify and quantify the risks associated with each option for input to management trade-off processes that include minimizing risk. Even if mission specific data do not exist, failure rates and failure probabilities can be bracketed by comparisons with components where data do exist. When specific data do not exist, expert judgment data based on sound expert elicitation processes can be used to estimate top-level relative risk conclusions. Risk importance measures determined by a PRA will also serve to focus the evolution of the design.

### **b. PRA in Operation**

During operation, especially for new programs and missions, there are many questions related to the anticipated success of the program or mission. A PRA performed prior to operation can serve to predict impacts to the program that could be detrimental to success. Thus, given that the design is acceptable from a safety perspective, a PRA for operations can focus on those aspects of risk that relate to system operability and maintenance and the performance of the mission. Risk importance measures determined by the PRA can be used to optimize procedures and resource allocations during operation. A PRA for operations can also include performance considerations and regulatory requirements. If there are problems meeting performance or regulatory requirements, PRA can identify modifications to hardware, software, and operational parameters that may be the appropriate solutions.

c. PRA in Upgrade

After operating a system for a while, experience is gained and improvements may be required. In addition, changing technology, obsolescence of components, and aging will play significant roles in the need for improvement or upgrades to a system. To this end, a PRA can identify upgrade options that minimize risk. Generally each upgrade will have its advocates. PRA provides an assessment tool for evaluating the relative risk benefits of alternative upgrade options.

d. PRA at End of Life or in Decommissioning

When a product is at the end of its useful life, it is important that its end of operation and subsequent dismantling and disposal be conducted cost-effectively, with due consideration to regulatory requirements and regard to the safety of the surrounding population and environment. A PRA can be effectively used to assess dismantling, decommissioning, and disposal options that minimize risks. Transitioning to a replacement system can also be included in this category if the replacement system is drastically different from the system being replaced, or if the transition is terminal. If the replacement system is an improvement, transitioning can be included as an upgrade as described in paragraph II c. above.

Given the dissimilarities in the nature and consequences of the use of the various DOE facilities, a single approach for incorporating risk analyses into the safety assurance process is not practical or useful. However, risk methods and insights can be broadly applied to ensure that the best use is made of available techniques to foster consistency in DOE decision making. For example, probabilistic methodologies may be appropriate, as a decision support tool, in efforts which seek to prioritize activities or to analyze the risk from competing alternatives. Risk analysis approaches may also be useful in specific backfit analyses, system failure analyses, and the assessment of the reliability of safety controls. Other uses may include, but are not limited to, assessments of the overall risk of selected activities on a case-by-case basis, and certain environmental assessments and nuclear weapons applications.

Probabilistic risk assessment techniques can be an effective adjunct to the conventional approach to nuclear safety. It is sometimes argued that probabilistic risk assessment is not useful when there are limited data for a particular system or activity. This is actually the circumstance in which probabilistic risk assessment techniques can be most beneficial to safety evaluation. The comprehensive, integrated, and systematic character of the probabilistic risk assessment process is directly applicable to systems and activities with the largest uncertainties. Much can be learned about a system or activity from the initial qualitative understanding and model building that occurs in the use of PRA techniques. Unintended, adverse inter-system dependencies are uncovered at this stage as well as operations that can be improved.

As described above, DOE has employed risk assessment tools in a variety of activities, including the development of safety analyses and facility-level decision making. The level of formality of these assessments varies over a wide range. Other federal agencies involved in similar high-risk activities have, to varying degrees, relevant standards and defined organizational elements, procedures, and processes for the development and use of risk management tools. It is the purpose of this document to provide some guidance regarding important factors to consider when using these tools to ensure that the results are credible, defensible, and documented.

## **Chapter II DOE Risk Analysis Expectations**

When risk analyses techniques are used for purposes related to nuclear safety, i.e., can influence decisions made relating to nuclear facility safety bases, DOE has minimum expectations regarding a disciplined approach to such work.

1. Prior to embarking on an analysis using risk techniques, a planning document should be generated that would address the following items:
  - a. Define the purpose of the analysis, i.e., what is the goal; what is trying to be achieved.
  - b. Justify the use of risk analysis technique to achieve that purpose.
  - c. Describe the methodology, i.e., specifically what analyses will be done and how.
  - d. Describe how analysis inputs will be generated or derived.
  - e. Describe the models to be used.
  - f. Describe how the results will be used.
  - g. Describe how uncertainties will be handled and how they affect the interpretation and use of the results.
2. After the analysis has been completed, it should be peer reviewed. The review should address the following items;
  - a. Was the plan for the analysis followed?
  - b. Were the analysis inputs and assumptions justified and appropriate?
  - c. What conclusions can be drawn from the analysis?
  - d. What affect do the uncertainties have on the conclusions?

The following sections provide a discussion of a planning document for a study that employs risk methodologies. The level of detail included in a planning document should be tailored to the complexity and significance of the study that is planned. It is not intended that development of the plan become a burdensome exercise that would inhibit the decision to proceed with a study. However, the elements discussed below are useful considerations when undertaking a study, and should be addressed at some level in the project planning.

This document is not intended to be a "how to" treatise on PRA methods. There is an extensive body of literature that deals with those topics. This guide does liberally borrow from the references cited.

### **1. Planning**

#### **a. Purpose of the Analysis**

A description of the reasons why an analysis is being conducted is necessary to guide those performing it so that they may appropriately design their approach to address the issues at hand. Without this step, the rest of the assessment will be either incomplete or inadequate and, therefore, a waste of time, money, and effort. It is also necessary so as to

evaluate whether the analysis has achieved its intended purpose. This should be a high-level statement of purpose. It should be neutral with respect to the outcome.

As part of this element, the underlying decision that must be made, the options available, relevant decision factors and the stakeholders involved should be identified,

b. Justification of the Use of Risk Techniques to Achieve the Purpose.

The risk techniques that may be used range from full scope, limited scope, and simplified PRAs and various sub elements of them, such as event trees and fault tree analyses, uncertainty analyses, and expert elicitation.

PRA has become a principal analytical methodology for identifying and analyzing technical and safety risk associated with complex systems, projects, and programs. PRA facilitates risk management activities by identifying dominant contributors (those events that contribute most to risk) so that resources can be allocated to significant risk drivers and not wasted on items that insignificantly affect overall system risk.

PRA provides a framework to quantify uncertainties in events that are important to system safety. By requiring the quantification of uncertainty, PRA informs the decision-makers of the sources of uncertainty and provides information that helps determine the worth of investing resources to reduce uncertainty.

The PRA process identifies weaknesses and vulnerabilities in a system that can adversely impact safety, performance, and mission success. This information in turn provides insights into viable risk management strategies to reduce risk and directs the decision-maker to areas where expenditure of resources to improve design and operation may be more cost-beneficial.

The most useful applications of PRA have been in the evaluation of complex systems subject to low-probability and high-consequence scenarios and the evaluation of complex scenarios consisting of chains of events, each of which may adversely impact the system. These complex scenario impacts may include events that separately may appear to be slight or insignificant but collectively can combine and interact to cause high severity consequences.

c. Methodology Description

A "full-scope" analysis contains all major PRA components in terms of three basic questions: (1) What can go wrong? (2) How likely is it? (3) What are the consequences? Full-scope PRAs address all applicable end states that lead to failure to meet safety and mission objectives. Completeness of scenarios is an important consideration in a full-scope PRA. Uncertainty analysis should be performed to provide the decision-maker with a full appreciation of the overall degree of uncertainty about the PRA results and an understanding of which sources of uncertainty are critical to the results that guide decisions.

A "limited-scope" PRA applies the same general rigor as a full-scope PRA but focuses on some of the mission-related end states of specific decision-making interest, instead of all applicable end states. The scope is limited and is defined on a case-by-case basis, so that the results can provide specific answers to pre-identified mission-critical questions and safety concerns, rather than the assessment of all relevant risks. Similar to a "full-scope" PRA, sources of uncertainties that have a strong effect on the limited-scope PRA results and insights should be identified and quantified.

A "simplified" PRA applies identifies and quantifies major (rather than all) mission risk contributors (to all end states of interest) and generally applies to systems of lesser technological complexity or systems having less available design data than those requiring a full-scope PRA. Thus, a simplified PRA contains a reduced set of scenarios or simplified scenarios designed to capture only essential, sometimes top level, mission risk contributors. In a simplified PRA, the sources of uncertainties that have the strongest effects on the PRA results should be identified and, in cases where they affect the management decision process, should be quantified.

Event trees identify and evaluate potential scenarios leading to undesired consequences. The modeling of each accident scenario is an inductive process that usually involves graphical and logical tools/techniques. An event tree starts with the initiating event and progresses through the scenario, a series of successes or failures of intermediate events (also called pivotal events or top events), until end states are reached. The binary logic option of success or failure is usually employed at each branch point of an event tree.

The modeling of the failure causes (or their complements, successes) of each pivotal event or event tree top event is a deductive process that usually involves tools called fault trees. A fault tree consists of three parts. The top part is the top event, which corresponds to the failure of a pivotal event (or event tree top event) in the accident scenario. The middle part consists of intermediate events (faults) causing failure of the top event. These events are linked to the bottom part of the fault tree, the basic events, whose failure ultimately causes the top event to occur. The fault trees are then linked to the accident scenarios and simplified to support quantification. The combination of the inductive logic of event trees with the deductive logic of fault trees is a very powerful asset in PRA scenario modeling.

Quantification refers to the process of estimating the frequency and the consequences of the undesired end states. The frequency of occurrence of each end state is calculated using a fault tree linking approach resulting in a logical product of the initiating event frequency and the (conditional) probabilities of each pivotal event along the scenario path from the initiating event to the end state. The fault trees for each pivotal event are linked to the event tree to quantify the pivotal events in terms of the basic events. All like end states are then grouped; i.e., their probabilities are logically summed into the probability of the representative end state.

Because PRA attempts to model uncertain events (events that exhibit variability that cannot be eliminated), the risk model is, in essence, an uncertainty analysis model. Recognition of uncertainty analysis as the fabric of the PRA model is paramount to proper application of PRA results in the risk management decision-making process. PRA analysts find ways to quantify and present the uncertainty associated with risk results in a manner that is understandable to decision-makers. Any PRA insights reported to decision-makers should include an appreciation of the overall degree of uncertainty about the results and an understanding of which sources of uncertainty are critical. Presentation of PRA results without uncertainties significantly detracts from the quality and credibility of the PRA study.

Sensitivity analysis is a type of uncertainty analysis that focuses on modeling uncertainties in assumptions, models, and basic events. These analyses are frequently performed in a PRA to indicate those analysis inputs or elements whose value changes cause the greatest changes in partial or final risk results. A sensitivity analysis is aimed at evaluating result changes due to postulated input parameter changes. This type of analysis is often performed to determine which input parameters in a PRA are most important and deserve the greatest attention and need for improvement.

The PRA should conduct data analyses to support quantification. Data analysis refers to the process of collecting and analyzing information in order to estimate various parameters of the PRA models. These parameters are used to obtain probabilities of the various events including component failure rates, initiator frequencies, and human and software failure probabilities. Developing a PRA database of parameter estimates involves: (1) identification of the data needed; (2) data collection; and (3) parameter estimation using statistical methods to develop uncertainty distributions for the model parameters. In cases where there are no statistically significant data to support PRA parameter estimation, the PRA analyst may need to rely on expert judgment and elicitation. The data analysis task proceeds in parallel or in conjunction with the steps described above.

d. Describe How Analysis Inputs Will Be Generated or Derived

Information needed for decision making is characterized by its precision and certainty. In any decision making process there are competing factors regarding data collection: the need for more and better information and the cost or practicality of obtaining it. These competing factors need to be balanced, considering what level of analysis is appropriate to the decision to be made.



Various types of data need to be collected and processed when using risk techniques. These data may be component failure rates, repair times, initiating event probabilities, intermediate event probabilities, parameters for accident progression analyses, and parameters for consequence analyses. Many of these factors may be represented as data sets with some variability and/or uncertainty. This would be typical for risk methodologies, even if such data sets are only used to provide mean values, rather than using bounding or upper limit, or conservative values of parameters, when such data are available.

In order to achieve some sort of uniformity and repeatability, a well-defined protocol and criteria need to be established that would be used to obtain and qualify a statistical distribution for use in the methodology or for establishing mean values. DOE-STD-3010 is often the primary source for accident parameters, but it specifically cautions against using distributions of very limited experimental data. The protocol and the criteria for establishing distributions of parameters need to deal with the uncertainties associated with individual data points, confidence levels associated with a set of data, the amount of data needed to define a distribution, etc. Where adequate data are not available to establish distributions, reasonably conservative values should be selected. Sensitivity studies may be useful in determining the relative importance of parameters with limited data to support the analyses.

e. Describe the Models to Be Used

The elements of a PRA analysis models include identification of initiating events, application of event sequence diagrams or event trees, modeling of pivotal events, assignment of probabilities or frequencies, consequence modeling (source term and effects), and treatment of uncertainties (state of knowledge and variability). Many, if not most of the applications of risk methodologies within DOE only involve a subset of these elements. The particular focus of a project and the models to be employed should be described. For example, in assignment of probabilities or frequencies, Bayesian update techniques or expert elicitation may be employed. It is important to describe the methodologies and models that are important to the analysis results.

There are many hazard and risk assessment tools. They include:

1. Pareto analysis
2. Checklist analysis
3. Relative ranking/risk indexing
4. Preliminary risk analysis (PrRA)
5. Change analysis
6. What-if analysis
7. Failure modes and effects analysis (FMEA)
8. Hazard and operability (HAZOP) analysis
9. Fault tree analysis (FTA)
10. Event tree analysis (ETA)
11. Event and causal factor charting

## 12. Preliminary hazard analysis (PrHA)

Choosing the right method for the situation is, of course, key to any successful risk assessment. To select an appropriate risk assessment tool, several factors should be considered.

The type of results needed is an important factor in choosing a risk assessment technique. Depending on the reason for the risk assessment, many types of results may be needed to meet the study's objective. Following are five categories of information that can be produced from most risk assessments:

- Possible problems
- Ways in which these problems occur (i.e., failure modes, causes, sequence)
- Ways to reduce the frequency of these problems
- Areas needing further analysis or input for a quantitative risk analysis
- Ranking of results

The type of information available is another factor. Two important conditions define the information available to a risk assessment team: (1) the current phase of life for the activity or system and (2) the quality and timeliness of the documentation.

The first condition is usually fixed for any risk assessment. The stage of life limits the amount of information available to the risk assessment team. For example, if a risk assessment is to be performed on a proposed activity, it is unlikely that detailed descriptions of the activity, written procedures, or design drawings would be available. Therefore, if the choice is between hazard and operability (HAZOP) analysis and what-if analysis, this phase-of-life factor would call for a less detailed analysis technique, such as what-if.

The second condition deals with the quality and timeliness of existing documentation. For a risk assessment looking at an existing activity or system, the design drawings may not be up to date or do not exist in a suitable form. Using out-of-date information is not only futile, it is a waste of time and resources. Therefore, if all other factors point to a technique that must have such information, the information should be updated before performing the risk assessment.

Some techniques get bogged down when they are used to analyze very complicated problems. The complexity and size of a problem are based on the number of activities or systems, the number of pieces of equipment, the number of operating steps, and the number and types of events and effects being analyzed. For most risk assessment techniques, a larger number of equipment items or operating steps will increase the time and effort needed to perform a study. The effort required to perform a risk assessment is proportional to the types and number of events and effects being evaluated.

The choice of techniques can also be affected by the type of operation. Whether an activity is permanent or not affects the choice of technique in the following way: If all

other factors are equal, a more detailed approach may be used if the process will continue operating for a long time. A more detailed and better documented risk assessment of a permanent operation could be used to support other needed activities, such as safety programs or employee training programs. On the other hand, a less detailed technique might be chosen if the subject activity is a one-time operation.

More thorough techniques are appropriate for those systems involving significant risk and for situations in which failures are expected to have severe consequences. This approach increases the chances that possible problems will be uncovered.

f. Describe How the Results Will Be Used

This topic will be closely correlated with the topic of the purpose of the analysis. It should be more specific on the actions that are expected to be affected by the results. For example, will the results affect a specific project, and if so, how? Or will the results be used in a more generic sense, e.g., that has the potential for affecting multiple projects. It would be useful to identify upfront some metrics for decision making that can be objectively used when the study is completed.

g. Describe How Uncertainties Will Be Handled And How They Affect The Interpretation And Use Of The Results

The models used in both the general decision-making structure and in detailed risk assessments will never be perfect. The detail in a model and scope boundaries will determine how well the model reflects reality. Even if the data are perfect, the model usually brings some doubt into the results.

More detailed levels of risk analysis can reduce model uncertainty by more thoroughly accounting for potentially important loss sequences. However, more thorough analysis also costs more.

The simplest risk assessments are historical event summaries and account only for known accidents, and possibly some near misses that have occurred during some reporting period. Streamlined risk assessments require more resources, but they also account for more near misses, as well as other recognized accident scenarios that did not occur. More detailed risk assessments require even more resources, but they systematically identify and account for previously unrecognized accident scenarios.

Data uncertainty causes much concern during decision making. Data uncertainty arises from any or all of the following:

- The needed data do not exist
- The analysts do not know where to collect the data, or they do not have the staff, funds, or time to collect it

- The quality of the data is questionable, usually because of the methods used to gather it
- The data vary widely, making their use complex

Although steps can be taken to reduce uncertainty in data, all data have some uncertainty. This uncertainty cannot be ignored. Following are methods available for dealing with data uncertainty:

- Subjectively characterize uncertainty (for example, as high or low). A simple approach in which doubt in the final answer is estimated based on personal experience or belief.
- Perform calculations using best-case and worst-case situations. An approach that uses different calculations for best-case and worst-case conditions to reflect the range of possible outcomes.
- Analyze a number of possible situations (i.e., what-if scenarios). An expanded version of the previous approach that involves calculations for many other sets of conditions, usually including an estimate of how likely each set is to occur.
- Decrease the precision requirements. Using broader ranges when categorizing the frequency and consequence of accidents increases the certainty in the selection.
- Perform calculations using probability distributions in place of discrete estimates. A more complicated approach that uses statistics to describe data used in a model so that statistical descriptions of the expected outcomes can be formed.

Choose a simple method first for dealing with uncertainty. If decision makers need better estimates, the uncertainty can be reduced for the issues that most affect the model.

## **2. Peer Review**

In those situations where probabilistic methods are used as a decision support tool, the cognizant Secretarial Officer should ensure that a high quality analysis is conducted commensurate with the importance and complexity of the activity. The analysis should be performed and peer reviewed by qualified personnel using a graded approach that is consistent with industry and consensus standards and reflects the state of the art in modern risk analysis.

The quality of a risk analysis used to support a DOE application is gauged by its scope, level of detail, and technical acceptability. These should be commensurate with the application for which it is intended and the role of the risk analysis results in the safety issue to be informed. Clearly, if heavy emphasis is placed on risk insights and on risk analysis results in the decision making process, then more requirements that must be placed on the risk analysis, in terms of scope, level of detail, and technical acceptability. Conversely, this emphasis can be reduced if a safety decision could be based mostly on conventional prescriptive and deterministic approaches.

In all application cases, a risk analysis should be realistic with regard to the actual design, construction, operational practices, and operational experience of the DOE facility or activity.

After the analysis has been completed, it should be peer reviewed. The review should address the following items;

1. Was the plan for the analysis followed?
2. Were the analysis inputs and assumptions justified and appropriate?
3. What conclusions can be drawn from the analysis?
4. What affect do the uncertainties have on the conclusions?

The following paragraphs provide an approach for conducting a peer review.

a. Analysis Plan and Scope

Review questions

1. Has the purpose of the risk assessment been clearly defined? This should include a definition of the decision that needs to be made, the questions that must be answered to make the decision, and the type, precision, and certainty of the information necessary to answer the questions. Once the purpose of the risk assessment has been verified, the rest of the review will focus on judging how well the risk assessment process fulfills its purpose.

2. Are the boundaries of the risk assessments defined? Specific boundaries of the analysis are sometimes established. For the purposes of a review, the key is to be sure that established constraints are (1) consistent with the purpose of the analysis (e.g., critical issues are not being ignored) and (2) appropriately observed by the analysis team.

b. Inputs and Assumptions

Data include both qualitative and quantitative information collected and analyzed during an assessment. It is essential to understand how data were collected for the risk assessment. The data collection methods should be clearly defined and defended in the risk assessment report.

Review questions

1. Were appropriate data collected for the risk assessments?

- Did the risk assessment team develop the types of information needed by the decision makers?
- Is each type of information presented with the precision and certainty required by decision makers?
- Was an appropriate process used to gather and elicit the data dependably?
- Were skilled individuals used to facilitate the data collection process?

2. Were data collected from the best sources?

- Were appropriate subject matter experts involved throughout the risk assessment?
- Were appropriate databases used to collect historical experience data?
- Were the databases used appropriately?

3. Are raw data included in the risk assessment report, or are they otherwise available?

The raw data should be included as an appendix, or should be available in some form, so that the logical progression from data collection to data analysis to recommendations and conclusions is verifiable.

c. Data analysis

Once the data are collected, they must be analyzed so that proper conclusions can be drawn. As with data collection, the data analysis methods should be clearly defined and defended.

Review questions

1. Was the data analysis performed competently? The answer to this question is based on the experience and skill of the analysts as well as whether the analysts used established and accepted methods.

2. Is it easy to see how the collected data were analyzed? The reviewer should be able to easily see how the collected data were treated during the data analysis process. For example, raw data may be itemized on a table. The item numbers are then transferred to the data analysis component of the risk assessment to show how and where the raw data were actually analyzed. Also, data simulations may be used, and the impact from these simulations should be clear.

3. Are the actual results from the data analysis presented clearly? Often, large amounts of data are analyzed in a risk assessment. To ensure that the proper recommendations are presented and appropriate conclusions are drawn, the results of the data analysis should be presented in a tabular, matrix, or other summary format. The recommendations and conclusions can then be derived and defended from these summary results.

d. Recommendations and Conclusions

A risk assessment is not complete if it does not contain recommendations and conclusions. Recommendations are made by the analysis team to improve the risk performance. The conclusions are an interpretation of the results of the data analysis. Conclusions are often made about the overall acceptability of risk. They also include other key observations about the risks, such as contributions, costs, vulnerable populations, etc.

Review questions

1. Is it easy to see how the recommendations and conclusions were made? The reviewer should be able to easily see how the results from the data analysis were used to generate recommendations and conclusions. Recommendations and conclusions should be defended based on the data analysis results.
2. Do the conclusions answer the questions from which the risk-based decisions will be made? If the conclusions do not tie in with the purpose of the analysis, then the risk assessment did not meet its main objective.
3. Were sensitive policy issues treated with proper care? Some recommendations and conclusions may be inflammatory to some audiences and should be worded appropriately.
4. Was the organization of the report effective? The report itself should clearly lead readers from the scope of the risk assessment through the recommendations and conclusion without the need for additional supporting materials, explanations or presentations.

## References:

1. Issues and Recommendations for Advancement of PRA Technology in Risk-Informed Decision Making – Technology Insights, ACRS, NUREG/CR-6813, April 2003.  
*This document provides a historical perspective of USA PRA development in the nuclear power industry and identification and discussion of frequent issues in PRA reviews. It also discusses the relationship between deterministic and probabilistic safety approaches.*
2. An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities, Regulatory Guide 1.200 For Trial Use, US NRC, February 2004.  
*The Regulatory Guide addresses issues of technical adequacy and peer reviews of PRA submittals.*
3. Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, Office of Safety and Mission Assurance, NASA, August 2002.  
*This NASA guide is a reference for a complete discussion of PRA techniques and methodologies.*
4. Guiding Principles for Monte Carlo Analysis, US EPA, EPA/630/R-97/001, March 1997.  
*This document resulted from the efforts of a Technical Panel established by the EPA Risk Assessment Forum. It contains useful definitions, considerations in selection of models, discussion of selection of input data, and evaluation of variability and uncertainty.*
5. Risk-based Decision-making Guidelines, US Coast Guard, electronically available at: <http://www.uscg.mil/hq/g-m/risk/e-guidelines/RBDM.htm>  
*This electronically available document covers the total process of planning and conducting risk analyses. It is highly recommended.*
6. An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, Regulatory Guide 1.174, US NRC, November 2002.  
*The Regulatory Guide addresses many of the issues important to quality and completeness that are important to the type of applications that PRA may be used in DOE to support safety decisions.*



## GLOSSARY:

## PROBABILISTIC RISK ASSESSMENT CONCEPTS AND TERMINOLOGY

The following is a brief exposition on probabilistic risk assessment concepts and terminology. It generally follows the approach taken by the U. S. Nuclear Regulatory Commission, but is modified here for application to DOE facilities.

### **1. Risk and Risk Assessment:**

Risk is characterized by three questions: "What can go wrong?" "How likely is it?" and "What are the consequences?" These three questions can be referred to as the "risk triplet." The traditional definition of risk, that is, probability times consequences, is fully embraced by the "triplet" definition of risk.

The first question, "What can go wrong?" is usually answered in the form of a "scenario" (a combination of events and/or conditions that could occur) or a set of scenarios. This requires a qualitative understanding of the facility or activity. The development of scenarios should be done with or by the personnel who know the facility or activity best: the designers and/or operators.

The second question, "How likely is it?" can be answered in terms of the available evidence and the processing of that evidence to quantify the probability and the uncertainties involved. In some situations, data may exist on the frequency of a particular type of occurrence or failure mode (e.g., accidental overexposures). In other situations, there may be little or no data (e.g., core damage in a reactor) and a predictive approach for analyzing probability and uncertainty will be required. The quantification of scenarios should be done by personnel who can develop and manipulate logic models (e.g. fault trees and event trees) and data analysts who can perform the necessary computations.

The third question, "What are the consequences?" can be answered for each scenario by assessing the probable range of outcomes (e.g., dose to the public or worker). The outcomes or consequences are the "end states" of the analyses. This stage of the analysis involves personnel with expertise in the evaluation of physical and chemical phenomena.

The choice of consequence measures will depend on the safety issue being addressed (e.g. likelihood of physical damage to a structure, dose to a worker, etc).

A risk assessment is a systematic method for addressing the risk triplet as it relates to the performance of a particular system (which may include a human component) to understand likely outcomes, sensitivities, areas of importance, system interactions and areas of uncertainty. From this assessment the important scenarios can be identified.

### **2. Deterministic and Probabilistic Analyses:**

Safety assurance by DOE is implicitly related to the three questions discussed in item 1 above. In practice, DOE addresses these three questions through the orders, standards, guidance, and operational conditions that it uses to ensure safety of the many activities within the complex. These are based largely on deterministic analyses and safety is implemented by prescriptive requirements. Traditionally, the deterministic approach establishes requirements for engineering margin and for quality assurance in design, manufacture, and construction. In addition, it assumes that adverse conditions can exist and establishes a specific set of design basis events (i.e., what can go wrong?). The deterministic approach involves implied, but unquantified, elements of probability in the selection of the specific accidents to be analyzed as design basis events. It then requires that the design include safety systems capable of preventing and/or mitigating the consequences (i.e., what are the consequences?) of those design basis events in order to protect public health and safety. Thus, a deterministic analysis explicitly addresses two questions of the risk triplet. In addition, traditional safety analyses do not integrate results in a comprehensive manner to assess the overall safety impact of postulated initiating events.

Risk assessment considers risk (i.e., all three questions) in a more coherent, explicit, and quantitative manner. Risk assessment methodology examines systems and their interactions in an integrated, comprehensive manner. Probabilistic analysis explicitly addresses a broad spectrum of initiating events and their event frequency. It then analyzes the consequences of those event scenarios and weights the consequences by the frequency, thus giving a measure of risk.

### **3. Risk Insights:**

The term "risk insights", as used here, refers to the results and findings that come from risk assessments. The end results of such assessments may relate directly to public or worker health effects. For specific applications the results and findings may take other forms. For example, for reactors these include prediction of core damage frequency or offsite radiological release frequency. For other facilities or activities in the DOE complex, findings and results include risk results for disposal facilities for radioactive wastes, for production and maintenance of special nuclear materials, etc.

### **4. Risk-Based Approach:**

Decision-making is required in both the development of orders and guidance and the determination of compliance with those orders and guidance. A "risk-based" approach to decision-making is one in which such decision-making is solely based on the numerical results of a risk assessment. This places heavier reliance on risk assessment results than is currently practicable for DOE (and for other agencies). For example, the U.S. NRC does not endorse an approach that is "risk-based"; however, the Commission notes that this does not invalidate the use of probabilistic calculations to demonstrate compliance with certain criteria, such as dose limits.

### **5. Risk-Informed Approach:**

A "risk-informed" approach to decision-making represents a philosophy whereby risk insights are considered together with other factors to establish requirements that better focus attention on design and operational issues commensurate with their importance to public and worker health and safety. A "risk-informed" approach enhances the deterministic approach by: (a) allowing explicit consideration of a broader set of potential challenges to safety, (b) providing a logical means for prioritizing these challenges based on risk significance, operating experience, and/or engineering judgment, (c) facilitating consideration of a broader set of resources to defend against these challenges, (d) explicitly identifying and quantifying sources of uncertainty in the analysis (although such analyses do not necessarily reflect all important sources of uncertainty), and (e) leading to better decision-making by providing a means to test the sensitivity of the results to key assumptions. Where appropriate, a risk-informed regulatory approach can also be used to reduce unnecessary conservatism in purely deterministic approaches, or can be used to identify areas with insufficient conservatism in deterministic analyses and provide the bases for additional requirements or regulatory actions.

#### **6. Risk-Informed Approach and Defense-in-Depth:**

The concept of defense-in-depth<sup>(1)</sup> has always been a rule of good practice in the nuclear field. Risk insights can make the elements of defense-in-depth more clear by quantifying them to the extent practicable. Although the uncertainties associated with the importance of some elements of defense may be substantial, the fact that these elements and uncertainties have been quantified can aid in determining how much defense is beneficial to safety. Decisions on the adequacy of or the necessity for elements of defense should reflect risk insights gained through identification of the individual performance of each defense system in relation to overall performance.

Defense-in-depth is an approach to safety that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility. The defense-in-depth philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility. The net effect of incorporating defense-in-depth into design, construction, maintenance, and operation is that the facility or system in question tends to be more tolerant of failures and external challenges.