Proceedings
of the
International Topical Meeting
on

Safety Margins in Criticality Safety

San Francisco, California
November 26-30, 1989

Sponsored by the American Nuclear Society's
Nuclear Criticality Safety Division

Published by the
American Nuclear Society, Inc.
La Grange Park, Illinois, 60525 USA

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION'S EXPERIENCE IN APPLYING PROBABILISTIC SAFETY ASSESSMENT TECHNIQUES TO NUCLEAR CRITICALITY ACCIDENT ANALYSIS

Robert R. Jackson - SAIC
1845 Terminal Drive, Suite 202
Richland, WA 99352
(509) 943-3133

I. ABSTRACT

Science Applications International Corporation (SAIC) has extensive experience in application of Probabilistic Safety Assessment (PSA) techniques in the nuclear fuel cycle. One specific application is estimating the likelihood for a nuclear criticality accident in proposed and online operations with fissile materials.

Typically, the need for a probabilistic safety assessment for a system originates either in the Safety Analysis Report process, ongoing safety assurance programs, or in design activities (cost-risk tradeoffs). Rigorous application of system safety analysis techniques, skilled and knowledgeable staff, and detailed system definition are crucial to producing analyses and conclusions useful to the designer, plant operator, and safety specialist.

Level of effort varies from a man-month to a man-year, depending on the complexity of the system analyzed and the number of plausible system states. Analytical results may result in design changes, final selection between competing designs, alterations to philosophy and conduct of operations, and process and flowsheet changes.

Principle factors impacting the scope of such analyses include availability of system specific data (design and performance), specificity and enforcement of administrative controls governing operation of the system of interest, and, of course, purpose for the study. Analytical tools include both inductive analyses (e.g., hazards and failure modes and effects) and deductive analyses (e.g., fault trees and event trees). Computer-aided analyses utilizing personal computer-based tools (e.g., SAIC's CAFTA+) are essential.

Analytical uncertainties fall into two categories: near term (primarily data related) and long term (maintenance of the PSA model current with system changes and experience).

II. GENERAL

Science Applications International Corporation (SAIC) has extensive experience as a subcontractor to the Department of Energy (DOE) site operating contractors in application of Probabilistic Safety Assessment (PSA) techniques to evaluate low frequency accidents in non-reactor nuclear facilities. One frequent application is assessing the likelihood of nuclear criticality accidents.

PSA tools and techniques have proven to be of value in analyzing existing and proposed operations with fissile materials. Furthermore, a PSA is essential to satisfying current DOE Design Criteria (cf. DOE Order 6430.1A).

Principal applications are in:

- o accident analyses to support safety analysis report preparation,
- o design tradeoff studies prior to significant plant modification, and
- o ongoing programs for plant safety maintenance and improvement.

Proper use of PSA techniques provides identification, description, and ranking of complicated failure sequences. Since fissile material processes are required to have multiple layers of design and administrative control barriers to preclude nuclear criticality incidents, failure sequences are generally complex and not immediately obvious to the analyst or to those responsible for conduct of operations. Detailed PSA models have proven to be very effective in examining both flowsheet and unit operations inter-relationships, particularly for offstandard conditions (e.g., rework modes, material recycles, and flowsheet deviations).

III. SAIC'S APPROACH TO CONDUCTING A PSA

The analytical tools used, and the level of analytical detail vary depending on the purpose of the assessment and the system (single unit

operation, production line) of interest. The overall strategy, generally used by SAIC, consists of assembling or developing a detailed system description, inductive analysis techniques (i.e., hazards analyses/failure modes and effects analyses) to identify accident precursors, and deductive analyses (i.e., fault trees/event trees) to model system states and fault conditions. This PSA approach is iterative, requiring the system definitions and PSA models to be progressively refined by intensive peer review, both by PSA experts and by customer representatives. This approach is consistent with generally accepted system safety analysis philosophy.

Inductive analyses generally focus on change; specifically, alterations to fissile material inventories and concentrations, variations in process geometry, deliberate and inadvertent variations in process physical and chemical states (especially phase changes), and changes to process states (normal operations, recycle, and abnormal operating conditions including accidents). The final product is a set of tables listing failures and circumstances, associated barriers and preventative measures, detection, associated consequences and mitigating factors. Failure rates or probabilities may be included.

The deductive analyses are initiated by agreement on precisely defined fault conditions (e.g., fissile material mass exceeds a specified value or fissile material concentration achieves a specified value, or a combination of both at a specified location under specific conditions). Use of the system fault condition "nuclear criticality accident occurs" has often proven to be too general for fault tree construction. A useful approach, based on our experience, is to utilize the set(s) of fault conditions to construct event trees. One virtue of this approach is that it separates and emphasizes the conditional probability that a nuclear criticality occurs given that a "near miss" system state exists (the set of fault conditions).

The fault tree construction process is interactive with the evolving inductive analysis. In our experience, these analyses overlap, generally due to schedule constraints. One objective at this stage in the analysis is to ensure that the results of the inductive analysis appear as basic events in the fault trees (i.e., completeness) and that the fault tree logic confirms that the failures and circumstances in the inductive analysis represent basic events (coherence and consistency).

The fault trees are quantified utilizing operations specific data as much as possible. Preferably, data are derived from the experiences associated with the specific system. The data base then reflects the training, experience, and culture (for want of a better term) of the operations staff. If this isn't possible, with a good deal of caution, data may be extrapolated from similar activities within the facility housing the system or similar activities at the same DOE site. The least desirable extrapolations are between DOE sites, or from various generic data bases. Such extrapolations are occasionally necessary but require a great deal of caution. One inclination in such a situation is to err on the side of excessive conservatism (i.e, pessimism).

The fault tree/event tree quantification requires multiple interations. The principal reason is to test, modify as necessary, and validate the logic of the model. Another reason is residual uncertainties regarding the basic event failure rates and probabilities used in quantifying the model. Typically, the customer is thoroughly involved in these iterations, both to serve as a check on the credibility of the results, and as a source of expert opinion on how well the model reproduces the known or anticipated system behavior.

Typically, SAIC requires one man-month of effort for a simple tradeoff study on a single process step. Evaluation of a complicated unit operation (e.g., an ion exchange operation) may require four to six man-months (and one customer representative full-time). Assessment of a process line (e.g., plutonium conversion) may require up to one man-year of effort and involve up to three representatives from the customer.

Involvement of the customer is important for two other reasons. The results belong to the customer and transfer of "ownership" is facilitated if the customer is knowledgeable. Second, the PSA model should be a "living" model, and the customer will have the responsibility of maintaining it.

IV. REQUIREMENTS FOR PERFORMING A PSA

A. Bases.

The bases for a credible and useful PSA are:

1. establishment of a clear objective,
2. precise system definition, and
3. adequate system characterization.

Prior to the initiation of a PSA, a clear and concise task objective must be developed. A typical PSA objective is to answer one or more of the following questions:

- Is the likelihood of a nuclear criticality in this operation 1E/year (or some other value)?
- Does this process (or flowsheet or component or operating mode) change increase or decrease the likelihood of a nuclear criticality? Or

- Of two or more design configurations, which poses the least impact on nuclear safety?

A less frequently requested but extremely valuable analysis results from the question, "Given that an undesirable failure sequence has occured (e.g., a 'near miss'), what is the most effective means of precluding it in the future?"

As with the task objective, a precise system definition is essential to bounding the analysis effort and ensuring successful results.

The system of interest may be a single task, a filtration step, a glovebox or a stand alone process. In any case, a precise definition of what constitutes the system versus what is outside the scope of the analysis is essential to focus the analysis and to permit characterization of the interfaces. Characterization of interfaces is particularly important due to inherent variations at the interfaces (e.g., fissile material compositions and concentrations) and due to provisions for flexibility and recovery in a plant (e.g., rework and recycle capabilities).

Finally, and possibly most important, is the availability and adequacy of the system descriptive documentation. Detailed flowsheets, up-to-date equipment drawings, the as-built configuration drawings, the mission description, and current operating procedures should be available to the analyst. Frequently the documentation for a system is not adequate to support a PSA. Creation of an adequate system description by the PSA team is a common "hidden" cost, and a major factor in PSA schedule slippages.

B. Conducting the PSA

The following are some general observations based on our experiences in conducting these studies.

The PSA team may consist of any number of members. The minimum skills and background required are direct operating experience either with the system of interest or with systems reasonably similar, and system safety analysis experience. These are generally different individuals. Nuclear criticality theory and analysis expertise is generally a requisite, on-call resource, but not necessarily part of the PSA team.

The PSA team must have direct and continuous access to the facility/process (if it exists). The PSA customer should dedicate, at a minimum, a full-time technical contact (preferably in the facility) who is knowledgeable of the configuration, operations, and history of the system.

For operating systems, it is usually necessary for one or more members of the PSA team to "tour" on the off-shifts. This experience occasionally results in significant revisions to opinions and assumptions predicated on other information sources, such as procedures.

Finally, an extremely valuable aid to conducting any PSA is a PC-based fault tree/event tree code with associated data base management capability. We use the SAIC code CAFTA+. Among the many advantages of using a PC-based code are transportability of work in progress, ease of model revision and re-evaluation, and report production.

V. PSA RESULTS AND IMPACTS

The PSA, at a minimum, achieves the original objective; that is, assessment of the likelihood of a nuclear criticality or of a "near miss" for a given system under specified conditions.

Subsequent decisions and actions regarding process configuration, flowsheet, conduct of operations, and adequacy of procedures and administrative controls are profoundly influenced by the results. Even when the final PSA conclusions indicate acceptable nuclear criticality safety, recommendations are made and usually implemented to enhance operational safety.

In our experience, however, this result, while important, is often of less utility than other conclusions and observations drawn from the analysis and the PSA model. One valuable side benefit of a thorough analysis and documentation of a process is an up-to-date and accurate process description. A number of studies we have performed have been or are currently being used as a reference material for indoctrinating new members to the operations staff.

Another incidental result of these analyses has been identification of inconsistencies, discrepancies, and occasionally contradictions in the conduct of sequential operations. Every nuclear criticality PSA we have performed has resulted in revisions to operating procedures and associated process documentation. Many times, the inconsistencies have little or no bearing on nuclear criticality safety, but instead pertain to general monitoring and conduct of operations.

The results of the PSA also provide useful information and insights regarding nuclear safety of the system of interest. The significant (in terms of impact on nuclear criticality safety) components, process steps, operator actions, and design or administrative controls are identified in the fault tree cutsets. Using various importance measures these may, in turn, be ranked in priority. Failures of administrative controls frequently show up at the top of the list as major contributions to system fault conditions. On the other hand, safety design features produce the lowest contributions to the system fault condition. Operations errors and failures of engineered safety features generally fall between these

two extremes. Often, system fault conditions are dominated by inadvertent use of system capabilities originally provided to enhance flexibility or capacity (e.g., excessive ion exchange bed capacity or provision of nonroutine transfer routes).

Another area where the PSA provides useful information is the description and comparison in quantitative terms of the range of system states. In general, normal operations pose less of a hazard than off-standard or unusual operations. Restoration/recovery activities from serious off-standard conditions and resumption of operations after extended outages, in general, seem to pose the most hazard.

One other benefit of a completed PSA is subsequent evaluations of proposed changes to the process, equipment, mission, or conduct of operations. If the PSA model is maintained current with the system configuration, it proves valuable throughout the system life cycle.

VI. CONCLUDING OBSERVATIONS

Probabilistic Safety Assessments are essential to analyze low frequency accidents. When applied to nuclear criticality safety concerns, a PSA provides both a quantitative indication of accident potential and useful insights regarding the system of interest.

The following observations are based on SAIC's experience:

1. The PSA should be initiated as early as is feasible in the project life cycle, given schedule and resource constraints.

2. The PSA model and results should be maintained current with the system throughout the project life cycle.

3. The supporting basic event data bases are improving and will continue to improve as more PSAs are performed.

4. The application of PSA techniques to design and operation tradeoff studies will continue to expand as its utility and cost effectiveness is recognized by plant management.