LA-UR-97-1529

CONF-970661--12

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36

TITLE: Safety Analysis, Risk Assessment, and Risk Acceptance Criteria

AUTHOR(S): Kamiar Jamali
Desmond Stack
Harold Sullivan
Dean Sanzo

SUBMITTED TO: Safety Analysis in Transition
Conference sponsored by EFCOG
June 9–13, 1997
Oakland, California

Los Alamos
Los Alamos National Laboratory
Los Alamos, New Mexico 87545

DISCLAIMER

Safety Analysis, Risk Assessment, and Risk Acceptance Criteria

K. Jamali
US Department of Energy
Core Technical Support and Facility Transition (DP-45)
Germantown, Maryland

D. W. Stack, L. H. Sullivan, and D. L. Sanzo
Los Alamos National Laboratory
Technology and Safety Assessment Division
Probabilistic Risk and Hazard Analysis Group (TSA-11)
Los Alamos, New Mexico

Introduction

This paper discusses a number of topics that relate safety analysis as documented in the Department of Energy (DOE) safety analysis reports (SARs), probabilistic risk assessments (PRA) as characterized primarily in the context of the techniques that have assumed some level of formality in commercial nuclear power plant applications, and risk acceptance criteria as an outgrowth of PRA applications. DOE SARs of interest are those that are prepared for DOE facilities under DOE Order 5480.23 and the implementing guidance in DOE STD-3009-94. It must be noted that the primary area of application for DOE STD-3009 is existing DOE facilities and that certain modifications of the STD-3009 approach are necessary in SARs for new facilities. Moreover, it is the hazard analysis (HA) and accident analysis (AA) portions of these SARs that are relevant to the present discussions. Although PRAs can be qualitative in nature, PRA as used in this paper refers more generally to all quantitative risk assessments and their underlying methods. HA as used in this paper refers more generally to all qualitative risk assessments and their underlying methods that have been in use in hazardous facilities other than nuclear power plants.[1] Our discussion includes both quantitative and qualitative risk assessment methods.

PRA has been used, improved, developed, and refined since the Reactor Safety Study (WASH-1400) was published in 1975[2] by the Nuclear Regulatory Commission (NRC). Much debate has ensued since WASH-1400 on exactly what the role of PRA should be in plant design, reactor licensing, "ensuring" plant and process safety, and a large number of other decisions that must be made for potentially hazardous activities. Of particular interest in this area is whether the risks quantified using PRA should be compared with numerical risk acceptance criteria (RACs) to determine whether a facility is "safe." Use of RACs requires quantitative estimates of consequence frequency and magnitude.

Department of Energy Safety Analysis Reports

SARs, as prepared for Department of Energy (DOE) nuclear facilities, have as their goal the documentation of the required nuclear facility safety basis under DOE Order 5480.23.[3] The safety basis is the combination of information related to the control of hazards at a facility (including design, engineering analyses, and administrative controls) on which DOE depends for its conclusion that activities at the facility can be conducted safely.

DOE Order 5480.23 requires those responsible for the design, construction, operation, decontamination, or decommissioning of nuclear facilities to develop safety analyses that establish and evaluate the adequacy of the safety bases of the facilities. The Order is rather general in its guidance; DOE-STD-3009[4] is more specific.

Important in Order 5480.23 and STD-3009 is the fact that there is neither a requirement nor a recommendation that PRA or risk quantification be used in meeting the requirements. Further, there is no requirement in Order 5480.23 to compare SAR hazard and accident analysis results against numerical RACs of any kind, i.e., for the public, the worker, or the environment. It should be made clear that STD-3009 provides offsite evaluation guidelines based on the consequences of the highest consequence scenarios only for the sake of identifying and evaluating safety-class systems, structures, and components (SSCs). Risk quantification, or the acceptance thereof, is in no way related to this process of comparison of consequences with the evaluation guidelines. Note that the use of the terminology "evaluation guidelines" was intentional in an attempt to prevent its potential confusion with "risk acceptance criteria." Despite this clear distinction in terminology, the evaluation guidelines have been frequently misused as *risk acceptance criteria.*

One approach to developing useful safety basis information entails deriving a set of accidents that is designed to determine design, functional, and operational requirements for the facility, process, etc. Depending on when the analysis is performed, these accidents might literally form the basis for the design of the facility [i.e., design-basis accidents (DBAs)], as well as part of its safety basis. Although there is no generally accepted name for a set of accidents used in determining a portion of the safety basis for an existing facility, the DOE-STD-3009 term "derivative design-basis accidents" is used to refer to this set of accidents because they are derived from the HA. For convenience, DBAs and derivative DBAs are referred to collectively as DBAs.

DOE recognized that safety assurance requires a balance of institutional and engineering approaches as part of an ongoing safety process. This recognition formed the basis for a new approach to safety with a focus on the inherent value of the examination process, as opposed to an absolute justification of the facility "as-is" against some predefined expectation. This new approach to safety is reflected in Order 5480.23 and STD-3009 in that there is neither a requirement nor a recommendation that PRA or risk quantification be used in meeting requirements. Furthermore, there is no requirement in Order 5480.23 to compare SAR hazard and accident analyses results against numerical criteria (other than offsite consequence evaluation guidelines used to identify safety-class SSCs). Therefore, risk quantification is not required to determine the safety basis for a facility, process, etc.

DOE's new approach to safety established a broadly defined "safety basis" with increased emphasis on

- institutional safety,
- examining all hazards,
- addressing the whole spectrum of accident conditions,
- consideration of workers and environment, and
- the appropriate use of safety analysis methods.

This led to designating HA as the principal safety tool for use in DOE SARs. The HA is performed to examine the complete spectrum of accidents, qualitatively determine frequency and consequence, identify preventive and mitigative features associated with each accident scenario, and identify unique and representative accidents for further analysis. The raw data in the HA then are summarized in terms of worker safety and defense in depth. From these summaries, safety-significant SSCs and Technical Safety Requirements (TSRs) are derived. Safety-significant SSCs

are SSCs not designated as safety-class SSCs but whose preventive or mitigative function is a major contributor to defense in depth and/or worker safety. The accidents identified in the HA for further analysis are such that the range of accident scenarios analyzed in the SAR form a complete set of bounding conditions to define the envelope of accident conditions to which the operation could be subjected. For operational accidents, accident scenarios are defined based on the physical possibility of phenomena as defined in the HA. Use of a lower binning category such as less than 1E-6/yr is generally appropriate, but it should not be used as a cutoff for dismissing physically credible low probability operational accidents without any evaluation of preventive or mitigative features in HA. This distinction is made to prevent "pencil sharpening" to meet some quantitative cutoff at the expense of objective evaluation of hazards.[4] Operational accident-frequency-based arguments may not be used to dismiss the need (1) for controls or (2) to designate safety-class or safety-significant SSCs.

DBAs and derivative DBAs are analyzed during accident analysis. Accident analysis refers to the quantification of accident consequences. The binning estimates used in the HA are adequate and representative of the level of effort desired for frequency determination.[4] Accident analysis need only document the basis used in HA for assigning accident likelihood to 2-orders-of-magnitude bins. The quantified accident consequences are compared with numerical evaluation guidelines to identify safety-class SSCs and any accident-specific assumptions requiring coverage by TSRs. Information obtained from these accidents is used to specify functional requirements for safety-class SSCs.

The new DOE approach to safety does not attempt to assess or quantify risk rigorously. Only order-of-magnitude estimates of accident frequencies and consequence magnitudes are used in the analysis. Although it is realized that uncertainties are inherent in portions of the deterministic analyses performed in analyzing DBAs, e.g., data and phenomenological uncertainties, there is no attempt to quantify them; however, where large uncertainties exist, it is recommended that analysis error on the conservative side.

Thus, the level of effort involved in risk quantification is substantially less than that required for PRA, particularly for frequency quantification. Although accident analysis typically makes use of fault trees and event trees, they are used primarily to gain a systems understanding. There is no provision or desire for comparison of accident analysis results with RACs to determine whether a facility is acceptable.

Design-Basis Accidents

The traditional nuclear power plant DBA approach as documented in Final Safety Analysis Reports (FSARs) is, in part, a demonstration of adequate (or more appropriately, *acceptable*) facility safety basis and is characterized by a set of postulated and *prescribed* accident initiators and the ensuing events that describe how the accidents unfold. Of course, it is not just the DBAs but the entirety of the SAR and related information that demonstrate acceptable safety. However, the focus of the discussions here is the hazard/accident analysis portion of the SARs. The NRC uses the DBA approach in connection with SAR preparation for commercial nuclear reactor licensing, emphasizing the use of DBAs to meet functional requirements. An important and integral part of this concept is that the limited set of DBAs is a surrogate for the complete spectrum of all release scenarios for a nuclear plant. Furthermore, demonstration of a plant's ability to meet the functional requirements invoked by the DBAs is a demonstration of *acceptable safety.*

DOE's DBAs as used in DOE SARs for *existing facilities* under STD-3009 are different in that the DBAs are not *prescribed* by DOE but are derived from the HA. These DBAs are not a surrogate set of accident scenarios for demonstration of acceptable safety. The STD-3009 approach may be

regarded as a hybrid approach that includes elements of traditional NRC SARs along with those of reactor PRAs. This approach attempts to identify those accident scenarios that should have been (or actually were) used as the basis for design of the facility, in addition to all other scenarios that would have been identified and analyzed in a PRA. The entire spectrum of all accidents substitutes for the deterministically prescribed set of NRC reactor DBAs and is used, in part, *for demonstrating the safety adequacy (as opposed to acceptability).*

Quantitative Risk Goals and Risk Acceptance Criteria

For convenience, all consequence, frequency, and magnitude (risk-based) criteria used to decide whether a facility, process, etc., is "safe" or "acceptable" will be referred to as RACs. RACs *should not to be confused with* either quantitative safety goals or evaluation guidelines used for identifying functional requirements or classifying SSCs. Quantitative safety goals are just that—goals, not requirements. Evaluation guidelines based only on consequence are used in STD-3009 to classify safety-class SSCs and to determine TSR coverage.

There are no frequency-consequence RACs in use by DOE Headquarters nor are any in use by the NRC. Both the NRC and the DOE have safety goals. There have been attempts by various groups to develop RACs.[5] However, there is no accepted set of RACs in the form of frequency-consequence curves in use by the DOE or NRC. The 25-rem limit of 10CFR100 does constitute a RAC for consequences, but there is no associated numerical frequency because the DBA is prescribed deterministically . More importantly, the specific value of 25 rem only makes sense in the context of the prescriptive definition of the DBA. In other words, no reactor would be capable of meeting any reasonably comparable RACs in the frequency and consequence space. The typical commercial reactor would have many release scenarios, all involving containment failure, at frequencies greater than 1E-6 or even 1E-5 per year, with the attendant consequences to the maximally exposed offsite (public) individual in the ranges of hundreds of thousands of rem.

The use of RACs requires a quantitative risk assessment approach as both frequencies and magnitudes of accident consequences must be derived. Uncertainties in the results also must be dealt with.

RACs, in the sense used here, are not in the same vein as Environmental Protection Agency (EPA)-type guidelines, which, for example, specify maximum allowable pollutant or contaminant levels in air and water. EPA guidelines require the measurement of known chemical quantities that are typically the result of chemical or radionuclide discharges occurring from routine operations and relatively high-frequency accidents (emission) or historical sources (waste spills or storage). When used to measure compliance, EPA risk guidelines are not used in conjunction with analysis of low-frequency accidents but rather to evaluate actual discharges (because these would dominate the total risk anyway).[6]

DOE Quantitative Safety Goals

DOE has adopted two quantitative safety goals to limit the risks of fatalities associated with its nuclear operations.[7] The goals are essentially identical to NRC design objectives (1) and (2).

(1) The risk to an average individual in the vicinity of a DOE nuclear facility for prompt fatalities that might result from accidents should not exceed one-tenth of one per cent (0.1%) of the sum of prompt fatalities resulting from other accidents to which members of the population are generally exposed. For evaluation purposes, individuals are assumed to be located within 1 mile of the site boundary.

(2) The risk to the population in the area of a DOE nuclear facility for cancer fatalities that might result from operations should not exceed one-tenth of one per cent (0.1%) of the sum of all cancer fatality risks resulting from all other causes. For evaluation purposes, individuals are assumed to be located within 10 miles of the site boundary.

These safety goals are stated in terms of risk and without regard to the possible types of accidents. It is not stated over what range of consequence frequencies and magnitudes they are applicable. To generate frequency-consequence RACs, a range of applicability must be assumed.

These goals can be translated into quantitative values based on national fatality statistics. Based on US cancer statistics, the cancer fatality goal translates into latent cancer fatality risks as follows.

	DOE Safety Goal	Societal Risk Statistic*	DOE Safety Goal Quantitative Value
Latent Cancer Fatalities	0.1% of cancer risk from all other causes	1.93E-3 fatalities/ person-yr	2E-6 fatalities/person-yr

*Accident frequency data from National Safety Council, 1990.

The safety goal value applies to a population within 10 miles of the site boundary. If a value of 5E-4 fatalities/rem is used to convert fatalities to rem (radiation risk factor from ICRP-60, "1990 Recommendations of the International Commission of Radiation Protection"), a value of 4 mrem/ person-yr is obtained as the equivalent quantitative safety goal in dose-frequency space. Assuming the safety goal is an isorisk criterion applicable over all frequency-consequence space, the following points are on the isorisk curve: 4 mrem at a frequency of 1/yr, 25 rem at a frequency of 1.6×10^{-4}/yr, and 4000 rem at a frequency of 10^{-6}/yr.

NRC Experience with Risk Assessment Criteria

The NRC spent several years trying to incorporate the results of fairly rigorous risk assessments (PRAs) into its regulatory process. Both the ACRS and the Union of Concerned Scientists identified a number of problems in using PRA to define safety aspects of nuclear power plants. Both groups were concerned that there would be use of "bottom-line" (numerical) estimates of PRAs despite their limitations. For example, there is concern that too much attention will be placed on comparing the calculated likelihood of a large-scale core-melt accident at a specific plant with a design objective of 1 in 10,000 per year of reactor operation.

A then-NRC Commissioner expressed concern about the reliance on PRA "bottom-line" results as follows.

> "The Commission appears to be headed toward an over-reliance, in its regulatory decisions, on estimates of the overall nuclear power plant risks which are based on uncertain and unreliable calculational techniques. These techniques cannot bear the weight the Commission intends them to support."

The Acting Director of the Division of Risk Analysis (in the 1980s) emphasized that the basic strengths of PRA are the insights gained as to the type and nature of the most important accident and risk sequences. *He also said that the use of PRA in regulation often focuses on the magnitude of the bottom-line numbers, which is PRA's weakest element. It is his opinion that avoiding the bottom-line numbness would be difficult. He stated that the substantial insights to be drawn form PRA with regard to accident sequences, system reliability, and human performance will be downgraded or even lost if analysts focus on bottom-line results.*

The use of quantitative safety goals, and RACs based on them, to decide if the risks from a given site, facility, or process are acceptable is troublesome. This is evidenced by the rather substantial

criticisms that have been leveled at quantitative RACs, as well as the fact that no universally accepted set of RACs exist for either DOE or NRC. There is no accepted method for turning the safety goals into RACs. Finally, the safety goals themselves are just that—goals, not requirements.

Risk Assessment Uncertainties

The underlying problem with using RACs is that the frequencies and probabilities generated by the risk assessment process have such large uncertainties (typically orders of magnitude) that the comparisons of point values are meaningless.

The state of the art of risk assessment continues to exhibit many uncertainties because it is difficult, if not impossible, to ensure that

1. the analysis is complete, especially the identification of external events;
2. sufficient and reliable data exist to model and quantify accident processes and plant behavior;
3. study analysts have made the best assumptions;
4. computer models represent reality; and
5. uncertainties have been aggregated correctly.

These uncertainties result from a lack of data or understanding of plant system response, human behavior, and accident processes. These five areas of large uncertainty are discussed in more detail below.

To perform a complete risk assessment, the analyst must ensure that all events and combinations of events that could initiate or direct the course of an accident have been identified. This is a difficult, if not impossible, task because there is always the possibility that a scenario has been overlooked. Unintentional omissions include unknown events that have never happened before or can result from the complicated nature of plant operation. Hundreds of thousands of scenarios may be considered in one study, and the chance that a significant combination of events may have been overlooked or screened out cannot be eliminated.

In addition, some events may be omitted purposely because they introduce substantial additional uncertainty into the risk assessment results and are especially difficult to model and quantify. For example, sabotage may be omitted because there is not a basis on which to predict the incidence of sabotage and measure the risk or because analysts assume that its worst consequence could not exceed the worst consequences of other accidents.

Data uncertainties arise because the actual data needed to quantify the systems analysis are usually scarce. Appropriate data may be scarce because of a lack of experience, as is the case with unusual events and failures, or because of a lack of understanding, as is the case concerning phenomena within the containment building during and after core melt. In such situations, little recorded historical experience exists to allow meaningful data to be obtained. Often "generic" data are used that can vary by orders of magnitude from the actual application.

In areas that are not well understood or where few data exist, assumptions may be necessary before analysts can proceed with the study, and the possibility that analysts will make invalid assumptions contributes to uncertainties. Assumptions may simplify a study or limit its scope, or they may be necessary in areas that are not well understood. Subsequently, such assumptions may be questioned by other experts or disputed by new evidence. One of the most basic assumptions used in risk assessments, for example, is that the facility was built to design specifications using concrete and steel reinforcing rods of the required strength.

How accurately computer models characterize accident scenarios, plant response, and human behavior is another area of uncertainty because risk assessment relies on abstract models to describe plant systems, phenomena within containment buildings, and accident consequences. For this reason, analysts intentionally insert a conservative bias into risk assessments where phenomenology is poorly understood. Currently, the problem of determining how representative risk assessment models are is compounded by an inability to validate the models or quantify the extent of these conservatisms.

Finally, note that accident scenarios are usually made up of logical combinations of events, including initiating events, human actions, and system failures. Uncertainties in each of these events are aggregated throughout the accident scenario to yield an overall accident scenario uncertainty. Exclusion of events with large uncertainties, or improper inclusion of these events, can yield erroneous results regarding the overall level of uncertainty.

Conclusions

The use of quantitative safety goals, and RACs based on them, to decide if the risks from a given site, facility, or process are acceptable is troublesome. This is evidenced by the fact that no universally accepted set of RACs exist for either DOE or NRC. Analysis difficulties that preclude the use of RACs include the following factors.

1. **Completeness.** The analysis might have missed dominant accidents during initiating event selection, particularly if the initiating events have gone through a frequency-based screening process.
2. **Uncertainty analysis.** Uncertainty analyses typically performed for PRAs deal only with data uncertainty, which is large in its own right. The analyses do not address the many other uncertainties involved in the PRA, including modeling, phenomenology, success criteria, completeness, maintenance, management, etc. True uncertainty analysis would yield many orders of magnitude in the results.
3. **HRA.** The current state of the art is unable to model or quantify human errors to the level of hardware component failures. Human error modeling might be a bigger issue than just uncertainty. Completeness of all aspects potentially involved in human error modeling is an important issue. This includes such things as poor communication, fatigue, stress, etc. Deliberate acts of malice or sabotage are not addressed, although the disgruntled employee is a much more credible initiating event for many low-frequency, high-magnitude consequence accidents.
4. **Common-cause analysis.** Seemingly independent events can have common maintenance, design, environmental conditions, test procedures, energy flow paths, physical location, energy supplies, etc., that cause them to be dependent under certain conditions. These dependencies can lead to simultaneous failures instead of assumed independent failures.

Quantitative risk assessment does serve many useful purposes. It is useful for risk ranking accident scenarios to gain insight into facility operations and mitigating systems. Risk assessment can quantify relative risk between different accident scenarios and their component parts. It can be used as the basis for risk-benefit studies. Additionally, risk assessment can be used to give a point of reference for the absolute (or real) level of risk involved, but this is perhaps one of the least valuable and uncertain uses of a risk assessment. It is appropriate to realize that risk assessment is a useful adjunct to deterministic accident analysis and is the only way to quantify risk. Thus, analyses requiring quantification, such as risk-based prioritization, risk ranking of accident scenarios, obtaining a point of reference for how risky an endeavor is, estimating risk reduction through mitigative and preventive systems and operations, sensitivity studies, and similar efforts,

are best carried out through risk assessment. Risk assessment tools such as event and fault trees are ideally suited to examining system interactions and dependencies as well as common-cause failures. Based on the results of a risk assessment, recommendations can be made as to potential system modifications and process improvements. Although point-value estimates by themselves have little value, properly presented uncertainty ranges may provide decision-makers valuable input about the relative likelihood of potential accidents.

Use of RACs to determine site, facility, or process acceptability or unacceptability is not defensible. RACs and quantitative safety goals should be viewed as reference points and absolute requirements. Finally, areas where large uncertainties exist, such as modeling, data, phenomenology, etc., must be acknowledged when performing risk assessments and comparing the results with quantitative safety goals.

The combined DBA, derivative DBA, and HA approach to SAR accident analysis such as employed in STD-3009 is recommended. The HA focus on completeness of identifying potential accidents and associated controls is appropriate. Use of HA to provide coarse accident-sequence frequency estimates is in line with its intended use. Accident analysis of resultant DBAs with a consequence evaluation guideline to identify safety-class SSCs and system functional requirements is appropriate.

References

1. *Guidelines for Hazard Evaluation Procedures*, Second Ed., AIChE, Center for Chemical Process Safety (1992).

2. USNRC, "Reactor Safety Study," WASH-1400 (NUREG-75/014) (October 1975).

3. USDOE, "Nuclear Safety Analysis Reports," DOE Order 5480.23 (April 1992).

4. USDOE, "Preparation Guide for US Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports," DOE-STD-3009-94 (July 1994).

5. American Nuclear Society, "American National Standard Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants," ANSI/ANS-51.1-1983 (1983).

6. J. Cohrssen and V. Covello, "Risk Analysis: A Guide to Principles and Methods for Analyzing Health and Environmental Risks," NTIS (1989).

7. Secretary of Energy, "Nuclear Safety Policy," memo SEN-35-91 (September 9, 1991).